

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕОРІЯ КОДУВАННЯ

УДК 004.77+004.056

Л. М. Куперштейн, М. Д. Кренцін, А. В. Дудатьєв, В. А. Каплун

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ ПІРИНГОВИХ МЕРЕЖ

Вінницький національний технічний університет, Вінниця

Анотація. Проаналізовано базові поняття пірингових мереж. Вказано на актуальні напрямки їх використання, а саме файлообмінні сервіси, системи телеконференцій, ігрові та торговельні сервіси та ін. Розглянуто різновиди структурної організації та визначено їх переваги та недоліки. За ступенем централізації виділено чисту, гібридну та федеративну архітектури. Також подано класифікацію однорангових пірингових мереж за способом з'єднання та функціями. Аналіз поширеності пірингових мереж у сучасному світі довів затребуваність і актуальність використання децентралізованої мережевої технології, особливо у сфері фінансів. Проаналізовано можливі типи атак на пірингові мережі. Виділено атаки як загального характеру, так і специфічні. Специфічні атаки орієнтовані на користувача, додаток або мережу. Наведено способи та механізми захисту для кожної із досліджуваних типів атак. Результати аналізу систематизовано, а саме для кожної атаки визначено вплив на дані, ступінь небезпеки та рівень захисту. Також вказано на напрям порушення інформаційної безпеки кожної атаки, а саме цілісність, доступність, конфіденційність. Не менш цікавою вона виявилася і для зловмисників, про що свідчить значна кількість зламів. Дослідження атак на P2P мережі показало їх широкий спектр як загального характеру, так і спеціалізованих. При цьому атаки диференційовано за ступенем небезпеки та аспектом порушення рівня безпеки. Найбільш небезпечними виявилися атаки, що можуть призвести до порушення конфіденційності та цілісності даних. До них відносяться такі атаки: розподілена відмова в обслуговуванні, отруєння індексу, атака Сивілли, атака затемнення, ботнети, маскарад. Проведене дослідження є базою для подальшого дослідження недоліків захисту пірингових мереж та розробки нових безпечних механізмів обміну даними в децентралізованих структурах.

Ключові слова: пірингова мережа, центральний сервер, вузол, маршрутизація, аутентифікація, брандмауер.

Abstract. The basic concepts of peer-to-peer networks are analyzed. The current areas of their use are indicated, namely file-sharing services, teleconferencing systems, gaming and trade services, etc. The types of structural organization are considered, and their advantages and disadvantages are determined. According to the degree of centralization, pure, hybrid and federal architectures are distinguished. The classification of peer-to-peer peer networks by connection method and function is also given. Analysis of the prevalence of peer-to-peer networks in the modern world has proved the demand and relevance of the use of decentralized network technology, especially in the field of finance. Possible types of attacks on peer-to-peer networks are analyzed. Both general and specific attacks are highlighted. Specific attacks are oriented on user, application or network. Methods and mechanisms of protection for each of the studied types of attacks are given. The results of the analysis are systematized, namely for each attack the impact on the data, the degree of danger and the level of protection is determined. It also indicates the direction of violation of information security of each attack, namely the integrity, accessibility, confidentiality. It turned out to be no less interesting for malefactors, as evidenced by the significant number of hacks. The research of attacks on P2P networks showed a wide range of both general and specialized. At the same time, attacks are differentiated according to the degree of danger and the aspect of security breach. The most dangerous were attacks that could violate the confidentiality and integrity of data. These include the following attacks: distributed denial of service, index poisoning, sibyl attack, eclipse attack, botnets, masquerade. The research is the basis for further study of the shortcomings of the protection of peer-to-peer networks and the development of new secure mechanisms for data exchange in decentralized structures.

Key words: peer-to-peer network, central server, peer, routing, authentication, firewall.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-5-14>.

Вступ

Концепція однорангової або пірингової (peer-to-peer (P2P) мережі була вперше використана в 1969 р. В свою чергу P2P розглядається як мережевий протокол, що забезпечує можливість створення мережі однорангових вузлів та їх взаємодію [1]. У багатьох випадках мережі P2P використовують існуючі протоколи стеку TCP/IP для передачі, а саме TCP, UDP або їх обгортки. Першою реальною реалізацією однорангової мережі стала мережа Usenet (1979 р.) [2]. У цій мережі, хоча клієнти кінцевих користувачів все ще отримують доступ до ресурсів через сервери, самі сервери взаємодіють як мережа P2P і спілкуються один з одним без центральних повноважень. Це означає, що суть однорангової мережі полягає в тому, що мережа не має центрального керуючого вузла і всі її учасники рівні [3]. Проте незалежно від того, що стан кожного вузла однаковий, їх можливості можуть значно відрізнятися.

Після створення «Usenet» однорангові мережі почали стрімко розвиватись. Змінилось кілька поколінь мереж, поки вони не набули поточного стану. Їх використання не обмежується обміном файлами, як це було раніше. Найбільшого поширення P2P мережі набули в областях, де важливий обмін конфіденційними даними між людьми. Це системи відеозв'язку та відеомовлення (P2PTV), IP-телефонія та системи інтернет-телебачення, фінансовий сектор тощо [4].

Актуальність

Подібно до традиційного Інтернету P2P мережі відкриті до багатьох як загальних мережевих атак, так і специфічних. Це пов'язано з тим, що на відміну від клієнт-серверних застосунків, P2P вузли мають рівні права, а також відсутнє класичне управління правами доступу (як в централізованих системах). Найпоширенішими атаками на пірингові мережі є «відмова в обслуговуванні» (denial of service – DoS) та її розподілена модифікація (distributed denial of service - DDoS), «людина посередині» (man-in-the-middle – MITM), «поширення хробака» (worm propagation), «атака забруднення» (pollution attack), «отруєння індексу» (index poisoning), «раціональна атака» (rational attack), «атака затемнення» (eclipse attack), «атака

Сивілли» (Sybil attack) та ін. [5]. Всі ці атаки відрізняються складністю реалізації та технологіями захисту від них.

Із появою пірингової технології блокчейн та реалізації на її основі фінансових сервісів, у тому числі криптовалютних, зацікавленість ними зловмисників значно зросла. Останнім часом офіційно зафіксовано ряд «гучних» інцидентів. Так у березні 2022 року було зареєстровано крипто-злам, що був націлений на ігровий сервіс на основі мережі блокчейнів. При цьому хакери зламали мережу «Ronin Network» та незалежний і сумісний з Ethereum ланцюг блоків. В загальному втрати склали 625 млн. доларів США. [6]. Ще одним не менш масштабним зломом такого типу було у січні 2022 викрадення 80 млн. доларів США у DeFi-платформи Qubit Finance, що побудована на Binance Smart Chain (блокчейн, створений для криптовалюти BNB). Злам було проведено 2022 року. При цьому хакери використали вразливість мосту Qubit (децентралізованої платформи грошового обміну) [7].

Також у вересні 2021 року було зареєстровано DDoS атаки на провайдера VoIP.ms. Атака була спрямована на всю інфраструктуру телефонії, унеможливаючи здійснення дзвінків [8].

Виходячи з вищеприданого, доцільним та актуальним є аналіз та систематизація знань про загрози P2P системам, методів їх попередження та виявлення для оцінки їх потенціалу, а також вдосконалення та розробки нових перспективних превентивних механізмів.

Метою дослідження є аналіз проблем безпеки пірингових мереж та прикладних систем на їх основі для розробки класифікації потенційних загроз, що дозволить більш чітко спрямовувати вектори підходів до їх захисту, а також методики тестування на проникнення.

Загальна характеристика пірингових мереж

Пірингова мережа – це технологія, що реалізує об'єднання однорангових вузлів рівного статусу з собі подібними. Кожен вузол є і приймачем, і надавачем послуг. Такі вузли можуть обмінюватись інформацією безпосередньо. За ступенем централізації P2P мережі бувають трьох типів [9]:

- чиста, яка передбачає поєднання всіх вузлів один з одним. На сьогоднішній день повністю чисті пірингові мережі майже не використовуються. Представниками чистих P2P мереж є IPFS та Orbit-DB.

- гібридна, що використовує центральний сервер для того, щоб надати вузлу інформацію про адресу іншого вузла в мережі. Використовується в системах обміну файлами, що працюють з протоколом BitTorrent та мережах по доставці контенту (CDN).

- федеративна, суть якої полягає в тому, що мережа поділена на групи, в кожній з яких є головний. Всередині групи вузли поєднані один з одним, але в межах всієї мережі групи поєднані за допомогою головних вузлів. Використовується в деяких іграх та соціальних мережах (Ether, DarkCrystal) [10].

Однорангові мережі також розподіляються за способом з'єднання: структуровані та неструктуровані [11]. Структурована мережа P2P використовує єдиний алгоритм, який гарантує те, що будь-який вузол може ефективно передати запит іншому вузлу, який має шуканий файл (дані), навіть, якщо файл рідкісний. Неструктурована пірингова мережа передбачає довільне встановлення з'єднання. Такі мережі легко створюються, але їх недоліком є те, що запити не завжди оброблюються.

Мережі P2P диференціюються за базовим функціональним призначенням:

- Файлообмін. Найпоширеніша функція. Дуже актуальним є для передачі великих файлів при невеликій пропускній здатності мережі. Прикладами таких програм є uTorrent, BitTorrent, FrostWire та ін. [12].

- Співпраця. Це може бути наприклад обмін повідомленнями, онлайн ігри, сумісна робота над документами. Прикладами таких систем є CASA, GENI, P2P cloud [13].

- Розподілені обчислення. Обчислювальна проблема розподіляється на невеликі незалежні частини. Прикладом такої системи є SETI@Home [14].

Класифікація атак на пірингові мережі

В загальному атаки на пірингові мережі поділяються на дві великі категорії: активні та пасивні [15]. Активну атаку можна визначити як таку, що спрямована на один або декілька вузлів P2P мережі. Основний мотив активної атаки – викликати пошкодження вузлів. Пасивні атаки спрямовані виключно на саму мережу, а не на її вузол. Основний мотив пасивної атаки – це порушення доступності, щоб учасники були обмежені у використанні конкретних послуг. На сьогодні відомо ряд поширених атак та загальні способи захисту від них [16]. Проте в залежності від прикладного застосування технології P2P як механізм атак так і методи захисту можуть суттєво відрізнятися.

1. Атака «Відмова в обслуговуванні» (Denial of service, DoS) – це атака на комп'ютер або мережу, що робить неможливим подальше використання сервісів мережі. Існує два способи виконати таку атаку: наповнювати мережу фіктивними пакетами (при цьому цільова доставка істинного трафіку ускладнюється) або ж змусити вузли працювати над складними (вибагливими по ресурсам) обчисленнями, аби у вузла не було змоги відповісти на інші запити, що надходять [17].

Захист: Для того, щоб захистити мережу від такої атаки використовують так зване «ціноутворення». Оскільки неможливо відрізнити справжні важкі обчислення, що можуть виконуватись вузлом, від фіктив-

вних, тому неможливо вчасно виявити і запобігти атаці. Тому вузол, що надає послугу, повинен надавати своїм клієнтам так звані «головоломки», адже лише у випадку її вирішення клієнту можна довіряти та відповідати на запит. Проте недоліком цього методу є те, що деякі справжні клієнти (наприклад мобільні пристрої) можуть швидше розряджатись, вирішуючи ці «головоломки». Також можна блокувати вразливі порти, на які можуть здійснюватися атаки. Ще одним способом є додавання спеціальних правил до брандмауера та використання спеціалізованих маршрутизаторів [18].

2. Коли в атаці залучено кілька хостів, тоді вона називається «розподілена відмова в обслуговуванні» (Distributed denial of service, DDoS). В цьому випадку атакуючі комп'ютери часто є персональними комп'ютерами з широкосмисловою мережею з'єднання, що були зламані вірусом або трояном. Злочинець при цьому може дистанційно керувати цими машинами (їх називають зомбі) і спрямувати атаку на будь-який хост чи мережу.

Захист: Існує три кроки, щоб запобігти DDoS-атакам: Спочатку необхідно пропускати інтернет-трафік через брокерську компанію, що допоможе клієнтам відфільтрувати серію шкідливої інформації. По-друге, необхідно використовувати моніторинг взаємодії вузлів для виявлення DDoS атак. Також у брокерів можуть бути свій власний чорний та/або білий список, які дозволяють брокерам припинити роботу трафіку у чорному списку до того, як він потрапив до кінцевого користувача, при цьому брокери завжди дозволяють трафік із білого списку [19].

3. Атака «Людина посередині» (Man-in-the-middle) – це атака, коли зловмисник непомітно вставляється між двома вузлами та керує їхньою комунікацією. Це може бути зміна, видалення чи вставка повідомлень. У багатьох випадках – це розсилання неправдивої інформації. Така атака є досить серйозною для більшості протоколів, особливо, коли є форма аутентифікації [20].

Захист: В прінгових мережах неможливо виявити атаку «Людина посередині», адже вони не мають центрального серверу, що здатен перевіряти та контролювати трафік. Проте для запобігання майбутніх атак слід використовувати шифрування інформації, що передається. Також необхідно по можливості використовувати методи аутентифікації для перевірки автентичності та валідності користувача.

4. Атака «Поширення хробака» (Worm propagation) полягає в тому, що хробак передає свої копії від одного вузла до іншого через мережеве підключення і працює окремо. Хробак може поширюватися через файли, електронну пошту, веб-сервер тощо. Існує ряд факторів, які дозволяють мережам P2P стати вразливими для такого роду атак [21]:

- Мережі P2P складаються із комп'ютерів, на яких виконуються однакові програми. Таким чином атакуючий може з першого дня зібрати всі вузли, які зможуть скомпрометувати всю мережу, знайшовши одне слабе місце в мережі.

- Вузли P2P, як правило, з'єднуються з багатьма іншими вузлами. Тому хробак не буде втрачати час на сканування інших жертв, а просто отримує список сусідніх вузлів та поширюється ними.

