УДК 681.3.07

О. В. Сілагін, І. Р. Арсенюк, В. І. Месюра, С. В. Кукунін

ПОКРАЩЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ КРИПТОВАЛЮТНИМИ АКТИВАМИ

Вінницький національний технічний університет, Вінниця

Анотація. Робота присвячена удосконаленню дуже актуальної та важливої у наш час програмно-апаратної технології управління криптовалютними активами. Ця технологія, як і додатки, що її реалізують, одержала назву «криптовалютний гаманець». З метою визначення першочергових напрямків удосконалення даної технології було детально проаналізовано сучасні програмно-апаратні рішення існуючих додатків по управлінню криптовалютними активами. Аналіз та вибір методологічних а також технологічних рішень здійснювався, у першу чергу, із застосуванням критеріїв функціональності, зручності та безпеки. У результаті аналізу було показано, що найефективнішою, за вищевказаними критеріями, є технологія, що базується на створенні окремих, так званих «не кастодіальних» мобільних додатків із прив'язкою до відбитку пальця або FACE ID. За результатами здійсненого аналізу було також виявлено, що жодне із наведених технологічних рішень не передбачає реалізацію функції автоматизованого оцінювання рівня привабливості пропозицій із продажу криптовалюти, а також подальшого ранжування пропозицій за цим показником. Саме тому, з метою розширення функціоналу інформаційної технології управління криптовалютними активами було розроблено нову інформаційну технологію, що передбачає уведення функцій оцінювання рівня привабливості пропозицій із продажу криптовалюти, а також ранжування пропозицій провайдерів, залежно від результатів такого оцінювання. Крім того, наведено етапи процесу оцінювання привабливості наявних пропозицій. Запропонована технологія, у свою чергу, є складовою частиною технології криптовалютного гаманця та використовує апарат нечітких множин. Також, у роботі формалізована та змодельована задача оцінювання рівня привабливості пропозицій продажу криптовалют із використанням теорії нечіткої логіки та нечітких множин.

Ключові слова: блокчейн технології, управління криптовалютними активами, функціонал, автоматизоване оцінювання рівня привабливості пропозицій, ранжування пропозицій.

Abstract. The work is devoted to the improvement of a very relevant and important in our time hardware and software technology for managing cryptocurrency assets. This technology, as well as applications that implement it, is called "cryptocurrency wallet". In order to determine the priority areas for improving this technology, modern software and hardware solutions of existing applications for managing cryptocurrency assets were analyzed in detail. The analysis and selection of methodological and technological solutions was carried out, first of all, using the criteria of functionality, convenience and security. As a result of the analysis, it was shown that the most effective, according to the above criteria, is the technology based on the creation of separate, so-called "non-custodial" mobile applications linked to a fingerprint or FACE ID. According to the results of the analysis, it was also found that none of the above technological solutions provides for the implementation of the automated assessment function of the level of proposals attractiveness for the sale of cryptocurrency, as well as further ranking of proposals by this indicator. That is why, in order to expand the functionality of the information technology of cryptocurrency assets management, a new information technology has been developed, which provides for the introduction of functions for assessing the level of offer attractiveness for the sale of cryptocurrency, as well as ranking the provider offers, depending on the results of such an assessment. In addition, the stages of the process of assessing the attractiveness of existing proposals are given. The proposed technology, in turn, is an integral part of the cryptocurrency wallet technology and uses the fuzzy set apparatus. Also, the paper formalized and modeled the problem of assessing the level of attractiveness of cryptocurrency offer sales using the fuzzy logic theory and fuzzy sets.

Key words: blockchain technologies, cryptocurrency asset management, security, automatic search for the best exchange rate.
DOI: https://doi.org/10.31649/1999-9941-2022-55-3-33-43.

Вступ

На початку третього тисячоліття з'явилися революційні веб-технології, які не лише розширили поняття валютних та контрактних відносин, а й мали також величезний соціальний ефект у тому, що повернули людству довіру до «електронного документу». Мова йде про блокчейн технології та пов'язані з ними криптовалюти. Блокчейн – це децентралізована база даних, заснована на одноранговій мережі, загальному реєстрі та криптографії публічного та приватного ключів. Коли цифрова угода здійснюється у блокчейн, вона групується у криптографічно захищеному блоці з іншими угодами, які відбулися в останні декілька хвилин і розсилається усією мережею. Підтверджений блок транзакцій потім датується та додається до ланцюга у лінійному, хронологічному порядку. Нові блоки перевірених транзакцій пов'язані з більш старими блоками, утворюють ланцюжок блоків, які показують кожну транзакцію, досягнуту в історії цього блокчейну. Увійшовши в блокчейн-мережу, користувач підключається до інших комп'ютерів мережі для того, щоб обмінюватися з ними даними: блоками і записами. Отримавши нові дані, кожен користувач перевіряє їх коректність, і, переконавшись у достовірності, зберігає їх у себе, а також передає коректні дані далі мережею [1 – 5].

Найбільшого поширення блокчейн технології набули у сфері створення віртуальних грошей – криптовалют, а це, у свою чергу, дало поштовх для створення нового класу веб-додатків для управління криптовалютними активами, що одержали назву «криптовалютних гаманців».

Актуальність

Отже криптовалютний гаманець – це, по суті, інформаційна технологія, реалізована у програмному додатку, за допомогою якого можна управляти криптовалютою або криптовалютами певного користувача. Основними функціями гаманця є зберігання, а також продаж та закупівля криптовалюти від інших користувачів. Але, на відміну від класичних банківських електронних кабінетів, криптовалютний гаманець має свою специфіку, пов'язану з використаннями блокчейн технологій. На сьогоднішній день від-

чується дефіцит зручних, надійних і широкофункціональних сервісів з обслуговування криптовалют, тому тема дослідження є досить важливою та актуальною.

Аналіз відомих рішень

Хоча з моменту появи першої криптовалюти минуло лише близько 12 років, вже склалася певна класифікація криптовалютних гаманців. Так, за ступенем універсальності вони можуть бути одновалютними та мультивалютними, за типом зберігання криптовалюти їх можна розділити на «гарячі» та «холодні»; за типом зберігання приватних ключів – на «кастодіальні» та «не кастодіальні», а за типом інсталяції – на локальні, мобільні, серверні, апаратні, браузерні. У найпростішому варіанті – це просто дані, які забезпечують доступ до свого рахунку. Ці дані, залежно від типу гаманця, можуть являти собою стандартну пару «емейл + пароль», приватний ключ або seed-фразу.

Основним завданням гаманця є можливість зберігати, а також надсилати та отримувати криптовалюти від інших людей.

Відмінність між гарячим і холодним гаманцем полягає в тому, що гарячий гаманець працює при підключенні до інтернету, а холодний може працювати і без такого доступу. Гарячі електронні гаманці менш захищені, оскільки існує ризик крадіжки ваших персональних даних через інтернет, проте, при цьому вони більш затребувані серед користувачів. Холодні електронні гаманці, відповідно, більш безпечні.

Суть кастодіальних гаманців полягає у тому, що вони не дають доступу до свого приватного ключа, а просто зберігають його на своєму централізованому сервері. Найчастіше таке рішення надають криптовалютні біржі. Його перевага полягає в тому, що можна відновити доступ до облікового запису через пошту, якщо пароль був загублений. Недолік полягає у тому, що обліковий запис може бути заморожено у разі якогось втручання, а для розморожування, користувача можуть попросити пройти процедуру KYC (Know Your Customer – знай свого клієнта) підтвердження особистості. Також користувач може втратити гроші під час хакерських атак, що останнім часом є досить частим явищем.

Некастодіальні електронні гаманці працюють інакше. Вони надають повний контроль над своїми приватними ключами, не використовуючи сервер. Величезною перевагою такого рішення є те, що кошти належать тільки користувачеві. Ніхто інший не зможе ними заволодіти без його seed-фрази. Однак, у цьому полягає і недолік такого гаманця, адже, якщо seed-фраза буде втрачена, то доступ до гаманця вже ніяк не повернути.

Локальний (десктопний) гаманець – це програма, яка встановлюється на стаціонарний комп'ютер або ноутбук. Даний вид гаманців є одним з найскладніших для користувачів, але при цьому володіє найкращими показниками безпеки та анонімності. Слід відзначити, що найчастіше їх використовують досвідчені користувачі або компанії, які проводять розробки на блокчейн-технологіях. Десктопні електронні гаманці можна розділити на 2 види: товстий та тонкий.

- У випадку використання товстого гаманця передбачається завантаження на комп'ютер повної копії блокчейна. За фактом товстий гаманець криптовалют це повна нода мережі, яка не лише дозволяє вам керувати своїм рахунком, а й підтримує роботу блокчейна. З огляду на те, що об'єм блокчейн-біткоїна займає вже близько 250 Гб – для роботи гаманця, відповідно, потрібно високопродуктивне «залізо».
- Тонкий гаманець, на відміну від товстого, займає на комп'ютері всього кілька мегабайт пам'яті та встановлюється за пару хвилин. Це програма-клієнт, для роботи якої не потрібно завантажувати на комп'ютер увесь блокчейн. Він дозволяє створювати адреси криптовалют і виконувати транзакції. З блокчейном тонкі гаманці взаємодіють не безпосередньо, як товсті гаманці, а через сервер розробників програми. Тому вони вважаються менш захищеними, але, натомість, набагато зручнішими у використанні.

Апаратний гаманець криптовалют це окремий пристрій, що на вигляд нагадує «флешку». Такий блокчейн гаманець служить для «холодного» зберігання криптовалют і підключається до інтернету тільки тоді, коли потрібно зробити транзакцію. Апаратні гаманці надають зручний доступ до блокчейну з високим ступенем захисту, оскільки приватні ключі зберігаються тільки у пам'яті самого пристрою. Незважаючи на їх вартість (від 60 до 100 доларів), вони дозволяють здійснювати транзакції таким чином, що хакери не можуть до них дістатися. У випадку втрати такого гаманця ніхто крім вас не зможе нічого зробити із засобами, при цьому ви з легкістю зможете відновити до них доступ через seed-фразу на новий пристрій. Тому по співвідношенню надійності та зручності використання лідирують апаратні гаманці.

Web- або браузерні гаманці – ще один, досить простий тип гаманців для використання, він не вимагає від користувача якихось особливих знань у криптовалютах. Його основні переваги:

- користуватися гаманцем можна на різних пристроях, незалежно від вашого місця знаходження, головне, щоб був вільний доступ до Інтернету;
- немає необхідності у скачуванні усіх блоків мережі, що економить багато часу та дисковий простір;

– у більшості, подібні сервіси пропонують своїм користувачам додаткові зручності, такі як відсутність комісії на перекази між користувачами, надсилання монет іншим його користувачам на адресу електронної пошти або номер телефону.

Однак, ми повинні пам'ятати, що такі гаманці мають «кастодіальне» рішення. При використанні Web-гаманця доступ до коштів має і сторонній сервіс. Тому їх збереження залежить вже не тільки від самого користувача.

Мобільні гаманці криптовалют – це додатки, які можна встановити на мобільні пристрої (смартфони, планшети). Потрібно відзначити, що вони увібрали в себе всі кращі якості від перерахованих вище видів гаманців, адже можуть бути «не кастодіальними», досить анонімними і при цьому надають доступ до криптовалют у будь-якій точці світу де є Інтернет. Оскільки це окремий додаток, то найчастіше розробники наділяють його ще й корисними додатковими функціями. Що стосується безпеки, то мобільні гаманці займають «золоту середину», оскільки крім звичайного PIN-коду можуть мати прив'язку до відбитку пальця або FACE ID (зазвичай налаштовується користувачем за бажанням).