- P2P-програми також використовуються для передачі великих файлів. Деякі хробаки мають обмежувати їхній розмір, щоб передаватись одним TCP-пакетом. Це може призвести до реалізації більш складних атак.

- Програми P2P часто доступні на комп'ютерах співробітників замість серверів. Таким чином, зловмиснику легше отримати доступ до важливих даних (паролі, номери карток тощо).

- Користувачі P2P часто передають незаконний вміст (наприклад, захищена авторським правом музика), і вони схильні не повідомляти про незвичайну поведінку мережі.

Як тільки «хробаки» закінчують розмножуватися, їх метою зазвичай є запуск масової DDoS атаки в політичних або комерційних цілях.

Захист: Одним із методів захисту є використання брандмауера. У більшості випадків «хробак» сканує певний порт у комп'ютера для зараження, а брандмауери можуть заблокувати порт, який потребує хробак. Крім того, слід використовувати антивірусне програмне забезпечення, щоб захистити комп'ютери. До складу антивірусного програмного забезпечення входить сигнатура вірусу, якщо деякі атрибути файлу відповідають атрибутам в сигнатурі вірусу, антивірусне програмне забезпечення може видалити або ізолювати цей файл. Антивірусне програмне забезпечення може бути також вбудованим в операційну систему.

5. Атака «Забруднення» (Pollution attack) полягає в заміні файлу в мережі помилковим, і цей забруднений файл стає непридатним. Зловмисник створює цільовий вміст непридатним для використання шляхом зміни вмісту або його частини на інший незалежно від вмісту, а потім робить цей вміст доступним для обміну [22]. Щоб залучити людей до завантаження забрудненого файлу, його потрібно замаскувати як корисний вміст, наприклад, мати той самий формат і аналогічний розмір. Він також повинен підтримувати високу пропускну здатність з'єднання.

Захист: З боку користувача завантажений файл, який був забруднений, є нешкідливим для інших комп'ютерів, але він просто витрачає зайву пам'ять. Тому, як тільки користувач дізнається, що завантажені файли є забрудненими, він повинен видалити їх із системи P2P.

6. Рациональні атаки (Rational attacks). Щоб P2P-послуги були ефективними, вузли-учасники повинні співпрацювати, але в більшості сценаріїв вузол представляє зацікавлену сторону, і співпраця неможлива. Розумним припущенням є те, що велика частка P2P-вузлів є раціональними і намагатимуться максимізувати споживання системних ресурсів при мінімізації використання власних. Наприклад, вузли можуть зрозуміти, що, не надавши спільного доступу, вони заощаджують пропускну здатність для завантаження необхідних їм даних [26]. Якщо велика кількість вузлів є такими, що відмовляються від внесків (тобто лише хочуть отримувати дані і нічого не віддавати іншим вузлам), система може дестабілізуватися. У цьому випадку, якщо достатньо вузлів, що зацікавляться, система не може гарантувати належний рівень завантажень і вивантаження даних.

Захистом від такої атаки є алгоритм, що може гарантувати розумний рівень взаємності завантаження та вивантаження. Якщо вузли просто завантажують і ніколи не вивантажують, вони повинні бути «оштрафовані».

7. Атака «Сивілли» (Sybil attack). У багатьох пірингових системах передбачено надлишкове резервне копіювання, що є механізмом захисту цілісності та конфіденційності. P2P система повинна переконатися, що кожен ідентифікатор мережевого об'єкта вказує лише одну сутність. Якщо сутність діє як декілька множинних об'єктів, то зловмисник може контролювати частину мережі. Такий напад визначається як атака «Сивілли». Вона знищить резервне копіювання в одноранговій мережі P2P. Наприклад, коли звичайний вузол А робить резервне копіювання, він вибирає групу вузлів, таких як В, С, D, Е, що мають різні ідентифікатори. Але насправді вузли С, D та Е не існують, оскільки вони є шкідливими вузлами, створеними зловмисником, тому резервне копіювання не може завершитися, а система перестає нормально працювати.

Захист: Для того, щоб захиститись від атаки «Сивілли» необхідно використовувати метод самореєстрації [22, 27]. Це може бути включення IP-адреси вузла до його ідентифікатора. Таким чином, зловмисний вузол не зможе підробити справжні вузли, оскільки він буде прив'язаний до обмеженої кількості IP-адрес, і його можна помітити, якщо він створить більше сутностей. Але це рішення далеко не просте, оскільки, наприклад, можна генерувати підроблені ідентифікатори для інших вузлів, а потім система буде їх бачити як зловмисні. Ще одним способом захисту є використання складного протоколу на основі публічно-приватного ключа. Кожен вузол повинен підписувати своє повідомлення та час від часу відповідати на запити з боку якогось центрального вузла (проте це дає інші слабкі місця).

8. Атака «Затемнення» (Eclipse attack) передбачає виконання певних підготовчих дій. Спочатку зловмисник повинен отримати контроль над певною кількістю вузлів уздовж стратегічних маршрутів. Після цього атакуючий може розділити мережу на різні підмережі. Таким чином, якщо вузол хоче спілкуватися з вузлом з іншої підмережі, його повідомлення має у певний момент бути маршрутизованим через один із вузлів зловмисника. Зловмисник таким чином «затемнює» кожен підмережу іншою. У певному сенсі, атаки затемнення є розширеним варіантом атаки «Людина посередині», а також може бути продовженням атаки «Сивілли». В цьому випадку, зловмисник намагатиметься розмістити свої вузли на стратегічних маршрутах. Зловмисник може повністю контролювати підмережу з іншого боку підмережі [22]. Якщо зловмиснику вдається атака Eclipse, він може атакувати мережу набагато ефективніше:

- неефективно перенаправляти кожне повідомлення вузлу, якому воно не призначене;
- ігнорувати всі вхідні повідомлення, таким чином повністю відокремлюючи обидві підмережі;
- використовувати атаку «Забруднення» для того, щоб засмітити обидві підмережі, зробивши їх непридатними для подальшої взаємодії.

Захист. На відміну від атак «Людина посередині», дуже ретельно підібрані криптографічні протоколи можуть стати гарною спробою зупинити таку атаку. Ціноутворення також може допомогти проти версії з використанням атаки Sybil. Проблема таких рішень полягає в тому, що вони створюють серйозне уповільнення та перешкоджають нормальній масштабованості мережі. Основним захистом від атак «Затемнення» є використання чистої пірингової мережі [27]. Ще кращим рішенням було б додатково використовувати алгоритм рандомізації для визначення розташування вузлів. Якщо вузли в чистій P2P мережі розподілені випадковим чином, нападник не може контролювати позиції своїх вузлів. Тому було б майже неможливо відокремити дві підмережі одна від одної.

9. Атака «Отруєння індексу» (Index poisoning attack). Багато сучасних систем P2P мають індекси, що дозволяють користувачам знайти місця розташування бажаного контенту. Атака «Отруєння індексу» спрямована на процес індексного запиту користувачів і ускладнює пошук правильного вмісту в мережі P2P. Зловмисники просто вставляють велику кількість недійсних індексів в загальну таблицю, щоб завадити користувачам знайти правильний ресурс.

Захист: є два заходи захисту від атаки «Index poisoning». Перший з них – це аутентифікація версій і рекламні оголошення [23]. Як і деякі рейтингові веб-сайти та форуми, вміст повинен бути промодерований. Другий метод – рейтинг джерел. Якщо ці вузли є джерелами даних високого попиту, які надають і завантажують файли, то вони мають високий рейтинг. Якщо це джерела «сміттєвих» даних, що забруднюють систему, то відповідні однорангові вузли будуть у чорному списку.

10. Ботнети (Botnets). Однією з найбільш значущих загроз для Інтернету сьогодні є загроза ботнетів, які є скомпрометованими мережами під контролем зловмисника (мережа керується автономною програмою, що приховано встановлюється на комп'ютери-жертви та маскується під системний процес чи користувача ПЗ). Ботнет створює значні загрози для структурованих P2P мереж [24]. Порівняно з іншими шкідливими програмами в Інтернеті, ботнети відрізняються від традиційних атак в тому, що вони діють як скоординована атакуюча група. Машини, які часто беруть участь у ботнеті мають віруси, хробаки та трояни.

Захист: сьогодні існує ряд спеціальних методів виявлення та зупинки ботнетів (наприклад, розділення вузлів і проектування наборів тестів Тюрінга або головоломок, які користувачі повинні розгадати, щоб отримати доступ до перевантажених ресурсів).

11. Атака підслуховування (Eavesdropping attack) – це ще один вид атаки на мережі. Зловмисники можуть отримати доступ до даних у мережі та прослуховувати трафік. Одна з найбільших проблем безпеки, з якою стикаються користувачі, це здатність зловмисників моніторити мережі, а саме визначати паролі та ключі, отримати MAC-адресу, отримати IP-адресу, і в результаті, призвести до збою мережі [26]. У таких атаках можуть застосовуватись засоби прослуховування (для того, щоб почути чиїсь паролі для входу), моніторингу через камери відеонагляду (для того, щоб побачити паролі для входу) тощо.

Захист: першим кроком у запобіганні атаці підслуховування є використання міцної фізичної безпеки, а наступний крок – використання шифрування будь-якої важливої інформації.

12. Маскарадна атака – це тип атаки, в якій юридична особа нелегітимно представляє собою іншу сутність, яка має доступ до конфіденційної інформації чи системи. Маскарадні атаки надзвичайно серйозні. Вони можуть відбуватися різними способами. Зловмисники можуть отримати доступ до облікового запису законного користувача через викрадення пароля, обхід процесу авторизації або через IP-адресу. Якщо процес авторизації не повністю захищений, він може стати надзвичайно вразливим для маскарадної атаки [26].

Захист: поширеним методом обмеження цього типу атаки є фільтрація вхідних пакетів, які надходять із внутрішньої IP-адреси та фільтрація вихідних пакетів, які виходять з недійсної локальної IP-адреси.

13. Неправильне оновлення маршруту. Зловмисник може пошкодити таблиці маршрутизації, надсилаючи іншим вузлам недійсні дані або ж спрямовувати запити до невідповідних або до неіснуючих вузлів.

Захист: для запобігання такій атаці необхідно виконувати певні умови, наприклад, враховувати час обміну в обидва боки, щоб віддати перевагу найкоротшому шляху. Або ж, наприклад, у таблицях має передувати правильний префікс, який не може бути відтворений шкідливими вузлами [25].

14. Неправильний пошук маршруту. Пошук ключів у структурованих мережах P2P виконується шляхом маршрутизації запитів через серію вузлів. Кожен з цих вузлів використовує локальну таблицю маршрутизації для пересилання запиту до вузла, відповідального за ключ. Цей механізм використовується для зберігання, отримання, тиражування та аутентифікації даних. Оскільки шкідливий вузол може пошкодити цей механізм через систему оновлення маршрутизації, він може пересилати повідомлення неправильному або неіснуючому вузлу (таким чином не надавши правильному вузлу інформацію) [11].

Захист: запобігти такій атаці можна двома способами. По-перше, запитувач повинен переконатися, що кінцевий вузол підтверджує те, що він є правильною точкою завершення запиту. По-друге, система повинна призначити ключі вузлам у верифікований спосіб.

15. Атака «Викрадення сутності». Така атака спрямована на мережі, де вузол знає лише про деяку частину сусідніх вузлів, а інформацію необхідно надіслати до незнайомого вузла (таким чином вузол довіряє іншим у правильній маршрутизації даних). Однак зловмисник може використовувати цю довіру, щоб почати атаку на крадіжку особистих даних. Коли шкідливий вузол на шляху повідомлення стверджує, що це бажаний вузол призначення, то він може захопити маршрут і, наприклад, знищити чи перенаправити дані.

Захист: запропоновано метод, у якому використовуються докази, чорні списки та зловмисну маршрутизацію, і було показано, що він ефективно виявляє, позначає та перенаправляє трафік від зловмисника. Метод полягає в тому, що вузли підписують сертифікати доказу життя для часткових ідентифікаторів вузлів і розповсюджують їх випадково вибраним менеджерам доказів у мережі. Вихідні вузли можуть уникати зловмисників, запитуючи докази у кількох менеджерів доказів [26].

16. Атака відтоку. Ця атака спрямована на структуровані пірингові мережі. Ця характеристика робить таку систему привабливою для великої кількості користувачів і водночас уразливою до явищ відтоку [11]. Суть атаки полягає в тому, що до мережі підключається та відключається одночасно велика кількість вузлів, що створює ефект, який називається відтоком. Зловмисник може використати цю атаку, щоб досить швидко зіпсувати найкращу функцію мережі.

Захист: мережі P2P мають бути спроектовані так, щоб легко масштабуватись та витримувати сплеск навантаження.

17. Співставлення ідентифікаторів. У структурованих пірингових мережах є випадковий розподіл ідентифікаторів вузлів. Це випадкове розподілення дозволяє зловмиснику отримати певну інформацію про ідентифікатор і отримати контроль над певними ресурсами. Ця атака тісно пов'язана з атакою Сивілли. Але основна відмінність полягає в тому що атака Сивілли використовується для створення великої кількості випадкових ідентифікаторів, у той час як ця атака спрямована на отримання деяких конкретних.

Захист: найкраще рішення, щоб уникнути атаки співставлення ідентифікатора – це використовувати централізований орган, який розповсюджує ідентифікатори, але це непрактично, оскільки мережі P2P є масштабованими та децентралізованими. Тому захиститись від такої атаки можна лише якщо ідентифікатор залежить від деякої інформації за межами керування вузлом [27]. Наприклад, змусити вузол отримати свій ідентифікатор з IP-адреси, номера порту якоїсь хеш-функції.