Деякі з наведених технічних рішень пропонують пошук мінімального криптовалютного курсу або ранжування продавців за величиною курсу продаж, але поки ще ніхто не запропонував функціонал з багатокритеріального ранжування пропозицій з продажу криптовалюти, з урахуванням усіх суттєвих особливостей ринку торгівлі криптовалютою. Комплексний показник, що враховує всі ці особливості можна було б назвати рівнем «привабливості» пропозиції. Для прийняття рішень на основі «привабливості» пропозиції доцільно було б використати одну з існуючих інтелектуальних технологій ідентифікації [6, 7].

Мета

Метою дослідження є покращення існуючої технології управління криптовалютними активами «криптовалютний гаманець» за рахунок розширення її функціоналу. А саме, введення функцій оцінювання рівня «привабливості» пропозицій з продажу криптовалюти та ранжування пропозицій провайдерів у залежності від результатів оцінювання, а також розробка технології, що їх реалізує.

Задачі

Для досягнення поставленої мети потрібно розв'язати такі задачі:

1. Сформулювати перелік умов, технічних особливостей та ринкових характеристик, які суттєво впливають на рівень «привабливості».
2. Вибрати та застосувати одну з інтелектуальних технологій ідентифікації.
3. Змоделювати базу знань та механізм виведення результату.
4. Покращити існуючу інформаційну технологію управління криптовалютними активами за рахунок додавання нового функціоналу у вигляді технології з оцінювання рівня «привабливості» пропозицій провайдерів з продажу криптовалюти та ранжуванню цих пропозицій.

Розв'язання задач

Формулювання умов, технічних особливостей та ринкових характеристик, які суттєво впливають на рівень «привабливості» пропозиції

На відміну від звичайних «класичних» валют, криптовалюти несуть у собі деякі специфічні відмінності, пов'язані з процедурами їх створення, забезпечення, передачі та зберігання. По суті кожна з них є віртуальною готівкою, образом унікальної комп'ютерної технології, «законсервованої» у вигляді ланцюжків блокчейн, направлених ациклічних графів, консенсусних реєстрів (ledger) та ін. До таких відмінностей можна віднести:

– криптовалюти не належать жодній державі або державним союзним утворенням;
– не мають централізованого управління та емітентів;
– забезпечують анонімність користувачів;
– у більшості фіксована верхня межа загального обсягу емісії;
– можлива як емісія, так і демісія;
– великий час підтвердження транзакцій;
– платіж (передача криптовалюти між адресами) відбувається без посередників (банків та операторів платіжних систем);
– платіж є незворотній – немає механізму скасування підтвердженої операції;
– менш залежні від коливань світової та локальних економік;
– практично не використовуються у банківській діяльності для створення цінних паперів;
– їх розповсюдження та використання безпосередньо залежить від технологічної зрілості регіонів.

Ураховуючи ці відмінності, ми можемо сформувати певний онтологічний словник в області знань, яку можна охарактеризувати як оцінювання «привабливості» пропозицій з продажу криптовалюти.

Це буде по кожній із криптовалют: x_1 – вид криптовалюти; x_2 – об'єм продажу; x_3 – курс продажу криптовалюти; x_4 – величина комісійних; x_5 – стабільність криптовалюти; x_6 – наявність або відсутність

фіксації курсу на час обробки запиту; x_7 – швидкість проведення операції; x_8 – надійність виконання запиту, що означає те, що запит точно буде оброблено і неможливість його відхилення, що також може призвести до втрати коштів через стрибки курсу.

Одночасно він може бути представлений як вхідний вектор змінних $X(x_1, x_2, \ldots, x_8)$ для технології ідентифікації, на виході якої одержуємо показник рівня «привабливості» пропозиції Y, так, як це наведено на рис. 1.

Рисунок 1 – Технологія ідентифікації рівня привабливості

Аналіз та вибір інтелектуальної технології ідентифікації

Серед інтелектуальних технологій, за допомогою яких можна розв'язати усі задачі проекту, можна виділити штучні нейронні мережі (ШНМ), генетичні алгоритми та нечітку логіку. Розглянемо їх детальніше.

ШНМ традиційно використовують у ряді різноманітних задач, наприклад комп'ютерного зору, розпізнавання мовлення, машинного перекладу, соціально-мережевої фільтрації, відеоіграх, та у медичному діагностуванні.

Недоліком цього методу є відсутність твердих правил щодо вибору швидкості навчання та розміру мережі для вирішення конкретного завдання, невизначеність у підборі кількості нейронів у шарі мережі та кількості шарів ШНМ. Також цей підхід потребує проведення дуже великої кількості експериментів.

Генетичні алгоритми можуть використовуватись для пошуку рішень у дуже великих і важких просторах пошуку.

Відразу ж відзначимо, що застосування генетичного алгоритму в даній задачі є недоцільним, тому що критерій добору хромосом і використання процедур є евристичним, що зовсім не гарантує знаходження найкращого рішення. Іншим недоліком є велика обчислювана складність.

Нечітка логіка [6] є узагальненням класичної логіки на випадок, коли істинність розглядається як лінгвістична змінна, що приймає значення типу: "дуже істинно", "більш-менш істинно", "не дуже хибно" і т. д.