18. Атака зберігання та отримання тісно пов'язана з раціональною атакою, оскільки зловмисники відмовляються надавати послуги іншим вузлам або заперечують існування даних. Ця атака може бути небезпечною в системі, яка не призначає вузлам ідентифікатори, які можна верифікувати. У такій системі вузол може взяти на себе відповідальність за дані, які він бажає сховати чи відмовитись надавати [11].

Захист: щоб запобігти цій атаці, система повинна забезпечити реплікацію. Реплікація має бути оброблена таким чином, щоб кілька вузлів відповідали за реплікацію.

19. Атака «Переповнення запитів». Структурована P2P мережа складається з великої кількості вузлів, які не підключені до всіх інших вузлів. Якщо вузол виконує запит до сусідніх вузлів на отримання даних, а ті, в свою чергу, не маючи її, роблять запити своїм сусіднім вузлам, то мережа породжує дуже багато запитів. Таким чином зловмисник може генерувати подібні запити у великій кількості, перешкоджаючи при цьому основному трафіку всередині мережі [28].

Захист: обмежувати кількість вхідних запитів від одного вузла за одиницю часу.

20. Атака «Порушення анонімності». У контексті структурованих мереж P2P, кожен вузол має таблицю маршрутизації, що містить набір відповідних однорангових вузлів відносно певного ключа. Таким чином запит надходить від одного вузла до іншого через проміжні вузли. А це в свою чергу виключає повну анонімність. Зловмисник може контролювати всю інформацію, що проходить через нього, щоб отримати знання інших про інші вузли, які його оточують. У цьому випадку, зловмисник може взяти більшість файлів, запити про які проходять через нього [26].

Захист: проблема анонімності зводиться до захисту ідентифікаторів вузлів, що запитують дані та вузла, що надає інформацію про ключ доступу до іншого вузла.

21. Атака «Порушення конфіденційності». Сьогодні P2P-мережі стають все більшими популярними, адже вони призначені для спільного використання ресурсів і надання послуг. Проблема конфіденційності полягає в тому, що користувачі можуть випадково або несвідомо дозволити їх приватні або особисті файли, до яких буде відкрито доступ. У цій ситуації вони ризикують розкрити свою приватну інформацію іншим користувачам мережі.

Захист: користувач повинен бути уважним при наданні доступу до файлів.

Зведену характеристику атак та методів захисту від них наведено у таблиці 1.

Таблиця 1 – Характеристика атак на P2P мережі та методів захисту від них

№	Назва атаки	Поведінка	Що порушує	Стратегії захисту	Ступінь небезпеки	Рівень захисту
1	Відмова в обслуговуванні	1. Закидання в мережу підібраних пакетів. 2. Завантаження вузла вибагливим обчисленням	Доступність	Ціноутворення, брендмауер, спеціалізовані маршрутизатори	Середній	Легкий
2	Розподілена відмова в обслуговуванні	Хакер контролює контрольних зомбі, а через тих «зомбі» відбувається контроль атакуючих «зомбі»	Доступність	Через надійний сервер, забезпечити систему оповіщення. Створити чорний і білий списки для довірених відвідувань	Високий	Важкий
3	Людина посередині	Зловмисник вставляє себе непомітно між двома вузлами та перехоплює, змінює та надсилає дані між цими двома вузлами	Цілісність, доступність, конфіденційність	Механізм шифрування і технологія аутентифікації	Середній	Середній
4	Розповсюдження хробака	Передає свої копії від одного вузла до інших автоматично	Цілісність, доступність, конфіденційність	Брандмауер, антивірус, безпечна операційна система	Середній	Середній
5	Атака забруднення	Поділиться файлом, який не використовується	Цілісність, доступність	Забрати такий файл	Низький	Легкий
6	Раціональна атака	Лише завантажувати дані і ніколи не вивантажувати інші	Доступність	Штрафна система	Середній	Середній

Продовження таблиці 1

7	Отруєння індексу	Змінюється індексація інформації, щоб вузлу було важко знайти правильний зміст	Доступність	Аутифікація версій і реклама, рейтинг джерела	Високий	Середній
8	Атака Сивілли	Контролює кількість сутностей	Цілісність, конфіденційність	Алгоритм саморесстрації	Високий	Важкий
9	Атака затемнення	Шкідливі вузли працюють разом, щоб обдурити добрі вузли	Цілісність, доступність	Indegree і Outdegree методи	Високий	Важкий
10	Ботнети	Зараження комп'ютерів автономною програмою, що використовує ресурси на свій лад	Цілісність, доступність, конфіденційність	Розділення вузлів та тести Тьюринга	Високий	Важкий
11	Атака підслуховування	Викрадення конфіденційної інформації за допомогою засобів «підслуховування»	Цілісність, конфіденційність	Фізичні методи захисту та шифрування даних	Середній	Середній
12	Маскарад	Одна особа видає себе за іншу, що має доступ до даних	Цілісність, конфіденційність	Фільтрація вхідних та вихідних пакетів даних	Високий	Середній
13	Неправильне оновлення маршруту	Пошкодження таблиць маршрутизації	Доступність	Префікси у таблицях індексації, найкоротший шлях обміну даними	Низький	Легкий
14	Неправильний пошук маршруту	Пересилання таблиць маршрутизації неправильним вузлам	Доступність	Призначення ключів у верифікований спосіб та взаємопідтвердження при запитках	Низький	Легкий
15	Викрадення Сутності	Шкідливий вузол перехоплює маршрут та видає себе за кінцевий, якому належить інформація	Цілісність, конфіденційність	Докази, чорні списки, зловмисна маршрутизація	Середній	Середній
16	Атака відтоку	Одночасне підключення та відключення великої кількості вузлів	Доступність	Правильне проектування мережі	Низький	Легкий
17	Співставлення ідентифікаторів	Визначення ідентифікатора вузла для контролю його ресурсів	Цілісність, доступність, конфіденційність	Залежність ідентифікатора вузла від зовнішніх для вузла даних	Середній	Середній
18	Атака зберігання та отримання	Перехоплення ідентифікатора вузла та відмова у наданні даних	Цілісність, доступність, конфіденційність	Реплікація даних	Середній	Легкий
19	Переповнення запитів	Надсилання запитів про пошук інформації у великій кількості	Доступність	Обмеження кількості вхідних запитів від вузла	Середній	Легкий
20	Порушення анонімності	Отримання проміжної інформації про запити та місцезнаходження даних через проміжні вузли	Конфіденційність	Захист ідентифікаторів вузлів різними методами	Низький	Середній
21	Порушення конфіденційності	Випадкове надання користувачем доступу до конфіденційної інформації	Конфіденційність	Уважність користувача при роботі з системою	Низький	Легкий

Також, коли йдеться про безпеку, людський фактор завжди має враховуватися. Зростання клієнтів різноманітних пірингових мереж відбулось завдяки простоті установки та використання, невисокій вартості та перспективного результату. Початківці та не лише не відчувають великих труднощів з використанням таких додатків щоб завантажити файли. Проте ці файли можуть бути «забрудненими» тощо. Ще одна проблема безпеки, яку створюють додатки P2P – це те, що людина помилково може почати вивантажувати в систему купу непотрібних файлів окрім запитуваного, а це, в свою чергу, спричиняє непотрібне нагромадження даних в системі. Також користувач може бути вразливим місцем для зловмисника, через що той може отримати доступ до мережі для спричинення інших видів атак. Тому, враховуючи вищеприписані проблеми, необхідно бути уважним при розробці та використанні P2P системою.

Висновки

Аналіз поширеності пірінгових мереж у сучасному світі довів затребуваність і актуальність використання децентралізованої мережевої технології, особливо у сфері фінансів. Не менш цікавою вона виявилася і для зловмисників, про що свідчить значна кількість зламів. Дослідження атак на P2P мережі показало їх широкий спектр як загального характеру, так і спеціалізованих. При цьому атаки диференційовано за ступенем небезпеки та аспектом порушення рівня безпеки. Найбільш небезпечними виявилися атаки, що можуть призвести до порушення конфіденційності, цілісності та доступності (атаки «людина по середині», «хробаки», «ботнет» та ін.). Не дивлячись на ряд механізмів захисту від потенційних загроз залишається актуальною атака нульового дня. Тому завжди актуальним буде розробка нових та вдосконалення існуючих методів захисту пірінгових сервісів. Отримані результати дослідження ляжуть в основу розробки класифікації загроз P2P мереж.

Список літератури

- [1] J. Buford, H. Yu, E. K. Lua, *P2P Networking and Applications*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008, p. 408.
- [2] The Social Forces Behind the Development of Usenet By Michael Hauben. [Online]. Available: <http://www.columbia.edu/~hauben/book/ch106.x03>. Accessed on: January 20, 2022.
- [3] P2P Networking. [Online]. Available: <https://nakamoto.com/p2p-networking/>. Accessed on: January 20, 2022.
- [4] Peer-To-Peer VOiP. [Online]. Available: <https://www.tmcnet.com/voip/0907/feature-articles-peer-to-peer-voip.htm>. Accessed on: January 20, 2022.
- [5] All.Net [Online]. Available: <http://all.net/>. Accessed on: February 10, 2022.
- [6] Axie Infinity's Ronin network suffers hack and theft of over \$600 million – CNN. [Online]. Available: <https://edition.cnn.com/2022/03/29/tech/axie-infinity-ronin-hack/index.html>. Accessed on: January 22, 2022.
- [7] Hackers Steal Cryptocurrency Worth \$80 Million From Decentralised Finance Platform Qubit Finance [Online]. Available: <https://www.ndtv.com/business/cryptocurrency-worth-80-million-stolen-from-defi-platform-qubit-finance-2737888>. Accessed on: Jan. 22, 2022.
- [8] HackRead | Latest Cyber Crime – InfoSec-Tech – Hacking News. [Online]. Available: <https://www.hackread.com/canadian-voip-ms-hit-by-extortion-ddos-attacks/>. Accessed on: April 10, 2022.
- [9] Л. М. Куперштейн, М. Д. Кренцін, “Аналіз тенденцій розвитку пірінгових мереж”, *Вісник Хмельницького національного університету*, № 4, с. 25-29, 2021.
- [10] Decentralized Social Networks. Comparing federated and peer-to-peer... | by Jay Graber | Stories from the Decentralized Web | Medium. [Online]. Available: <https://medium.com/decentralized-web/decentralized-social-networks-e5a7a2603f53>. Accessed on: December 15, 2021.
- [11] A. Cabani, S. Ramaswamy, M. Itmi, S. Al-Shukri, J. Pécuchet. “Distributed Computing Systems: P2P versus Grid Computing Alternatives” in *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering*. Springer, Dordrecht, 2007, pp. 47-52. doi: 10.1007/978-1-4020-6268-1_9.
- [12] Best 10 Peer to Peer (P2P) File Sharing Programs and Applications XtendedView. [Online] Available: <https://xtendedview.com/internet/best-p2p-file-sharing-programs/5684/>. Accessed on: December 25, 2021.
- [13] H.M.N.D. Bandara, A. P. Jayasumana, “Collaborative applications over peer-to-peer systems—challenges and solutions”. *Peer-to-Peer Netw. Appl*, № 6, pp. 257–276, 2013. doi: 10.1007/s12083-012-0157-3.
- [14] SETI@home. [Online]. Available: <http://setiathome.ssl.berkeley.edu/>. Accessed on: April 4, 2022.
- [15] Md. Sadek Ferdous, Farida Chowdhury, Md. Moniruzzaman. “A Taxonomy of Attack Methods on Peer-to-Peer Network” in *Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security*, India, 2007, pp. 132-138.
- [16] Roger Wattenhofer. “Attacks on Peer-to-Peer Networks” in Semester Thesis of Swiss Federal Institute of Technology, 2005, Zurich, pp.1-36.
- [17] O. P. Voitovych, Y. V. Baryshev, L. M. Kupershtein, E. I. Kolibabchuk, “Investigation of Simple Denial-of-Service Attacks”, *Third International IEEE Conference “Problems of Infocommunications. Science and Technology”*, 2016, Kharkiv, Ukraine, pp. 1-4.
- [18] L. Kupershtein, T. Martyniuk, O. Voitovych, B. Kulchytskyi, A. Kozhemiako et al. “DDoS-attack detection using artificial neural networks in Matlab,” *Proc.SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-EnergyPhysics Experiments*, 2019. doi: 10.1117/12.2536478.

- [19] Н. В. Багнюк, В. М. Мельник, О. В. Клеха, І. А. Невідомський, “Види DDoS-атак та алгоритм виявлення DDoS-атак типу flood-attack”, *Комп’ютерно-інтегровані технології: освіта, наука, виробництво*, № 18, 2015, с. 6-12.
- [20] Elakrat Mohamed Abdallah, Jung, Jae Cheon, “Development of field programmable gate array-based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication net-work”, *Nuclear Engineering and Technology*, no. 50, pp. 780–787, June 2018. doi:10.1016/j.net.2018.01.018.
- [21] X. Fan, and Y. Xiang, “Propagation Modeling of Peer-to-Peer Worms”, in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Central Queensland University, Rockhampton, Australia, 2010, pp. 1128-1135.
- [22] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 6th ed. Prentice Hall, Upper Saddle River, NJ, 2013, 752 pp.
- [23] J. Liang, N. Naoumov, and K.W. Ross, “The Index Poisoning Attack in P2P File Sharing Systems” in *25th IEEE International Conference on Computer Communications. Polytechnic Univerisy*, Brooklyn, NY, 2006, pp. 1-12.
- [24] C. Schiller, J. Binkley, D. Harley, G. Evron, T. Bradley, C. Willems, M. Cross, “Botnets – The Killer Web App”, Syngress, Rockland, 2007, 482pp. ISBN-10: 1-59749-135-7.
- [25] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, D. Wallach, “Secure routing for structured peer-to-peer overlay networks”, *SIGOPS Oper. Syst. Rev.*, vol. 36, December 2003, pp. 299-314. doi:10.1145/844128.844156.
- [26] D. Stutzbach, R. Rejaie, “Understanding churn in peer-to-peer networks” in *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, New York, 2006, pp. 189-202.
- [27] A. Vasudeva, M. Sood, “Survey on sybil attack defense mechanisms in wireless ad hoc networks”, *Journal of Network and Computer Applications*, vol. 120, pp. 78-118, 2018. doi: 10.1016/j.jnca.2018.07.006.
- [28] W. Ai, L. Xinsong and L. Kejian, “Efficient flooding in peer-to-peer networks,” *2006 7th International Conference on Computer-Aided Industrial Design and Conceptual Design*, 2006, pp. 1-6, doi: 10.1109/CAIDCD.2006.329410.

Стаття надійшла: 04.05.2022.

References

- [1] J. Buford, H. Yu, E. K. Lua, *P2P Networking and Applications*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008, p. 408.
- [2] The Social Forces Behind the Development of Usenet By Michael Hauben. [Online]. Available: <http://www.columbia.edu/~hauben/book/ch106.x03>. Accessed on: January 20, 2022.
- [3] P2P Networking. [Online]. Available: <https://nakamoto.com/p2p-networking/>. Accessed on: January 20, 2022.
- [4] Peer-To-Peer VOiP. [Online]. Available: <https://www.tmcnet.com/voip/0907/feature-articles-peer-to-peer-voip.htm>. Accessed on: January 20, 2022.
- [5] All.Net [Online]. Available: <http://all.net/>. Accessed on: February 10, 2022.
- [6] Axie Infinity's Ronin network suffers hack and theft of over \$600 million – CNN. [Online]. Available: <https://edition.cnn.com/2022/03/29/tech/axie-infinity-ronin-hack/index.html>. Accessed on: January 22, 2022.
- [7] Hackers Steal Cryptocurrency Worth \$80 Million From Decentralised Finance Platform Qubit Finance [Online]. Available: <https://www.ndtv.com/business/cryptocurrency-worth-80-million-stolen-from-defi-platform-qubit-finance-2737888>. Accessed on: Jan. 22, 2022.
- [8] HackRead | Latest Cyber Crime – InfoSec- Tech – Hacking News. [Online]. Available: <https://www.hackread.com/canadian-voip-ms-hit-by-extortion-ddos-attacks/>. Accessed on: April 10, 2022.
- [9] L. M. Kupershtein, M. D. Krentsin, “Analiz tendentsii rozvytku pirynhovoykh merezh”, *Visnyk Khmelnytskoho natsionalnoho universytetu*, № 4, pp. 25-29, 2021 [in Ukrainian].
- [10] Decentralized Social Networks. Comparing federated and peer-to-peer... | by Jay Graber | Stories from the Decentralized Web | Medium. [Online]. Available: <https://medium.com/decentralized-web/decentralized-social-networks-e5a7a2603f53>. Accessed on: December 15, 2021.
- [11] A. Cabani, S. Ramaswamy, M. Itmi, S. Al-Shukri, J. Pécuchet, “Distributed Computing Systems: P2P versus Grid Computing Alternatives” in *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering*. Springer, Dordrecht, 2007, pp. 47-52. doi: 10.1007/978-1-4020-6268-1_9.
- [12] Best 10 Peer to Peer (P2P) File Sharing Programs and Applications XtendedView. [Online] Available: <https://xtendedview.com/internet/best-p2p-file-sharing-programs/5684/>. Accessed on: December 25, 2021.

- [13] H.M.N.D. Bandara, A. P. Jayasumana, "Collaborative applications over peer-to-peer systems—challenges and solutions". *Peer-to-Peer Netw. Appl*, № 6, pp. 257–276, 2013. doi: 10.1007/s12083-012-0157-3.
- [14] SETI@home. [Online]. Available: <http://setiathome.ssl.berkeley.edu/>. Accessed on: April 4, 2022.
- [15] Md. Sadek Ferdous, Farida Chowdhury, Md. Moniruzzaman. "A Taxonomy of Attack Methods on Peer-to-Peer Network" in *Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security*, India, 2007, pp. 132-138.
- [16] Roger Wattenhofer, "Attacks on Peer-to-Peer Networks" in Semester Thesis of Swiss Federal Institute of Thechnolog, 2005, Zurich, pp.1-36.
- [17] O. P. Voitovych, Y. V. Baryshev, L. M. Kupershtein, E. I. Kolibabchuk, "Investigation of Simple Denial-of-Service Attacks", *Third International IEEE Conference "Problems of Infocommunications. Science and Technology"*, 2016, Kharkiv, Ukraine, pp. 1-4.
- [18] L. Kupershtein, T. Martyniuk, O. Voitovych, B. Kulchytskyi, A. Kozhemiako et al. "DDoS-attack detection using artificial neural networks in Matlab," *Proc.SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-EnergyPhysics Experiments*, 2019. doi: 10.1117/12.2536478.
- [19] N. V. Bahniuk, V. M. Melnyk, O. V. Klekha, I. A. Nevidomskyi, "Vydy DDoS-atak ta alhorytm vyivlennia DDoS-atak typu flood-attack", *Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo*, vol. 18, 2015, pp.6-12 [in Ukrainian].
- [20] Elakrat Mohamed Abdallah, Jung, Jae Cheon. "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication net-work", *Nuclear Engineering and Technology*, no. 50, pp. 780–787, June 2018. doi:10.1016/j.net.2018.01.018.
- [21] X. Fan, and Y. Xiang, "Propagation Modeling of Peer-to-Peer Worms", in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Central Queensland University, Rockhampton, Australia, 2010, pp. 1128-1135.
- [22] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 6th ed. Prentice Hall, Upper Saddle River, NJ, 2013, 752 pp.
- [23] J. Liang, N. Naoumov, and K.W. Ross, "The Index Poisoning Attack in P2P File Sharing Systems" in *25th IEEE International Conference on Computer Communications. Polytechnic Univerisy*, Brooklyn, NY, 2006, pp. 1-12.
- [24] C. Schiller, J. Binkley, D. Harley, G. Evron, T. Bradley, C. Willems, M. Cross, "Botnets – The Killer Web App", Syngress, Rockland, 2007, 482pp. ISBN-10: 1-59749-135-7.
- [25] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, D. Wallach, "Secure routing for structured peer-to-peer overlay networks", *SIGOPS Oper. Syst. Rev*, vol. 36, December 2003, pp. 299-314. doi:10.1145/844128.844156.
- [26] D. Stutzbach, R. Rejaie, "Understanding churn in peer-to-peer networks" in *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, New York, 2006, pp. 189-202.
- [27] A. Vasudeva, M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks", *Journal of Network and Computer Applications*, vol. 120, pp. 78-118, 2018. doi: 10.1016/j.jnca.2018.07.006.
- [28] W. Ai, L. Xinsong and L. Kejian, "Efficient flooding in peer-to-peer networks," *2006 7th International Conference on Computer-Aided Industrial Design and Conceptual Design*, 2006, pp. 1-6, doi: 10.1109/CAIDCD.2006.329410.

Відомості про авторів

Куперштейн Леонід Михайлович – кандидат технічних наук, доцент кафедри захисту інформації.

Кренцін Михайло Дмитрович – аспірант кафедри захисту інформації.

Дудатсьєв Андрій Веніамінович – кандидат технічних наук, доцент кафедри захисту інформації.

Каплун Валентина Аполінаріївна – старший викладач кафедри захисту інформації.

L. M. Kupershtein, M. D. Krentsin, A. V. Dudatyev, V. A. Kaplun ANALYSIS OF SECURITY PROBLEMS OF PEER-TO-PEER NETWORKS

Vinnitsia National Technical University, Vinnitsia

УДК 004.31: 004.627

В. А. Лужецький, Л. А. Савицька, В. А. Каплун

СПЕЦІАЛІЗОВАНИЙ ПРОЦЕСОР ДЛЯ УЩІЛЬНЕННЯ ДАНИХ

Вінницький національний технічний університет, Вінниця

Анотація. Одним із ефективних підходів щодо ущільнення даних є підхід, що базується на використанні оптимізуючих властивостей чисел Фібоначчі. Суть підходу полягає в тому, що в процесі ущільнення блок цифрових даних розглядається як надвелике ціле додатне число, що подається у вигляді лінійної форми Фібоначчі. Реалізація методів ущільнення даних на основі лінійної форми Фібоначчі програмними засобами вимагає великих витрат часу, які пов'язані з обчисленнями над числами великої розрядності (до 8000 двійкових розрядів). Для деяких застосувань такі витрати часу є неприпустимими, тому існує потреба створення спеціалізованого процесора, який забезпечить пришвидшення процесу ущільнення даних. Розроблення математичних і структурних моделей спеціалізованого процесора та його компонентів здійснено з використанням функціонально-структурного підходу щодо проектування цифрових пристроїв. Виходячи з узагальненої моделі процесу адаптивного ущільнення даних на основі лінійної форми Фібоначчі визначено основні функції, які має реалізовувати спеціалізований процесор. Цей процесор входить до складу комп'ютерної системи і певним чином підключений до центрального процесора комп'ютера. Оскільки файли, що підлягають ущільненню, та ущільнені файли зберігаються в пам'яті комп'ютера, то передбачається, що центральний процесор буде виконувати зчитування і запис файлу, формування послідовностей P і P^* та реалізовувати функцію оптимізації на рівні послідовностей. На спеціалізований процесор покладаються обчислення над числами великої розрядності. Для реалізації сукупності всіх функцій запропоновано побудувати не один операційний автомат, а здійснити його декомпозицію на автомати, кожен з яких реалізує відповідну функцію. Розглянуто математичні моделі та структури таких модулів спеціалізованого процесора: моделювання джерела даних, кодування, декодування, оптимізації на рівні блоків, формування структури послідовності P^* . Апаратна реалізація обчислень над числами великої розрядності і можливість реалізації основних функціональних перетворень окремими модулями у конв'єрному режимі забезпечує пришвидшення процесу ущільнення даних порівняно з програмною реалізацією.

Ключові слова: ущільнення даних, лінійна форма Фібоначчі, спеціалізований процесор, операційний автомат.

Abstract. One of the effective approaches to data compression is the approach based on the use of optimizing properties of Fibonacci numbers. The essence of the approach is that in the process of compaction the block of digital data is considered as a large positive integer, given in the form of a linear Fibonacci form. The implementation of data compression methods based on the linear form of Fibonacci software requires a lot of time, which is associated with calculations over large numbers (up to 8000 binary digits). For some applications, such time is unacceptable, so there is a need to create a specialized processor that will speed up the process of data compression. The development of mathematical and structural models of a specialized processor and its components is carried out using a functional-structural approach to the design of digital devices. Based on the generalized model of the process of adaptive data compression based on the linear Fibonacci form, the main functions to be implemented by a specialized processor are identified. This processor is part of a computer system and is in some way connected to the computer's CPU. Because the files to be compressed and the compressed files are stored in computer memory, the CPU is expected to read and write the file, generate P and P^* sequences, and implement a sequence-level optimization function. The specialized processor is responsible for calculations over large numbers. To implement a set of all functions, it is proposed to build more than one operating machine, and to decompose it into machines, each of which implements the corresponding function. Mathematical models and structures of such modules of the specialized processor are considered: modeling of a data source, coding, decoding, optimization at the level of blocks, formation of structure of sequence P^* . Hardware implementation of calculations over large numbers and the ability to implement basic functional transformations of individual modules in the pipeline mode provides acceleration of the data compression process compared to software implementation.

Key words: data compression, linear Fibonacci form, specialized processor, operating machine.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-15-25>.

Вступ

Ущільнення інформації скорочує обсяг пам'яті, що необхідна для її зберігання, і кількість часу, який потрібен для її передавання каналами з фіксованою пропускною здатністю. За останнє десятиліття продуктивність процесорів зростає експоненційно порівняно зі швидкістю доступу до пристроїв пам'яті, що є ґрунтовною причиною застосовувати ущільнення інформації для збільшення загальної продуктивності системи. Задача проектування комп'ютерних систем та їх компонентів часто формулюється як задача створення засобів високої продуктивності з урахуванням заданих обмежень на апаратні витрати. Основний шлях її вирішення полягає у використанні спеціалізованих процесорів, які апаратно реалізують елементи математичних обчислень.

Актуальність

Одним із ефективних підходів щодо ущільнення даних є підхід, що базується на використанні оптимізуючих властивостей чисел Фібоначчі [1]. Суть підходу полягає в тому, що в процесі ущільнення блок цифрових даних будь-якої довжини розглядається як надвелике ціле додатне число, що подається у вигляді лінійної форми Фібоначчі [2,3,4]. Реалізація методів ущільнення даних на основі лінійної форми Фібоначчі програмними засобами вимагає великих витрат часу, які пов'язані з обчисленнями над числами великої розрядності (до 8000 двійкових розрядів). Для деяких застосувань такі витрати часу є неприпустимими, тому існує потреба створення спеціалізованого процесора, який забезпечить пришвидшення процесу ущільнення даних.

Мета досліджень

Метою статті є пришвидшення процесу ущільнення даних, що базується на використанні лінійної форми Фібоначчі, шляхом розробки спеціалізованого процесору.

Постановка задач

Спеціалізований процесор для ущільнення даних (DC-процесор) – це цифровий операційний пристрій, який входить до складу комп'ютерної системи і певним чином підключений до центрального процесора комп'ютера. Відомо, що будь-який операційний пристрій за виконуваними функціями і структурою складається з двох частин: операційного і керуючого автоматів. Доволі часто через складність обчислювальних процедур побудова єдиного цілісного операційного автомату викликає певні труднощі. Тому на практиці використовують його декомпозицію на більш прості операційні автомати, що реалізують потрібний набір функцій. Враховуючи сказане, в даній статті розв'язуються такі задачі:

- розробка узагальненої структури спеціалізованого процесора для ущільнення даних;
- аналіз виконуваних функцій та розробка структури модулів DC-процесора.