Зазначені лінгвістичні значення (терми) представляються нечіткими множинами. Нечіткі множини – це засоби формалізації природно-лінгвістичних висловлювань та логічних висновків. Ідея, що лежить в основі формалізації причинно-наслідкових зв'язків між змінними «входи-виходи», полягає в описі цих зв'язків на природній мові з використанням теорії нечітких множин та лінгвістичних змінних. Моделі об'єктів будуються шляхом проектування та налаштування нечітких баз знань, що представляють собою сукупності лінгвістичних висловлювань типу ЯКЩО <входи>, ТО <виходи>. Налаштовуючи нечітку базу знань через зміну параметрів функцій належності лінгвістичних термів можна ідентифікувати нелінійні залежності з необхідною точністю. Нечіткі межі множини кількісних значень, що відповідають певному лінгвістичному терму змінних вхідного вектору з рис. 1, є серйозною запорукою для використання нечітких баз знань і нечіткого логічного виводу в задачі оцінювання «привабливості» пропозицій з продажу криптовалют.

Серед трьох, незалежних одна від одної, теорій ідентифікацій та прийняття рішень – нечітких множин, нейронних мереж та генетичних алгоритмів, для задачі оцінювання «привабливості» пропозицій з продажу криптовалют, найбільш доцільним є застосування теорії нечітких множин та нечіткої логіки. Основою створюваної технології є формування із застосуванням методів нечіткої логіки, матричної бази знань та застосуванням до неї продукційної системи навчання та виводу. Головною перевагою застосу-

вання інтелектуальної технології нечітких множин є можливість налаштування та адаптації бази знань до конкретних умов прийняття рішень, а саме навчання.

Ієрархічна модель логічного виведення (формалізація та фазифікація моделі)

Нами розглядається об'єкт з одним виходом та n входами вигляду:

$$y = f_y\,(x_1, x_2, \dots, x_n), \tag{1}$$

де y – вихідна змінна; $x_1, x_2, \dots, x_n$ – вхідні змінні.

Змінні $x_1, x_2, \dots, x_n$ та *y* можуть бути кількісними і якісними.

Для встановлення залежності (1) будемо розглядати вхідні змінні $x_j,\ i = \overline{1,n}$ та вихідну змінну *y* як лінгвістичні змінні [6].

Для оцінки лінгвістичних змінних $x_j, i = \overline{1,n}$ та *y* будемо використовувати якісні терми з наступних терм-множин:

$A_i = \{a_i^1, a_i^2, \dots, a_i^{l_i}\}$ – терм-множина змінної $x_j, i = \overline{1,n}$, $D = \{d_1, d_2, \dots, d_m\}$ – терм-множина *y,* де a_i^p – p-й лінгвістичний терм змінної $x_j, p = \overline{1,l_j},\ i = \overline{1,n}$. d_j - j-й лінгвістичний терм змінної y, m – число різноманітних рішень області, що розглядається. Потужності терм-множин A_i , $i = \overline{1,n}$ у загальному випадку можуть бути відмінними, тобто $l_1 \neq l_2 \neq \cdots \neq l_n$.

Назви окремих термів $a_i^1, a_i^2, \dots, a_i^{l_i}$ можуть також відрізнятися один від одного для різноманітних лінгвістичних змінних $x_j, i = \overline{1,n}$.

Лінгвістичні терми $a_i^p \in A_i$ та $d_j \in D$, $p = \overline{1,l_j}$, $i = \overline{1,n}$, $j = \overline{1,m}$ будемо розглядати як нечіткі множини.

Для зручності одночасного оперування та створення експертних висновків згрупуємо ті показники, що формують оцінювання вартості купівлі криптовалюти в окрему групу, а ті, що оцінюють ризики під час купівлі криптовалюти в іншу, та замінимо лінійну модель вектора вхідних змінних (див. рис. 1) на ієрархічну. Ієрархічний взаємозв'язок між вхідними параметрами, групами вхідних параметрів і вихідною змінною (інтегральним показником), представимо у вигляді дерева рішень (рис. 2), якому відповідає система відношень (2) – (4). Одночасно фазифікуємо нечіткі змінні, а саме поставимо їм у відповідність деяку кількість нечітких лінгвістичних термів, кожен з яких представляє нечітку множину значень певного показника. Функції належності цих нечітких термів будуть визначені пізніше.

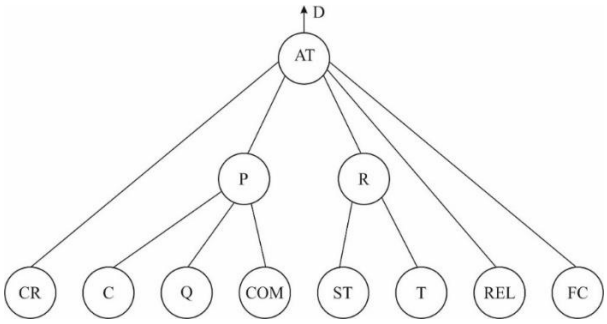

Рисунок 2 – Ієрархічне дерево рішень

$$AT = f_A\,(CR, P, R, FC, REL); \tag{2}$$

$$P = f_P\,(C, Q, COM); \tag{3}$$

$$R = f_R\,(T, ST), \tag{4}$$

де: AT (attractiveness) – нечітка логічна вихідна змінна, глобальний показник привабливості пропозиції, залежить від виду криптовалюти, локального показника оцінювання рівня вартості пропозиції криптовалюти, локального показника оцінювання рівня ризику втрат від нестабільності курсу та швидкості підтвердження транзакції, можливості фіксації курсу та показника рівня довіри до продавця, приймає значення одного з 11 лінгвістичних термів, які представляють популярну шкалу оцінювання товарів і послуг 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, що використовується для рейтингування товарів та послуг;

CR (cryptocurrency) – чітка вхідна змінна, код криптовалюти, представляє собою порядковий номер криптовалюти з таблиці кривтовалют;

P (price) – нечітка логічна вихідна змінна, локальний показник оцінювання рівня вартості пропозиції криптовалюти, з врахуванням показника курсу, показника об'єму пропонованої валюти, показника величини комісійних, приймає значення: М – мала, МС – менше середньої, С – середня, БС – більше середньої, В – велика;

R (risk) – нечітка логічна вихідна змінна, локальний показник оцінювання рівня ризику втрат від нестабільності курсу та швидкості підтвердження транзакції, залежить від нестабільності курсу та часу підтвердження транзакції, приймає значення: М – малий, МС – менше середнього, С – середній, БС – більше середнього, В – великий;

C (course) – нечітка логічна вхідна змінна, показник рівня курсу за яким продається криптовалюта, формується по відношенню до математичного очікування курсових пропозицій по видам криптовалют. Приймає значення: М – малий, МС – менше середнього, С – середній, БС – більше середнього, В – великий.

Q (quantity) – нечітка логічна вхідна змінна, кількість пропонованої криптовалюти. Приймає значення: М – мала, МС – менше середньої, С – середня, БС – більше середньої, В – велика;

COM (commission) – нечітка логічна вхідна змінна, показник величини комісійних під час проведення транзакції, формується по відношенню до математичного очікування комісійних провайдерів. Приймає значення: М – малий, МС – менше середнього, С – середній, БС – більше середнього, В – великий;

ST (stability) – нечітка логічна вхідна змінна, показник стабільності курсу криптовалюти. Приймає значення: М – мала, МС – менше середньої, С – середня, БС – більше середньої, В – висока;

T (time) – нечітка логічна вхідна змінна, показник величини часу на підтвердження запиту, формується по відношенню до усередненого часу обробки та підтвердження запиту. Приймає значення: М – малий, МС – менше середнього, С – середній, БС – більше середнього, В – великий;

REL (reliability) – нечітка логічна вхідна змінна, показник надійності продавця, демонструє рівень довіри до продавця в тому, що запит буде підтверджено, приймає значення: НВ – невідомий, М – малий, С – середній, В – великий;

FC (fixation of the course) – чітка вхідна бінарна змінна, показник фіксації курсу на час підтвердження транзакції, приймає значення 0, 1 (істина). При значенні 1 відключає вплив локального показника R.

Моделювання нечіткої бази знань

При моделюванні бази знань представимо співвідношення значень вхідних та вихідних змінних у вигляді таблиці (матричне представлення) [6, 7]. Задача експерта – розбити при цьому всі можливі доцільні комбінації значень восьми вхідних змінних на 11 груп, що відповідають значенням (термам) вихідної змінної.

Візьмемо *N* можливих доцільних комбінацій (за думкою експерта), які зв`язують входи і виходи об`єкта ідентифікації, і розподілимо їх таким чином:

$$N = k_1 + k_2 + \cdots k_m,$$

де k_j – число експериментальних даних, які відповідають вихідному рішенню $d_j, j = \overline{1,m}$, m – число вихідних рішень (для нашого випадку $m = 11$), причому, в загальному випадку $k_1 \neq k_2 \neq \cdots \neq k_m$.

Передбачається, що $N < l_1 \cdot l_2 \cdot \ldots \cdot l_n$, тобто число відібраних експериментальних даних менше повного перебору різних станів вхідного вектору X. Де l_i $(i = \overline{1,n})$ – число термів лінгвістичної змінної x_i, а *n* – кількість вхідних змінних.

Пронумеруємо *N* доцільних комбінацій таким чином:

11, 12, 1k_1 – номери комбінацій вхідних змінних для вирішення d_1;

21, 22, 2k_2 – номери комбінацій вхідних змінних для вирішення d_2;

…

j1, j2, jk_j – номери комбінацій вхідних змінних для вирішення d_j;

…

m1, m2, mk_m – номери комбінацій вхідних змінних для вирішення d_m.

Матрицею знань для нашого випадку буде таблиця, сформована за такими правилами (табл. 1):

1) Розмірність матриці дорівнює $(n+1) \times N$, де $(n+1)$ – число стовбців, а $N = k_1 + k_2 + \cdots k_m$ – число рядків (*n* = 8, *m* = 11).

2) Перші n стовбців матриці відповідають вхідним змінним x_i, $i = \overline{1,n}$, а $(n+1)-$й стовбець відповідає значенням d_j вихідної змінної y $(j = \overline{1,m})$.

3) Кожен рядок матриці являє собою деяку комбінацію значень вхідних змінних, віднесених експертом до одного з можливих значень вихідної змінної y. При цьому: перші k_1 рядків відповідають значенню вихідної змінної $y = d_1$, другі k_2 рядків $y = d_2$,…, останні k_m рядків – значенню $y = d_m$.

4) Елемент a_i^{jp}, який стоїть на перетині і-го стовбця і jp-го рядка відповідають лінгвістичній оцінці параметра x_i у рядку нечіткої бази даних з номером jp. При цьому лінгвістична оцінка a_i^{jp} вибирається із терм-множини, яка відповідає змінній x_i, тобто $a_i^{jp} \in A_i$, $i = \overline{1,n}$, $j = \overline{1,m}$, $p = \overline{1,k_1}$.

Таблиця 1 – Узагальнена матриця знань

Номер вхідної комбінації значень	Вхідні змінні				Вихідна змінна
	x_1	x_2	…x_i…	x_7	
11 12 … $1k_1$	a_1^{11} a_1^{12} $a_1^{1k_1}$	a_2^{11} a_2^{12} $a_2^{1k_1}$	$\ldots a_i^{11} \ldots$ $\ldots a_i^{12} \ldots$ $\ldots a_i^{1k_1} \ldots$	a_7^{11} a_7^{12} $a_7^{1k_1}$	d_1
…					
j1 *j2* … jk_j	a_1^{j1} a_1^{j2} $a_1^{jk_j}$	a_2^{j1} a_2^{j2} $a_2^{jk_j}$	$\ldots a_i^{j1} \ldots$ $\ldots a_i^{j2} \ldots$ $\ldots a_i^{jk_j} \ldots$	a_7^{j1} a_7^{j2} $a_7^{jk_j}$	d_j
…					
m1 *m2* … mk_m	a_1^{m1} a_1^{m2} $a_1^{mk_m}$	a_2^{m1} a_2^{m2} $a_2^{mk_m}$	$\ldots a_i^{m1} \ldots$ $\ldots a_i^{m2} \ldots$ $\ldots a_i^{mk_m} \ldots.$	a_n^{m1} a_n^{m2} $a_n^{mk_m}$	d_m