Узагальнена модель процесу адаптивного ущільнення

У роботі [5] автори запропонували таку узагальнену модель процесу адаптивного ущільнення даних на основі лінійної форми Фібоначчі:

$$C_A = \{P, A, M, C, D, P_M, P_C, P^*, S, f\},$$

де P – вихідна послідовність символів алфавіту $A = \{0,1\}$;

$M = \{M_i\}$ – множина правил моделювання джерела даних;

$C = \{C_j\}$ – множина правил кодування даних;

$D = \{D_j\}$ – множина правил декодування даних;

$P_M = \{P_{M_i}\}$ – множина послідовностей, що є результатом моделювання;

$P_C = \{P_{C_{ij}}\}$ – множина послідовностей, що є результатом кодування;

P^* – послідовність ущільнених даних;

S – правило формування структури послідовності;

f – функція оптимізації.

Процес відновлення даних описується такою узагальненою моделлю:

$$DC = \{A, P^*, P, D, S\},$$

де $A = \{0,1\}$ – алфавіт;

P^* – послідовність ущільнених даних;

P – послідовність відновлених (вихідних) даних;

D – множина правил декодування даних;

S – правило формування структури послідовності P^* .

Саме ці моделі покладено в основу створення спеціалізованого процесора для ущільнення даних.

Узагальнена структура спеціалізованого процесора для ущільнення даних

У складі комп'ютерної системи спеціалізований і центральний процесори обмінюються потоками даних, виконуючи функції, перелік яких наведено в табл. 1.

Таблиця 1 – Розподіл виконуваних функцій між процесорами

Процес	Виконувані функції	
	Центральний процесор	Спеціалізований процесор
ущільнення	1. Зчитування файлу та формування послідовності P . 2. Формування послідовності P^* та запис файлу.	1. Моделювання за правилами. 2. Кодування за правилами. 3. Оптимізація на рівні блоків.
відновлення	1. Зчитування файлу та формування послідовності P^* . 2. Формування послідовності P та запис файлу.	1. Декодування за правилами.

Оскільки файли, що підлягають ущільненню, та ущільнені файли зберігаються в пам'яті комп'ютера, то передбачається, що центральний процесор буде виконувати зчитування і запис файлу,

формування послідовностей P і P^* та реалізувати функцію оптимізації на рівні послідовностей. На DC-процесор покладаються обчислення над числами великої розрядності.

Схему оброблення потоку даних у DC-процесорі наведено на рис. 1.

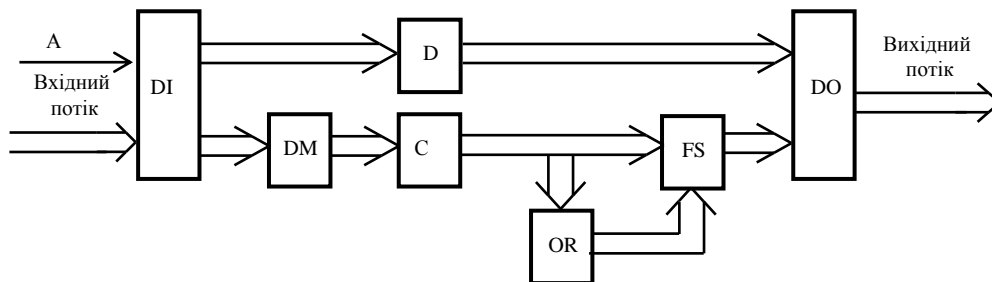


Рисунок 1 – Функціональна модель DC-процесора

Появлення заявки A на вхідній шині DC-процесора приводить до ініціювання процесу «ВХІДНИЙ ДИСПЕТЧЕР» (DI), який визначає тип заявки (ущільнення чи відновлення) і спрямовує потік даних (P чи P^*) до потрібного процесу. В разі заявки на ущільнення потік даних спрямовується до процесу «МОДЕЛЮВАННЯ ДЖЕРЕЛА ДАНИХ» (DM), після якого дані надходять до процесу «КОДУВАННЯ» (C). За результатами кодування ініціюється процес «ОПТИМІЗАЦІЯ РЕЗУЛЬТАТІВ» (OR), який, у свою чергу, ініціює процес «ФОРМУВАННЯ СТРУКТУРИ» (FS). У разі заявки на відновлення потік даних спрямовується до процесу «ДЕКОДУВАННЯ» (D). Завершення процесу OR або D приводить до дії процесу «ВИХІДНИЙ ДИСПЕТЧЕР» (DO), який збирає готові результати і організовує з них потік даних до центрального процесора.

Для реалізації сукупності всіх процесів пропонується побудувати не один операційний автомат, а здійснити його декомпозицію на автомати, кожен з яких реалізує відповідний процес. Виходячи з цього, DC-процесор має структуру, до складу якої входять такі модулі (рис. 2):

- модуль системних операцій (МСО), що здійснює зв'язок з центральним процесором і реалізує процеси DI і DO;
- модуль моделювання джерела даних (ММДД), що реалізує процес DM;
- модуль кодування (МКод), що реалізує процес C;
- модуль декодування (МД), що реалізує процес D;
- модуль оптимізації (МО), що реалізує процес OR;
- модуль формування структури послідовності P^* (МФСП), що реалізує процес FS;
- модуль керування (МКер), що координує роботу решти модулів.

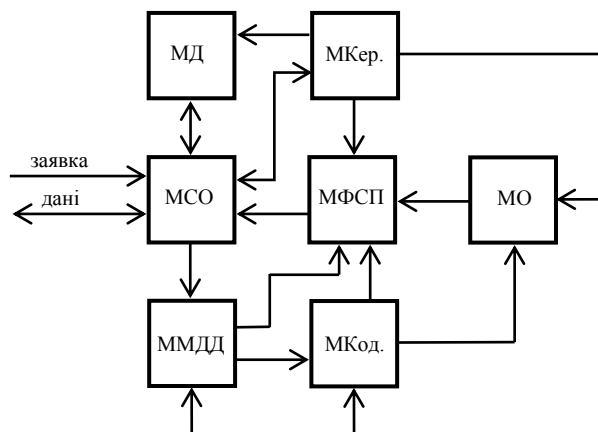


Рисунок 2 – Структура DC-процесора

Кожен з модулів МСО, ММДД, МКод, МФСП, МД і МО далі розглядається як окремий операційний автомат.

Відомо, що операційний автомат описується такими множинами [6].

1. Множиною вхідних слів $D = \{d_1, \dots, d_n\}$, що надходять до автомату як операнди.
2. Множиною вихідних слів $R = \{r_1, \dots, r_n\}$, що є результатами виконання операцій.
3. Множиною внутрішніх слів $S = \{s_1, \dots, s_n\}$, що використовуються для представлення інформації в процесі виконання операцій.

4. Множиною мікрооперацій $Y = \{y_m\}$, $m=1, \dots, M$, що реалізують перетворення $S = f_m(S)$ над словами інформації, де f_m – функція перетворення даних.

5. Множиною логічних умов $X = \{x_l\}$, $l=1, \dots, L$, де $x_l = f_l(S)$ і f_l – булева функція.

Таким чином, функція операційного автомата задана, якщо визначено множини D , R , S , Y , X . Час не є аргументом функції операційного автомата. Функція встановлює список дій, виконуваних автоматом, і характеризує засоби, що використовуються для обчислень, але не сам обчислювальний процес. Множині D відповідають входи операційного автомата. Множині R ставляться у відповідність виходи даних. Множині внутрішніх слів S ставляться у відповідність запам'ятовувальні пристрої, реєстри та лічильники.

Порядок виконання дій у часі визначається у формі функцій керуючого автомата. Функція керуючого автомата описується схемою алгоритму, що встановлює порядок перевірки логічних умов x_1, \dots, x_L і порядок виконання мікрооперацій y_1, \dots, y_M .

Дотримуючись цих теоретичних положень, розглянемо функції та структури модулів DC-процесора.

Структура модуля моделювання джерела даних

Запропоновані в [7] моделі джерела даних характеризуються такими параметрами:

- довжина блоку l (значення задається від l_{\min} до l_{\max});
- основа системи числення B (задається значення 256 або визначається за змістом блоку даних);
- значення числових еквівалентів байтів (незмінені чи зменшені на S_{\min});
- порядок використання елементів послідовності $s_0, s_1, s_2, \dots, s_{l-1}$, де s_j – числовий еквівалент ASCII коду j -го байту ($j=0, 1, 2, \dots, l-1$).

Для реалізації цих моделей потрібно таке:

1. Визначити $S_{\max} = \max(s_0, s_1, s_2, \dots, s_{l-1})$ і здійснювати обчислення за формулами:

$$N_M = \sum_{j=0}^{l-1} s_j B^j \quad \text{і} \quad N_C = \sum_{j=0}^{l-1} s_{(l-j-1)} B^{(l-j-1)} .$$

Число B для кожного блоку даних змінюється від $(S_{\max} + 1)$ до 256.

2. Визначити $S_{\min} = \min(s_0, s_1, s_2, \dots, s_{l-1})$ і здійснювати обчислення за формулами:

$$N_M = \sum_{j=0}^{l-1} d_j B^j \quad \text{і} \quad N_C = \sum_{j=0}^{l-1} d_{(l-j-1)} B^{(l-j-1)} , \quad \text{де} \quad d_j = s_j - S_{\min} .$$

Число B для кожного блоку даних змінюється від $(S_{\max} - S_{\min} + 1)$ до 256.

При цьому використовуються такі мікрооперації:

- | | |
|------------------------------|-----------------------------|
| - порівняння «більше» (cph); | - порівняння «менше» (cpl); |
| - додавання (add); | - віднімання (sub); |
| - інкремент (inc); | - декремент (dec); |
| - множення (mul); | - запис у реєстр (mov); |
| - зчитування з пам'яті (ld); | - запис у пам'ять (st). |

Нехай P_i – блок даних, що підлягають ущільненню та N – число, що є результатом моделювання джерела даних. Тоді маємо такі множини, що описують модуль ММДД як операційний автомат.

1. Множина вхідних слів $D = \{P_i, l\}$.
2. Множина вихідних слів $R = \{N, S_{\min}, S_{\max}, B\}$.
3. Множина внутрішніх слів $S = \{P_i, l, S_{\min}, S_{\max}, N, B\}$.
4. Множина мікрооперацій $Y = \{cph, cpl, add, sub, mul, inc, dec, mov, ld, st\}$.

5. Множина логічних умов $X = \{x_0, x_1, x_2, x_3\}$, де: x_0 – умова, що $s_i > s_j$; x_1 – умова, що $s_i < s_j$; x_2 – умова, що Ліч1=0, x_3 – умова, що Ліч2=257; x_4 – умова, що Ліч1=Pr1.

Зробивши функціонально-структурне відображення, в якому кожному математичному елементу формалізованого опису операційного автомата ставиться у відповідність елемент структури, отримаємо структурну схему модуля ММДД, яку наведено на рис. 3.

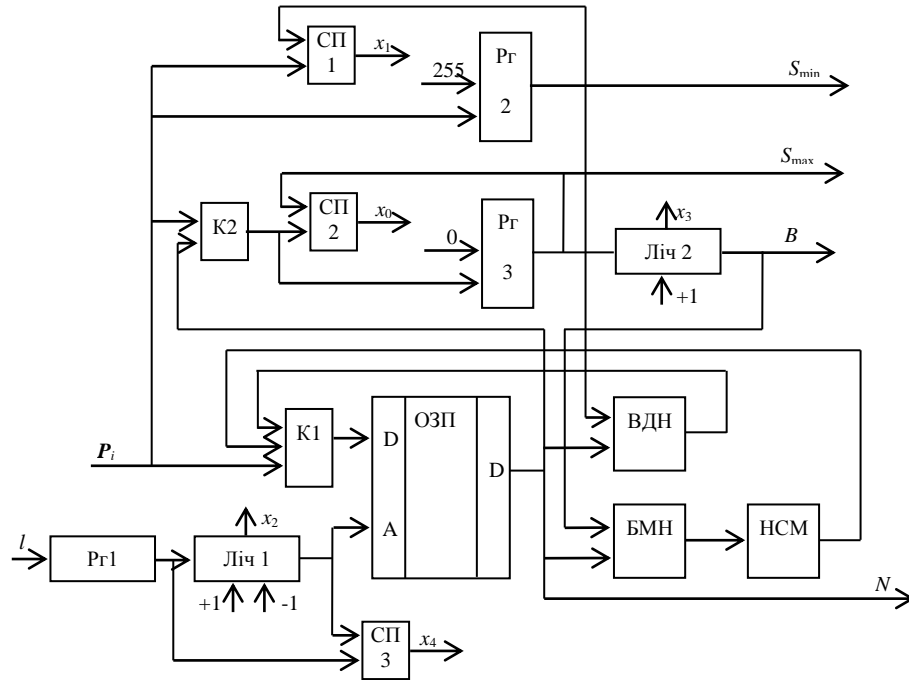


Рисунок 3 – Структурна схема модуля моделювання джерела даних

Тут пам'ять ОЗП обсягом l байтів використовується спочатку для зберігання блоку даних P_i , а потім для накопичення коду числа N . У регістрі $Pr1$ зберігається код довжини блоку даних. Лічильник Ліч1 забезпечує послідовний запис і зчитування байтів даних у порядку від молодшого байту до старшого та навпаки. Схема порівняння СП1 і регістр $Pr2$ використовуються для визначення $S_{\min} = \min(s_0, s_1, s_2, \dots, s_{l-1})$, а СП2 і $Pr3$ – для визначення $S_{\max} = \max(s_0, s_1, s_2, \dots, s_{l-1})$. За допомогою віднімача ВДН обчислюються числові еквіваленти байтів $d_j = s_j - S_{\min}$, $j=0, 1, \dots, l-1$. Блок множення БМН і нагромаджувальний суматор НСМ використовуються для обчислень за наведеними вище формулами. Лічильник Ліч2 використовується для формування значень B у діапазоні від $(S_{\max} + 1)$ до 256.