Уведена матриця знань визначає систему логічних висловлювань типу «ЯКЩО-ТО, ІНАКШЕ», які пов`язують значення вхідних змінних $x_1 \div x_n$ з одним із можливих типів вирішення d_j, $j = \overline{1,m}$:

ЯКЩО ($x_1 = a_1^{11}$) І ($x_2 = a_2^{11}$) І….І ($x_n = a_n^{11}$) АБО
($x_1 = a_1^{12}$) І ($x_2 = a_2^{12}$) І….І ($x_n = a_n^{12}$) АБО…
($x_1 = a_1^{1k_1}$) І ($x_2 = a_2^{1k_1}$) І….І ($x_n = a_n^{1k_1}$),
ТО $y = d_1$, ІНАКШЕ
ЯКЩО ($x_1 = a_1^{21}$) І ($x_2 = a_2^{21}$) І….І ($x_n = a_n^{21}$) АБО
($x_1 = a_1^{22}$) І ($x_2 = a_2^{22}$) І….І ($x_n = a_n^{22}$) АБО…
($x_1 = a_1^{2k_2}$) І ($x_2 = a_2^{2k_2}$) І….І ($x_n = a_n^{2k_2}$),
ТО $y = d_2$, ІНАКШЕ
ЯКЩО ($x_1 = a_1^{m1}$) І ($x_2 = a_2^{m1}$) І….І ($x_n = a_n^{m1}$) АБО
($x_1 = a_1^{m2}$) І ($x_2 = a_2^{m2}$) І….І ($x_n = a_n^{m2}$) АБО…
($x_1 = a_1^{mk_m}$) І ($x_2 = a_2^{mk_m}$) І….І ($x_n = a_n^{mk_m}$),
ТО $y = d_m$, (5)

де $d_j (j = \overline{1,m})$ – лінгвістична оцінка вихідної змінної *y*, яка визначається з терм множини *D*; a_i^{jp} – лінгвістична оцінка змінної x_i в *p*-ому рядку *j*-ї диз`юнкції, яка вибирається з терм множини A_i, $i = \overline{1,n}$, $j = \overline{1,m}$, $p = \overline{1,k_1}$; k_j – кількість правил, які визначають значення вихідної змінної $y = d_j$.

Будемо називати подібну систему логічних висловлювань *нечіткою базою знань.*

Фрагмент нечіткої бази знань для локального показника P, де y = P, x_1 = C, x_2 = Q, x_3 = COM, буде мати такий вигляд:

ЯКЩО (C = *M*) І Q = *M*) І (COM = M) АБО
(C = *MC*) І Q = *M*) І (COM = M) АБО

(C = M) I Q = MC) I (COM = M) АБО
(C = M) I Q = M) I (COM = MC) АБО
(C = MC) I Q = MC) I (COM = M),
ТО P = M, ІНАКШЕ,
ЯКЩО (C = M) I Q = MC) I (COM = MC) АБО
(C = MC) I Q = M) I (COM = MC) АБО
(C = MC) I Q = MC) I (COM = MC) АБО
(C = C) I Q = MC) I (COM = MC) АБО
(C = MC) I Q = C) I (COM = MC) АБО
(C = MC) I Q = MC) I (COM = C),
ТО P = MC, ІНАКШЕ,
…
ЯКЩО (C = B) I Q = B) I (COM = БС) АБО
(C = Б) I Q = БС) I (COM = Б) АБО
(C = БC) I Q = B) I (COM = B) АБО
(C = B I Q = B) I (COM = B),
ТО P = B (6)

Аналогічно формуємо нечітку базу знань для локального показника R, де y = R, x_1 = T, x_2 = ST.

ЯКЩО (T = M) I (ST = M) АБО
(T = MC) I (ST = M) АБО
(T = M) I (ST = MC),
ТО R = M, ІНАКШЕ,
ЯКЩО (T = MC) I (ST = MC) АБО
(T = C) I (ST = MC) АБО
(T = MC) I (ST = C),
ТО R = MC, ІНАКШЕ,
…

ЯКЩО (T = B) I (ST = MB) АБО
(T = MB) I (ST = B) АБО
(T = B) I (ST = B),
ТО R = B (7)

А також фрагмент бази знань для глобального показника AT, де y = AT, x_1 = CR, x_2 = P, x_3 = R, x_4 = FC, x_5 = REL.

ЯКЩО (CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B) АБО
(CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B) АБО
(CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B) АБО
(CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B), ТО
AT = 10, ІНАКШЕ,
ЯКЩО (CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B) АБО
(CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B) АБО
(CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B) АБО
(CR = 1) I (P = M) I (R = M) I (FC = 0) I (REL = B), ТО
AT = 9, ІНАКШЕ,
…
ЯКЩО (CR = 1) I (P = B) I (R = B) I (FC = 0) I (REL = HB) АБО
(CR = 1) I (P = B) I (R = BC) I (FC = 0) I (REL = HB) АБО
(CR = 1) I (P = B) I (R = B) I (FC = 0) I (REL = M) АБО
(CR = 1) I (P = BC) I (R = B) I (FC = 0) I (REL = M), ТО
AT = 0. (8)

З використанням операцій ∪ (АБО) і ∩ (І) система логічних висловлювань (4) може буди подана у більш компактному вигляді:

$$\cup_{p=1}^{k_j}\left[\cap_{i=1}^{n}\left(x_i = a_i^{jp}\right)\right] \rightarrow y = d_j, j = \overline{1,m}. \quad (9)$$

Таким чином шукане співвідношення (1), яке встановлює зв`язок між вхідними параметрами x_i та вихідною змінною *y,* формалізовано у вигляді системи нечітких логічних висловлювань (6) – (8), яка базується на уведеній нами матриці знань (табл. 1).

Функції належності лінгвістичних термів

За визначенням [6], функція належності $\mu^T(x)$ характеризує суб`єктивну міру (в діапазоні $[0,1]$) впевненості експерта в тому, що чітке значення *x* відповідає нечіткому терму *T*. Найбільше розповсюдження в практичних додатках [8, 9] отримали трикутні, трапецієподібні, дзвоноподібні (гаусові) функції належності, параметри яких дозволяють змінювати форму функцій.

У роботі [7] запропонована проста та зручна для налаштування аналітична модель функцій належності змінної *x* довільному нечіткому терму *T* у вигляді:

$$\mu^T(x) = \frac{1}{1+\left(\frac{x-b}{c}\right)^2}, \tag{10}$$

де b і c – параметри налаштування; b – координата максимуму функції $\mu^T(b) = 1$; c – коефіцієнт концентрації – розтягу функції (рис. 3).

Для нечіткого терма *T* число b являє собою найбільш можливе значення змінної *x.*

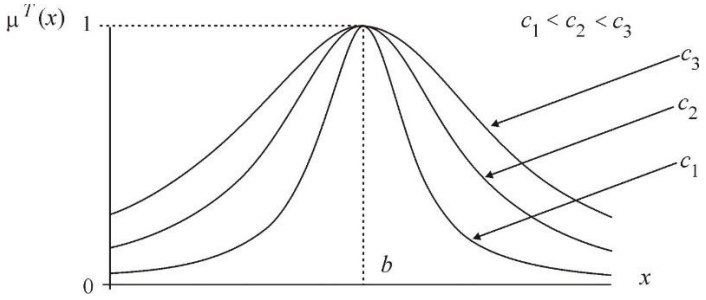

Рисунок 3 – Модель функції належності

Моделювання механізму виведення результату

У попередньому матеріалі ми визначилися:

- з множиною рішень $D = \{d_1,\ d_2, \dots, d_m\}$, які відповідають вихідній змінній *y*;
- вектором вхідних змінних $X = (x_1,\ x_2, \dots, x_n)$;
- сформували матрицю знань.

Для виведення результату, скористаємося методом, що запропонований у роботі [7]. Ідея методу полягає у використанні нечітких логічних рівнянь. Ці рівняння будуються на базі матриці знань чи ізоморфній їй системі логічних висловлювань (5 – 7) і дозволяють обчислювати значення функцій належності різних розв'язків при фіксованих значеннях вхідних змінних об'єкта. Ці нечіткі логічні рівняння отримані з нечіткої бази знань (4) шляхом заміни лінгвістичних термів a_i^{jp} і d_j на відповідні функції належності, а операції ∪ та ⋂ – на операції ∨ і ∧. Детально механізм нечіткого логічного виведення результату описаний в [7].

Розробка технології оцінювання рівня «привабливості» пропозицій з продажу криптовалюти та ранжування пропозицій в залежності від результатів оцінювання

Як говорилось раніше, розроблювана технологія рейтингування продавців криптовалюти за рівнем «привабливості» є складовою частиною загальної технології по управлінню криптовалютними активами під назвою «криптовалютний гаманець» і покращує цю технологію за рахунок розширення функціоналу.

Вихідними даними для роботи технології є:

1. Запит на купівлю криптовалют певного виду

$$\text{LIST\_ ORDER (CR1(V1), CR2(V2), …, CRN(VN)),} \tag{11}$$

де CR1, CR2, …, CRN – види криптовалют; а V1,V2, …, VN – відповідно, об'єми закупівлі різних видів криптовалют.

2. Перелік активних на даний момент провайдерів, що вийшли на ринок з пропозиціями на продаж певного виду криптовалюти в певних об'ємах

$$LIST\_\ CR1(PROVIDER1(Q1), PROVIDER2(Q2), \dots, PROVIDERM\ (QM)), \quad (12)$$

де PROVIDER1, PROVIDER2, … , PROVIDERM – ідентифікатори провайдерів; Q1, Q2, … , QM – відповідні об'єми продажу криптовалют.

Результатом роботи технології є список LIST_ CR1_RAN цих же провайдерів, ранжований за рівнем «привабливості».

Кожен провайдер характеризується наступними атрибутами, які мають суттєвий вплив на привабливість пропозиції з продажу криптовалюти: PROVIDER (CR (cryptocurrency), C (course), Q (quantity), COM (commission), ST (stability), T (time), REL (reliability), FC (fixation of the course)), де CR – вид криптовалюти на продаж, C – курс продажу криптовалюти, Q – об'єм продажу, COM – величина комісійних, ST – стабільність криптовалюти, T – час проведення операції, REL – надійність виконання запиту, рівень довіри в тому, що запит точно буде оброблено і неможливість його відхилення, що також може призвести до втрати коштів через стрибки курсу, FC – наявність або відсутність фіксації курсу на час обробки запиту.

Під час роботи технологія використовує матрицю значень вхідних та вихідних змінних (табл. 1) та ізоморфну їй матрицю функцій належності, що в сукупності формує базу знань. Для заповнення матриці знань використовуються продукційні правила (6 – 8), які створюються із залученням експертів з біржової діяльності ринку криптовалют. Експертами задаються також первинні коефіцієнти *b* та *c* функцій належності – це буде етап «грубого» або структурного налаштування. Етап «тонкого» налаштування здійснюється автоматизовано у середовищах для моделювання систем на нечіткій логіці за методологіями та технологіями, описаними у [7]. Крім нечіткої бази знань технологія використовує також базу даних на продавців та ринкові характеристики криптовалют, яка у процесі експлуатації може поповнюватись та корегуватись. Так на основі інформації з бази даних формуються останні 4 показники, такі як ST (stability), T (time), REL (reliability), FC (fixation of the course).