Структура модуля кодування

Для кодування великих чисел використовуються два правила $C_{\text{лфф}}$ і $C_{\text{слфф}}$. Перше правило передбачає перетворення числа N у лінійну форму Фібоначчі (ЛФФ), а друге – числа N_1 , що є частиною числа N . Тому основною функцією модуля кодування є формування лінійної форми Фібоначчі.

Реалізація цієї функції передбачає виконання таких дій.

1. Обчислення елементів убутої послідовності чисел Фібоначчі за формулою:

$$\varphi_1(j-2) = \varphi_1(j) - \varphi_1(j-1), \quad j=12l, (12l-1), \dots, 1.$$

2. Визначення символів a_i коду Фібоначчі числа $N = (a_n a_{n-1} \dots a_2 a_1)$.

3. Обчислення за формулою:

$$q = \sum_{j=n}^1 a_j \varphi_1(j-1).$$

4. Обчислення за формулою:

$$w_i = w_{i-2} - w_{i-1}, \quad i = 2, 3, \dots, w_0 = N, w_1 = q \text{ поки } w_i > 0.$$

Якщо обчислення виконані j разів, то результатом перетворення числа N у лінійну форму Фібо-

наччі є цілі додатні числа: j , $q_2 = w_{j+1}$ і $q_1 = w_j$.

5. Формування кодів Q_j , Q_1 , Q_2 , l_{Q_1} і l_{Q_2} .

Враховуючи все це, маємо такі множини, що описують модуль МКод як операційний автомат.

1. Множина вхідних слів $D = \{N, l\}$.

2. Множина вихідних слів $R = \{Q_j, l_{Q_1}, l_{Q_2}, l_{Q_{N_2}}, Q_1, Q_2, Q_{N_2}\}$.

3. Множина внутрішніх слів $S = \{N, N_1, N_2, l, \varphi_1(12 \cdot l), \varphi_1(12 \cdot l - 1), q, j, q_1, q_2\}$.

4. Множина мікрооперацій $Y = \{cph, add, sub, inc, dec, mov, ld, st\}$.

5. Множина логічних умов $X = \{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$, де: x_0 – умова, що $n_1 > n_2$; x_1 – умова, що Ліч1=0, x_2 – умова, що Ліч2=0, x_3 – умова, що Ліч3=0, x_4 – умова, що Ліч4=0, x_5 – умова, що Ліч5=0, x_6 – умова, що ОЗП6[Ліч5]=0, x_7 – умова, що ОЗП7[Ліч5]=0, x_8 – умова, що ОЗП5[Ліч4]=0.

Виконавши функціонально-структурне відображення, отримаємо структурну схему модуля кодування, яку наведено на рис. 4.

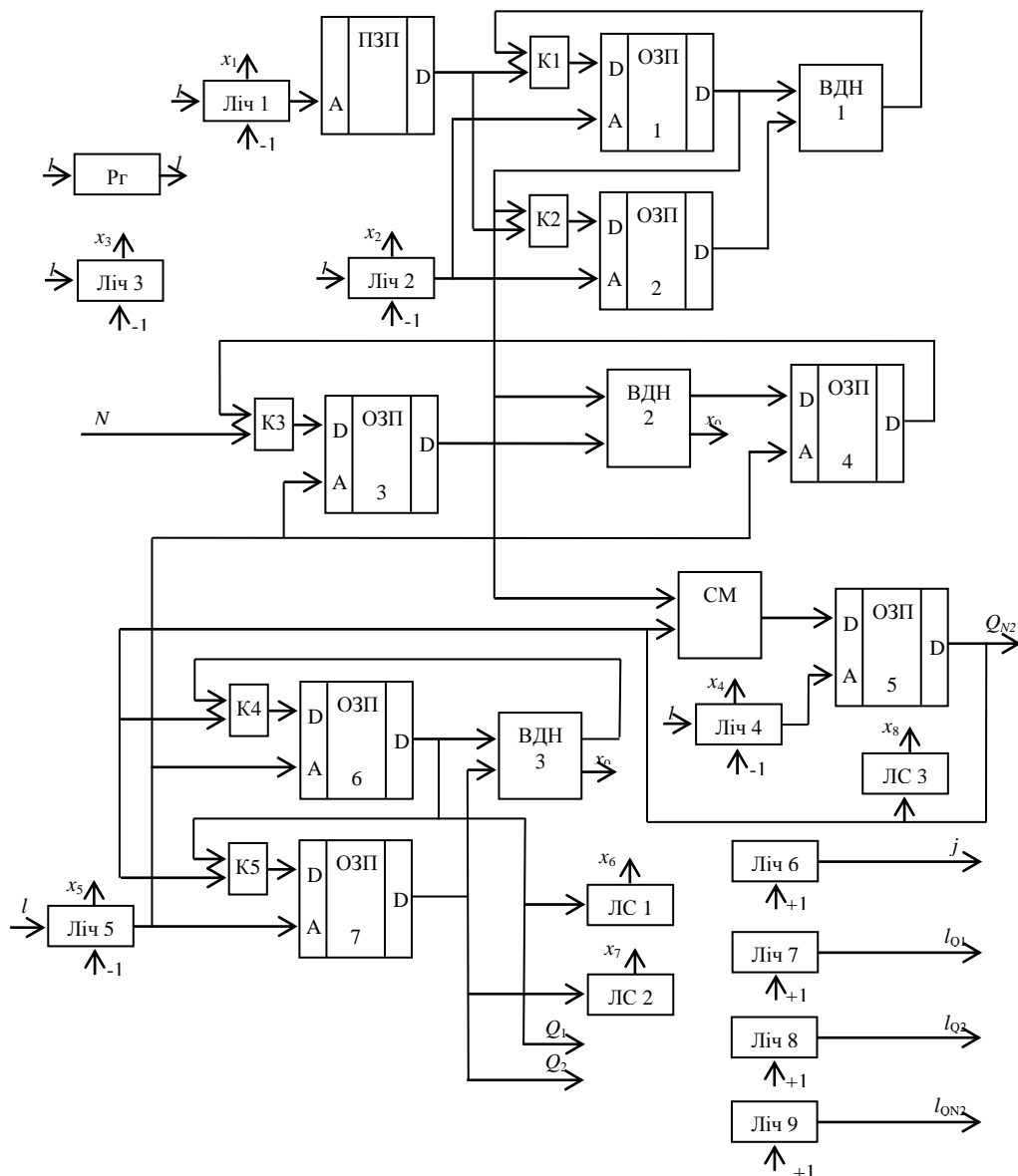


Рисунок 4 – Структурна схема модуля кодування

У постійному запам'ятовувальному пристрої (ПЗП) зберігаються два числа Фібоначчі, які використовуються як початкові для формування убутної послідовності чисел Фібоначчі. Оскільки ці числа мають велику розрядність, то вони зберігаються у певній кількості комірок ПЗП. Для вибору потрібної адреси

комірки використовується лічильник Ліч1. Перед початком формування послідовності чисел Фібоначчі початкові числа переписуються в оперативні запам'ятовувальні пристрої ОЗП1 і ОЗП2. Формування кодів адрес для них забезпечує лічильник Ліч2. Віднімач ВДН1 використовується для обчислення послідовності чисел Фібоначчі, а ВДН2 спільно з ОЗП3 і ОЗП4 – для порівняння числа, що перетворюється, з числами Фібоначчі. Лічильник Ліч3 формує коди адрес для ОЗП3 і ОЗП4. Зміну напрямків надходження даних до ОЗП1, ОЗП2, ОЗП3, ОЗП6 і ОЗП7 забезпечують комутатори К1, К2, К3, К4 і К5, відповідно.

Обчислення q забезпечується суматором СМ і ОЗП5, крім цього вони забезпечують обчислення числа N_2 при формуванні скороченої ЛФФ(*). Складові j , q_1 і q_2 лінійної форми Фібоначчі визначаються з використанням ОЗП6, ОЗП7, ВДН3 і Ліч6. Коди l_{Q_1} , l_{Q_2} і $l_{Q_{N_2}}$ одержуються за допомогою Ліч7, Ліч8 і Ліч9. Логічні схеми ЛС1, ЛС2 і ЛС3 формують логічну "1", коли на їхні входи надходить код, що складається з усіх нулів. Це забезпечує відкидання старших незначущих байтів коду числа.

Структура модуля декодування

Основою правил декодування є зворотне перетворення Фібоначчі, яке передбачає виконання j разів обчислень за рекурентною формулою $w_{i+1} = w_i + w_{i-1}$, $i = 1, 2, \dots, j$.

У разі правила декодування $D_{\text{лфф}}$ число N є остаточним результатом декодування. Для правила декодування $D_{\text{сллф}}$ результатом обчислень є число N_1 , до якого потрібно додати число N_2 , щоб отримати остаточний результат. Число N_2 – це числовий еквівалент складової коду ущільненого блоку даних.

Враховуючи сказане, маємо такі множини, що описують модуль МД як операційний автомат.

1. Множина вхідних слів $\mathbf{D} = \{Q_j, l_{Q_1}, l_{Q_2}, l_{Q_{N_2}}, Q_1, Q_2, Q_{N_2}, l\}$.
2. Множина вихідних слів $\mathbf{R} = \{N\}$.
3. Множина внутрішніх слів $\mathbf{S} = \{Q_j, l_{Q_1}, l_{Q_2}, l_{Q_{N_2}}, Q_1, Q_2, Q_{N_2}, N, l\}$.
4. Множина мікрооперацій $\mathbf{Y} = \{\text{add}, \text{dec}, \text{mov}, \text{ld}, \text{st}\}$.
5. Множина логічних умов $\mathbf{X} = \{x_1, x_2, x_3, x_4\}$, де: x_1 – умова, що Ліч1=0, x_2 – умова, що Ліч2=0, x_3 – умова, що Ліч3=0, x_4 – умова, що Ліч4=Рг.

Виконавши функціонально-структурне відображення, отримаємо структурну схему модуля декодування, яку наведено на рис. 5.

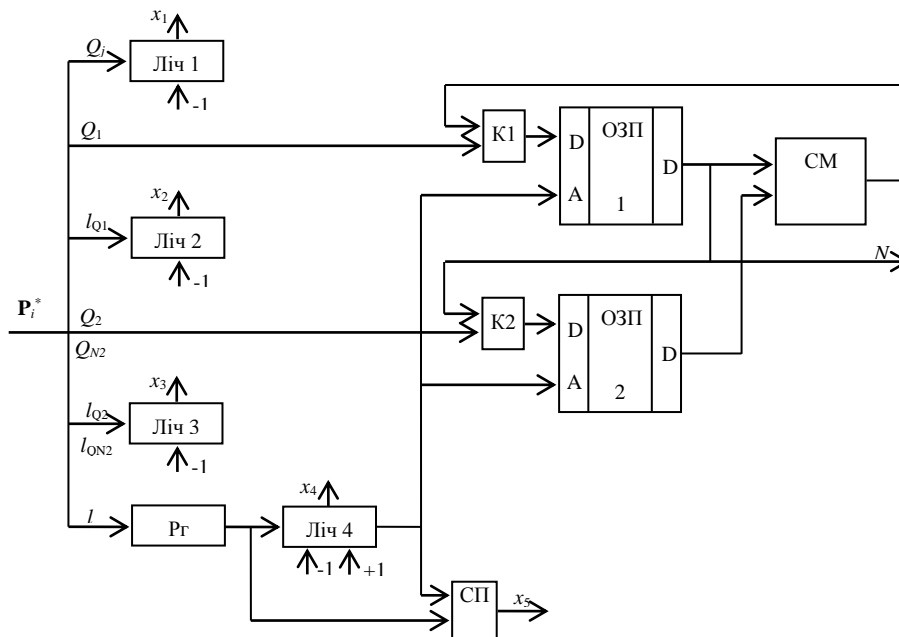


Рисунок 5 – Структурна схема модуля декодування

Тут лічильники Ліч1, Ліч2 і Ліч3 зберігають початкові та поточні значення кодів Q_j , l_{Q_1} і l_{Q_2} ($l_{Q_{N_2}}$), відповідно. Лічильники Ліч2 і Ліч3 забезпечують запис кодів Q_1 і Q_2 (Q_{N_2}) в оперативні запам'ятовувальні пристрої ОЗП1 і ОЗП2. Кількість обчислень за рекурентною формулою (2.13) визначається змістом Ліч1. Лічильник Ліч4 формує коди адрес для ОЗП1 і ОЗП2 в процесі обчислень і при виведенні кодів результату декодування. Зміну напрямків надходження даних до ОЗП1 і ОЗП2 забезпечують комутатори К1 і К2.

Структура модуля оптимізації

Для вибору найкращого результату ущільнення використовується така функція оптимізації на рівні блоків даних:

$$f_{\text{бл}}^{\text{нп}} = \min \left\{ \left(l_{\text{ф}}^{(1)}, l_{\text{ф}}^{(2)}, l_{\text{сф}}^{(1)}, l_{\text{сф}}^{(2)} \right)^{(i)}, l \right\}.$$

Ця функція передбачає спочатку вибір серед лінійних форм Фібоначчі такої форми, що утворює перетворений блок найменшої довжини $l_{\text{перет.}}$, і формування ознак:

$$c_1 = 0 \text{ і } c_2 = 0, \text{ якщо } l_{\text{перет.}} = l_{\text{ф}}^{(1)} = \min \left(l_{\text{ф}}^{(1)}, l_{\text{ф}}^{(2)}, l_{\text{сф}}^{(1)}, l_{\text{сф}}^{(2)} \right);$$

$$c_1 = 1 \text{ і } c_2 = 0, \text{ якщо } l_{\text{перет.}} = l_{\text{ф}}^{(2)} = \min \left(l_{\text{ф}}^{(1)}, l_{\text{ф}}^{(2)}, l_{\text{сф}}^{(1)}, l_{\text{сф}}^{(2)} \right);$$

$$c_1 = 0 \text{ і } c_2 = 1, \text{ якщо } l_{\text{перет.}} = l_{\text{сф}}^{(1)} = \min \left(l_{\text{ф}}^{(1)}, l_{\text{ф}}^{(2)}, l_{\text{сф}}^{(1)}, l_{\text{сф}}^{(2)} \right);$$

$$c_1 = 1 \text{ і } c_2 = 1, \text{ якщо } l_{\text{перет.}} = l_{\text{сф}}^{(2)} = \min \left(l_{\text{ф}}^{(1)}, l_{\text{ф}}^{(2)}, l_{\text{сф}}^{(1)}, l_{\text{сф}}^{(2)} \right).$$

Потім порівнюються довжина лінійної форми Фібоначчі $l_{\text{перет.}}$ і довжина початкового блоку даних l . Якщо $l_{\text{перет.}} < l$, то формується ознака $p=1$, а якщо $l_{\text{перет.}} \geq l$, то формується ознака $p=0$.

Виходячи з цього, маємо такі множини, що описують модуль МО як операційний автомат.

1. Множина вхідних слів $\mathbf{D} = \{ l_{Q_1}, l_{Q_2}, l_{Q_{N_2}}, Q_1, Q_2, Q_{N_2}, l \}$.
2. Множина вихідних слів $\mathbf{R} = \{ l_{Q_1}, l_{Q_2}, l_{Q_{N_2}}, Q_1, Q_2, Q_{N_2}, c_1, c_2, p \}$.
3. Множина внутрішніх слів $\mathbf{S} = \{ l_{Q_1}, l_{Q_2}, l_{Q_{N_2}}, Q_1, Q_2, Q_{N_2}, c_1, c_2, p, l, l_{\text{перет.}} \}$.
4. Множина мікрооперацій $\mathbf{Y} = \{ \text{add}, \text{mov}, \text{сф} \}$.
5. Множина логічних умов $\mathbf{X} = \{ x_1, x_2, x_3, x_4, x_5, x_6 \}$, де: x_1 – умова, що $l > l_{\text{ф}}^{(1)}$, x_2 – умова, що $l_{\text{ф}}^{(2)} > l_{\text{ф}}^{(1)}$, x_3 – умова, що $l_{\text{сф}}^{(1)} > l_{\text{ф}}^{(1)}$, x_4 – умова, що $l_{\text{сф}}^{(2)} > l_{\text{сф}}^{(1)}$, x_5 – умова, що $l > l_{\text{сф}}^{(1)}$, x_6 – умова, що $B > 256$.

Виконавши функціонально-структурне відображення, отримаємо структурну схему модуля оптимізації, яку наведено на рис. 6.

Тут регістри Rг1, Rг2, Rг3, Rг4 і Rг5 зберігають початкові значення кодів l_{Q_1} , l_{Q_2} , $l_{Q_{N_2}}$, l і B , відповідно. Регістри Rг6 – Rг11 призначені для зберігання поточних значень кодів l_{Q_1} , l_{Q_2} , $l_{Q_{N_2}}$ та їх сум. Зміну напрямків надходження кодів до Rг13 і Rг14, в які записуються остаточні результати, забезпечують комутатори К1 і К2. Для порівняння значень кодів l_{Q_1} , l_{Q_2} , $l_{Q_{N_2}}$, l і B за алгоритмом ущільнення використовуються схеми порівняння СП1 – СП6. Для зберігання ознак, що формуються за результатами порівняння, використовуються тригери Т1 – Т3.

Структура модуля формування структури послідовності

Результат ущільнення складається з певного набору елементів, який має таку структуру:

$$S = \{ l_k \| l_{\pi} \| \pi \| \text{Бл}^* 1 \| \text{Бл}^* 2 \| \dots \| \text{Бл}^* k \},$$

де $\text{Бл}^* i = \{ B_o \| S_{\text{min}} \| Q_j \| l_{Q_1} \| l_{Q_2} \| Q_1 \| Q_2 \}$.

Тут складники мають такі довжини: $l, l_k, l_\pi, Q_j, l_{Q_1}, l_{Q_2} - 2$ байти; $B_0, S_{\min} - 1$ байт; $Q_1 - l_{Q_1}$ байтів; $Q_2 - l_{Q_2}$ байтів; $\pi - k/8$ байтів.

Згідно з розподілом виконуваних функцій між процесорами (див. табл. 1), формування послідовності \mathbf{P}^* , що має структуру S , та запис файлу реалізуються центральним процесором, а формування блоку перетворених даних здійснюється спеціалізованим процесором. З метою зменшення часу обміну даними між процесорами пропонується формувати послідовність бітових ознак π вигляді сукупності байтів у спеціалізованому процесорі.

Виходячи з цього, маємо такі множини, що описують модуль МФСП як операційний автомат.

1. Множина вхідних слів $\mathbf{D} = \{ l, l_k, m, Q_j, l_{Q_1}, l_{Q_2}, l_{QN2}, Q_N, Q_1, Q_2, Q_{N2}, B_0, S_{\min}, c_1, c_2, p \}$.
2. Множина вихідних слів $\mathbf{R} = \{ l, l_k, l_\pi, \pi, C, m, \text{Бл}^*i \}$.
3. Множина внутрішніх слів $\mathbf{S} = \{ l, l_k, m, l_{Q_1}, l_{Q_2}, l_{QN2}, \pi, C, \text{Бл}^*i \}$.
4. Множина мікрооперацій $\mathbf{Y} = \{ \text{inc, dec, mov, ld, st} \}$.
5. Множина логічних умов $\mathbf{X} = \{ x_1, x_2, x_3, x_4, x_5 \}$, де: x_1, x_2, x_3, x_4, x_5 – умова, що Ліч1=0, Ліч2=0, Ліч3=0, Ліч4=0, Ліч5=0, відповідно.

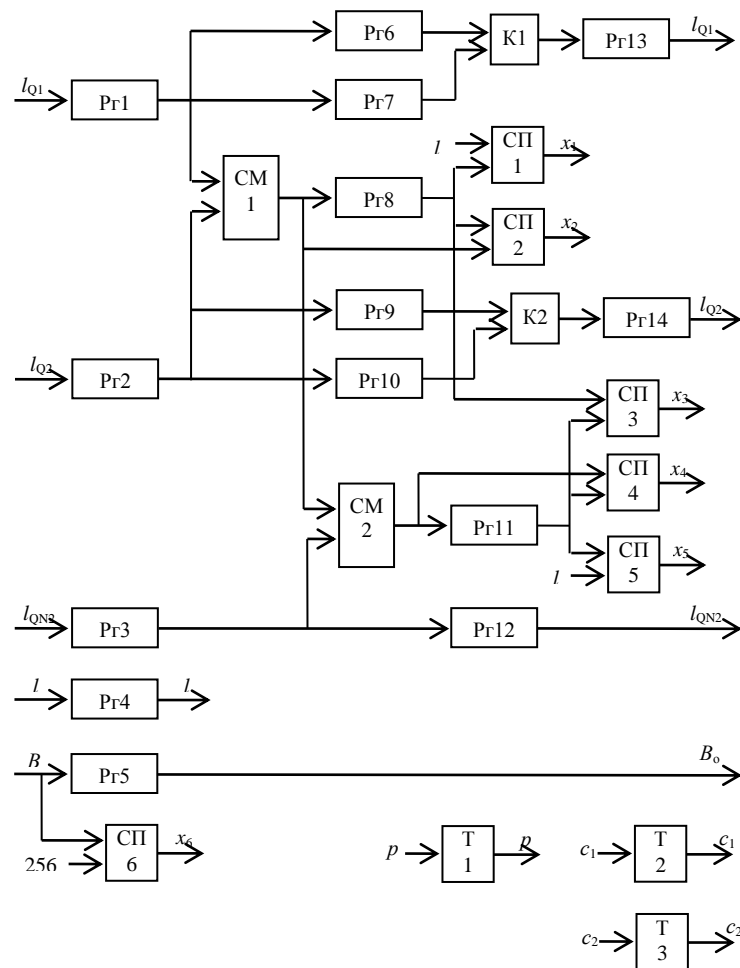


Рисунок 6 – Структурна схема модуля оптимізації

Виходячи з цього, маємо такі множини, що описують модуль МФСП як операційний автомат.

1. Множина вхідних слів $\mathbf{D} = \{ l, l_k, m, Q_j, l_{Q_1}, l_{Q_2}, l_{QN2}, Q_N, Q_1, Q_2, Q_{N2}, B_0, S_{\min}, c_1, c_2, p \}$.
2. Множина вихідних слів $\mathbf{R} = \{ l, l_k, l_\pi, \pi, C, m, \text{Бл}^*i \}$.
3. Множина внутрішніх слів $\mathbf{S} = \{ l, l_k, m, l_{Q_1}, l_{Q_2}, l_{QN2}, \pi, C, \text{Бл}^*i \}$.
4. Множина мікрооперацій $\mathbf{Y} = \{ \text{inc, dec, mov, ld, st} \}$.
5. Множина логічних умов $\mathbf{X} = \{ x_1, x_2, x_3, x_4, x_5 \}$, де: x_1, x_2, x_3, x_4, x_5 – умова, що Ліч1=0, Ліч2=0, Ліч3=0, Ліч4=0, Ліч5=0, відповідно.

Виконавши функціонально-структурне відображення, отримаємо структурну схему модуля формування структури послідовності, яку наведено на рис. 7.

Тут регістри Pr1 – Pr8 і Pr11 – Pr15 зберігають значення кодів l , l_k , m , Q_j , l_{Q_1} , l_{Q_2} , l_{QN2} , Q_N , Q_1 , Q_2 , Q_{N2} , B_0 , S_{\min} . У регістрі Pr9 з бітових ознак p формується байт ознак шляхом зсуву коду. Лічильник Ліч1 підраховує кількість виконаних зсувів. Регістр Pr10 і лічильник Ліч2 забезпечують формування байтів ознак C . Байти ознак π і C накопичуються в пам'яті ОЗП1 і ОЗП2, відповідно. Комутатори K1, K2, K3, лічильник Ліч5 і пам'ять ОЗП3 забезпечують формування структури блоку Бл^{*i}.

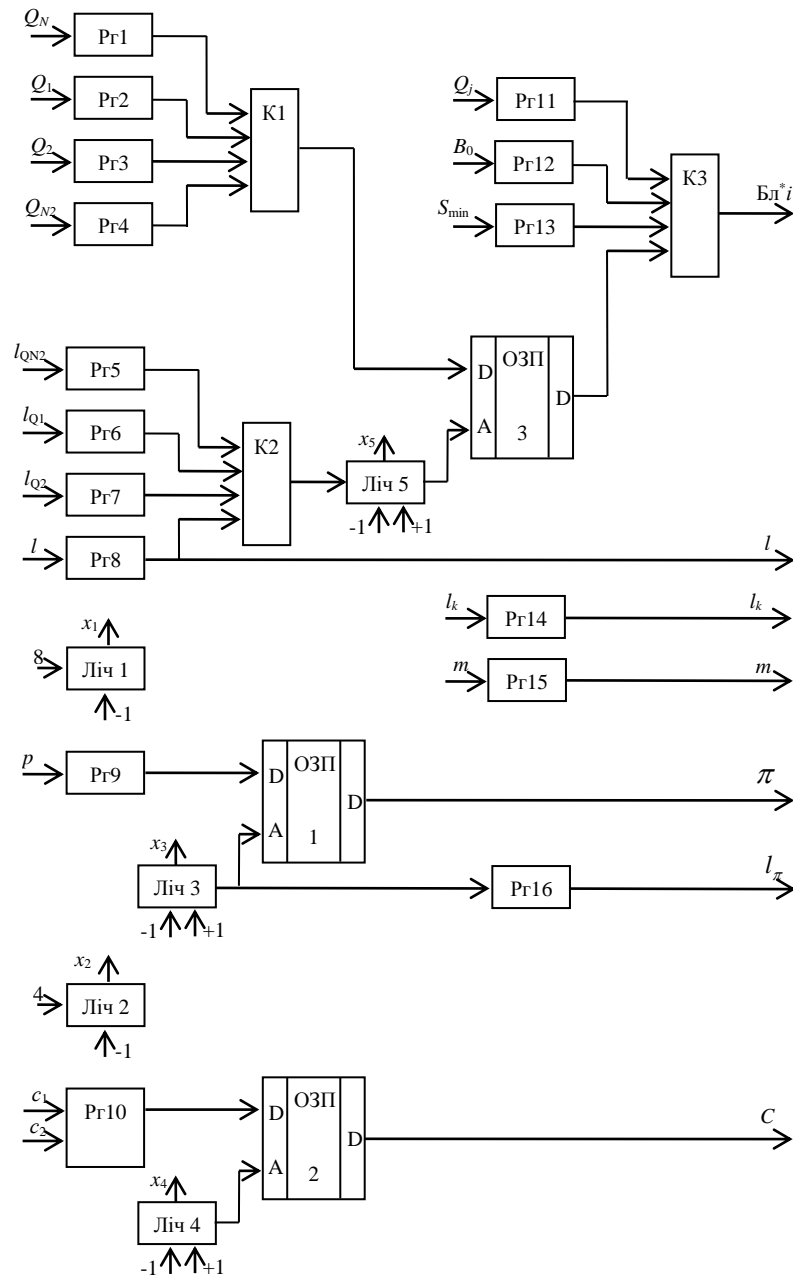


Рисунок 7 – Структурна схема модуля МФСП

Висновки

Реалізація методів ущільнення даних на основі лінійної форми Фібоначчі програмними засобами вимагає великих витрат часу, які є неприпустимими для деяких застосувань, тому для скорочення витрат часу розроблено структури спеціалізованого процесора та його компонентів. Оскільки значна частина часових витрат пов'язана з обчисленнями над числами великої розрядності (до 8000 двійкових розрядів), тому саме ці обчислення реалізуються апаратно DC-процесором, який певним чином підключений до

центрального процесора комп'ютера. При цьому центральний процесор забезпечує зчитування і запис файлу, формування послідовностей P і P^* та реалізацію функцій оптимізації на рівні послідовностей.