Структуру технології наведено на рис. 5.

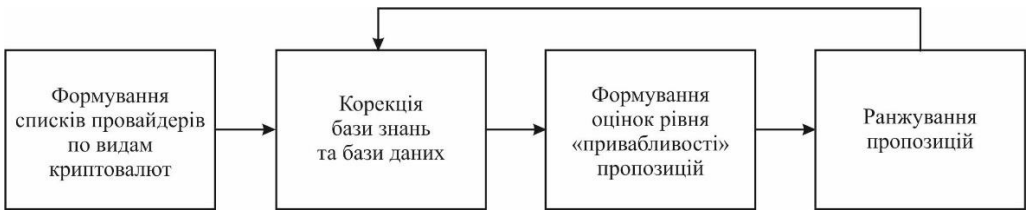

Рисунок 5 – Етапи роботи технології оцінювання привабливості пропозицій

Першим етапом роботи технології є формування списків провайдерів, що виступили з пропозиціями по певному виду криптовалюти LIST_CR1, LIST_CR2, … , LIST_CRN.

Другим етапом є формування функцій належності в залежності від конкретного списку провайдерів по певній криптовалюті.

Третій етап – нечітке логічне виведення результату оцінювання привабливості пропозиції провайдера

Четвертий етап – формування черг провайдерів (ранжування) для закупівлі криптовалют відповідно до рівня «привабливості» LIST_CR1_RAN, LIST_CR2_RAN, … , LIST_CRN_RAN .

Висновки

У результаті проведених досліджень покращено інформаційну технологію управління криптовалютними активами за рахунок розширення її функціоналу, а саме: уведення функцій оцінювання рівня «привабливості» пропозицій з продажу криптовалюти та ранжування пропозицій провайдерів, залежно від результатів оцінювання. Також розроблена інформаційна технологія, що їх реалізує.

Наукова новизна:

– покращено існуючу інформаційну технологію управління криптовалютними активами «криптовалютний гаманець»;

– уперше формалізована та змодельована засобами нечіткої логіки задача оцінювання привабливості пропозицій з продажу криптовалюти;

– на основі теорії нечітких множин розроблена нова інформаційна технологія оцінювання привабливості пропозицій з продажу криптовалюти.

Список літератури

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf. Accessed on: September 10, 2022.

[2] Christidis Konstantinos, Michael Devetsikiotis, *Blockchains and Smart Contracts for the Internet of Things*. [Online]. Available: http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408. Accessed on: September 10, 2022.
[3] Boohyung Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment", *The Journal of Supercomputing*, pp. 1-16. 2016.
[4] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems", arXiv preprint arXiv:1608.00695, 2016.
[5] Andreas M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. "O'Reilly Media, Inc.", 2014, 298 p.
[6] Л. Заде, *Понятие лингвистической переменной и ее применение к принятию приближенных решений*. М.: Мир, 1976, 167 с.
[7] О. П. Ротштейн, *Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі*. Вінниця: «УНІВЕРСУМ – Вінниця», 1999, 320 с.
[8] H. J. Zimmermann, *Fuzzy Sets, Decision Making and Expert Systems*. Kluwer: Dordrecht, 1987, 335p.
[9] О. М. Роїк, А. В. Поплавський, "Нечіткий підхід до вирішення задачі ідентифікації кольорових відтінків", *Оптико-електронні інформаційно-енергетичні технології*, № 2, с. 39-42. 2016.

Стаття надійшла: 20.05.2021.

References

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf. Accessed on: September 10, 2022.
[2] Christidis Konstantinos, Michael Devetsikiotis, *Blockchains and Smart Contracts for the Internet of Things*. [Online]. Available: http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408. Accessed on: September 10, 2022.
[3] Boohyung Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment", *The Journal of Supercomputing*, pp. 1-16. 2016.
[4] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems", arXiv preprint arXiv:1608.00695, 2016.
[5] Andreas M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. "O'Reilly Media, Inc.", 2014, 298 p.
[6] L. Zade, *Ponyatie lingvisticheskoy peremennoy i ee primenenie k prinyatiyu priblizhennyih resheniy*. M.: Mir, 1976, 167 s [in Russian].
[7] O. P. Rotshtein, *Intelektualni tekhnolohii identyfikatsii: nechitki mnozhyny, henetychni alhorytmy, neironni merezhi*. Vinnytsia: «UNIVERSUM – Vinnytsia», 1999, 320 p. [in Ukrainian].
[8] H. J. Zimmermann, *Fuzzy Sets, Decision Making and Expert Systems*. Kluwer: Dordrecht, 1987, 335p.
[9] O. M. Roik, A. V. Poplavskyi, "Nechitkyi pidkhid do vyrishennia zadachi identyfikatsii kolorovykh vidtinkiv", *Optoelectronic Information-Energy Technologies*, № 2, pp. 39-42. 2016 [in Ukrainian].

Відомості про авторів

Сілагін Олексій Віталійович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук.

Арсенюк Ігор Ростиславович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук.

Месюра Володимир Іванович – кандидат технічних наук, доцент, професор кафедри комп'ютерних наук.

Кукунін Сергій Сергійович – провідний програміст, Spotlight Media Labs, Inc.

O. V. Silagin, I. R. Arseniuk, V. I. Mesiura, S. S. Kukunin

DESIGNING OF THE SYSTEM OF DIGITAL CORRECTION AND BITMAP IMAGES IMPROVING QUALITY IN THE RADIOGRAPHY FIELD

Vinnytsia National Technical University, Vinnytsia