Використаний функціонально-структурний підхід щодо проектування цифрових пристроїв забезпечив розробку математичних і структурних моделей спеціалізованого процесора та його компонентів. Побудова окремих модулів для реалізації основних функціональних перетворень забезпечує одночасне виконання цих перетворень у конвеєрному режимі. Апаратна реалізація обчислень над числами великої розрядності і можливість реалізації основних функціональних перетворень у конвеєрному режимі забезпечує пришвидшення процесу ущільнення даних порівняно з програмною реалізацією.

Список літератури

- [1] В. А. Лужецький, Л. А. Савицька, "Розробка та дослідження методів адаптивного ущільнення даних на основі лінійної форми фібоначчі," *Східно-європейський журнал передових технологій*, №1/9 (73), с. 16-22, 2015.
- [2] А. В. Анисимов, Я. П. Рындин и С. Е. Редько, "Обратное преобразование Фибоначчи," *Кибернетика*, № 3, с. 9-11, 1982.
- [3] А. В. Анисимов, "Линейные формы Фибоначчи и параллельные алгоритмы большой размерности," *Кибернетика и системный анализ*, № 3, с. 106–115, 1995.
- [4] В. А. Лужецький і Мохаммад Аль-Майта, "Спосіб зображення цілих чисел великого діапазону," *Вимірювальна та обчислювальна техніка в технологічних процесах*, № 1, с. 156–162, 1998.
- [5] В. А. Лужецький, Л. А. Савицька, Шахзада Ашрафул Хок, "Узагальнена модель адаптивного ущільнення даних," *Інформаційні технології та комп'ютерна інженерія*, № 1(14), с. 56-63, 2009.
- [6] В. М. Глушков, Ю. В. Капитонова, А. Т. Мищенко, *Логическое проектирование дискретных устройств*. К.: Наукова думка, 1987.
- [7] В. А. Лужецький, Л. А. Савицька, "Моделі і методи адаптивного ущільнення даних на основі лінійної форми Фібоначчі," *Збірник наукових праць Харківського університету Повітряних сил*, № 1 (42), с. 53-57, 2015.

Стаття надійшла: 25.04.2022.

References

- [1] V. A. Luzhetskyi, L. A. Savytska, "Rozrobka ta doslidzhennya metodiv adaptivnoho ushchilnennya danykh na osnovi liniynoyi formy Fibonachchi," *Skhidno-yevropeyskyi zhurnal peredovykh tekhnolohiy*, №1/9 (73), s. 16-22, 2015 [in Ukrainian].
- [2] A. V. Anisimov, Ya. P. Ryndin, S. Ye. Redko, "Obratnoye preobrazovaniye Fibonachchi," *Kibernetika*, № 3, с. 9-11, 1982 [in Russian].
- [3] A. V. Anisimov, "Lineynyye formy Fibonachchi i parallelnyye algoritmy bolshoy razmernosti," *Kibernetika i sistemnyy analiz*, № 3, с. 106–115, 1995 [in Russian].
- [4] V. A. Luzhetskyi, Mokhammad Al-Mayta, "Sposib zobrazhennya tsilykh chysel velykoho diapazonu," *Vymiryuvalna ta obchyslyuvalna tekhnika v tekhnolohichnykh protsesakh*, № 1, с. 156–162, 1998 [in Ukrainian].
- [5] V. A. Luzhetskyi, L. A. Savytska, Shakhzada Ashraful Khok, "Uzahalнена model adaptivnoho ushchilnennya danykh," *Informatsiyni tekhnolohiyi ta kompyuterna inzheneriya*, № 1(14), с. 56-63, 2009 [in Ukrainian].
- [6] V. M. Glushkov, Yu. V. Kapitonova, A. T. Mishchenko, *Logicheskoye proyektirovaniye diskretnykh ustroystv*. K.: Naukova dumka. 1987 [in Russian].
- [7] V. A. Luzhetskyi, L. A. Savytska, "Modeli ta metody adaptivnoho ushchilnennya danykh na osnovi liniynoyi formy Fibonachchi," *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitryanykh syl*, № 1 (42), с. 53-57, 2015 [in Ukrainian].

Відомості про авторів

Лужецький Володимир Андрійович – доктор технічних наук, професор, завідувач кафедри захисту інформації.

Савицька Людмила Анатоліївна – кандидат технічних наук, доцент кафедри обчислювальної техніки.

Каплун Валентина Аполінаріївна – старший викладач кафедри захисту інформації.

V. A. Luzhetskyi, L. A. Savitska, V. A. Kaplun

SPECIALIZED DATA COMPRESSION PROCESSOR

Vinnitsia National Technical University, Vinnitsia

УДК 00467

А. М. Мельник

ОНТОЛОГІЯ ЯК ПРОГРАМНА НАДБУДОВА ДО СИСТЕМИ ДЛЯ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ НА ОСНОВІ ІНТЕРВАЛЬНИХ ДАНИХ

Західноукраїнський національний університет, Тернопіль

Анотація. У статті розглянуто важливу наукову проблему розроблення методів та засобів побудови дискретних моделей складних об'єктів у вигляді інтервальних різницевих рівнянь на основі поєднання онтологічного підходу та аналізу інтервальних даних для розширення сфери та умов застосування моделей при забезпеченні її заданих прогностичних властивостей, розв'язування якої слугуватиме поштовхом для розвитку прикладних досліджень у сферах оборони країни, охорони довкілля, медицини та інших галузях, де необхідною компонентою системи підтримки прийняття рішень є математичні моделі об'єктів з розподіленими параметрами. Охарактеризовано сутність підходу до математичного моделювання на основі інтервального аналізу; основною особливістю якого є багаторазова оцінка параметрів моделі «вхід-вихід», побудованої за результатами експериментів, в якому вихідні змінні отримують в інтервальному вигляді. Основними результатами досліджень, наведеними в статті є: опис підходу до використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів, з метою розширення сфери та умов застосування моделей при забезпеченні її заданих прогностичних властивостей; запропоновано покращену схему процесу розробки онто-керованої програмної системи математичного моделювання на основі інтервального аналізу; запропоновано схему процесу реалізації, використання та оновлення розглянутої онтологічної моделі предметної області математичного моделювання на основі інтервальних даних. Особливістю запропонованих в даній статті підходів є те, що вони можуть бути реалізовані як програмна надбудова до прикладних систем математичного моделювання на основі інтервального аналізу. Поєднання підходів на основі інтервального аналізу та онтологічного представлення предметної області забезпечує підвищення ефективності обчислювальних процедур ідентифікації моделей складних об'єктів, а також адаптивне використання різнотипних моделей для різних предметних областей в системах підтримки прийняття рішень.

Ключові слова: онтологія, схема використання, математичне моделювання, методи інтервального аналізу даних, архітектура програмного забезпечення, програмно-інструментальні засоби.

Abstract. The article considers an important scientific problem of developing methods and means of constructing discrete models of complex objects in the form of interval difference equations based on a combination of ontological approach and analysis of interval data to expand the scope and conditions of application of models. impetus for the development of applied research in the fields of national defense, environmental protection, medicine and other areas, where the necessary component of the decision support system are mathematical models of objects with distributed parameters. The essence of the approach to mathematical modeling based on interval analysis is characterized, the main feature of which is the multiple estimation of the parameters of the input-output model, built on the results of experiments in which the output variables are obtained in interval form. The main research results presented in the article are: description of the approach to the use of mathematical modeling ontology based on interval data for software development and use, in order to expand the scope and conditions of application of models while ensuring its given prognostic properties; a step-by-step scheme of the process of developing an onto-controlled software system of mathematical modeling based on interval analysis is proposed; the scheme of the process of realization, use and updating of the considered ontological model of the subject area of mathematical modeling on the basis of interval data is offered. The peculiarity of the approaches proposed in this article is that they can be implemented as a software add-on to applied systems of mathematical modeling based on interval analysis. The combination of approaches based on interval analysis and ontological representation of the subject area provides increased efficiency of computational procedures for identifying models of complex objects, as well as the adaptive use of different models for different subject areas in decision support systems.

Key words: ontology, usage scheme, mathematical modeling, methods of interval data analysis, software architecture, software and tools.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-26-38>.

Вступ

Сучасні тенденції розвитку інформаційних технологій передбачають використання інтелектуалізованих систем підтримки рішень, керованих моделями та даними, в умовах невизначеності. Одним із засобів що забезпечує розвиток таких систем є математичне моделювання як процес побудови математичних моделей із застосуванням методів їх ідентифікації так і оперування побудованими математичними моделями. Це дає можливість створити низку математичних макромоделей складних об'єктів, які використовуються в процесах прийняття рішень так і в процесах їх підготовки.

До побудови таких моделей існує два підходи дедуктивний та індуктивний. При дедуктивному підході необхідно встановити загальний вигляд моделі, а потім перевірити її адекватність на експериментальних даних, що ускладнює застосування цього підходу при побудові макромоделей систем підтримки прийняття рішень, керованих моделями та даними [1,2,3].

Індуктивний підхід, навпаки, ґрунтується на експериментальному дослідженні властивостей складного об'єкту із подальшою ідентифікацією математичної моделі. Побудовані в межах такого підходу моделі є простими і придатними для використання в інтелектуалізованих системах підтримки прийняття рішень та в експертних системах [4-6]. Проте, для побудови таких моделей необхідно розв'язувати задачі структурної ідентифікації математичних моделей складних об'єктів. Особливо ці задачі ідентифікації ускладнюються коли експериментальні дані отримані в інтервальному вигляді, а отримані моделі мають гарантовані прогностичні властивості.

Таким чином виникають протиріччя побудови макромоделей складних об'єктів з гарантованими прогностичними властивостями на основі інтервальних даних, а з іншого боку це призводить до ускладнення методів структурної та параметричної ідентифікації цих моделей, ускладнення самих моделей та ускладнення їх застосування в системах підтримки рішень, керованих моделями та даними, в умовах невизначеності.

Саме це протиріччя становить суть наукової проблеми зниження обчислювальної складності процесів побудови математичних моделей складних об'єктів в умовах інтервальної невизначеності з одночасним забезпеченням гарантованої точності цих моделей в межах необхідних для розв'язування задач прийняття рішень. При розв'язанні цієї проблеми розглядаються комп'ютерні (дискретні) моделі складних об'єктів у різних прикладних сферах.

Спираючись на припущення, що точність математичної моделі повинна бути спів мірна із точністю результатів експерименту, які представлено у вигляді числових інтервалів, що гарантовано включають спостережувані значення характеристик об'єкта, отримані для фіксованих умов його проведення, доцільно для побудови таких моделей використати методи аналізу інтервальних даних, а самі моделі матимуть вигляд інтервальних різницевого рівнянь. Разом з тим, представлення цих моделей у вигляді інтервальних різницевого рівнянь хоча і має переваги для комп'ютерного моделювання, проте вимагає застосування достатньо складних, у порівнянні із використанням стохастичних підходів, методів структурної та параметричної ідентифікації. Також розроблені математичні та комп'ютерні моделі відзначаються високою обчислювальною складністю, яка необхідна для забезпечення адекватності та достатньої точності для прийняття рішень.

Проблема складності також пов'язана із необхідністю розширення сфери застосування макромоделей у певній предметній області, при збереженні її прогностичних властивостей. З іншого боку, спираючись на гіпотезу про те, що онтологічний опис предметної області моделювання дає можливість формалізувати та розширити умови використання інтервальної моделі, то необхідно розробити гібридні методи налаштування структури моделі та параметрів з метою підвищення її прогностичних властивостей.

Таким чином, розроблення методів та засобів побудови дискретних моделей складних об'єктів у вигляді інтервальних різницевого рівнянь на основі поєднання онтологічного підходу та аналізу інтервальних даних для розширення сфери та умов застосування моделей при забезпеченні її заданих прогностичних властивостей є актуальною проблемою, розв'язування якої створює умови для розвитку теорії ідентифікації та математичного моделювання, а також слугуватиме поштовхом для розвитку прикладних досліджень у сферах оборони країни, охорони довкілля, медицини та інших галузях.

Актуальність

Математичне моделювання є одним з основних інструментів, що дозволяє описати об'єкт у простій формі, досліджувати його та прогнозувати поведінку. Математичне моделювання розуміється як процес побудови моделі та її застосування до певних прикладних задач [1-3]. Процеси математичного моделювання складаються з великої кількості процедур, які переважно реалізовані у відповідних інструментах, тобто у вигляді певних програмних систем [3].

Прикладами таких програмних середовищ є Matlab, GNU Octave, Scilab, SageMath. Ці інструменти є багатофункціональними і добре розробленими. Однак практикам часто потрібно використовувати більш спеціалізовані інструменти для побудови математичних моделей, а також адаптувати існуючі інструменти до нестандартних умов, які відсутні у зазначених середовищах. У цьому випадку виникають труднощі у використанні та інтерпретації таких інструментів, оскільки процедури моделювання приховані від дослідника, а це ускладнює їх використання шляхом внесення відповідних програмних змін [3].

У цьому випадку найбільш доцільним рішенням є створення онтологічного опису окремих методів математичного моделювання. У ньому детально описані компоненти процесу побудови моделі та її застосування. Потім цей онтологічний опис використовується для створення відповідного програмного забезпечення. Такий підхід, з одного боку, дозволить інтегрувати створене програмне забезпечення в різні прикладні системи, а з іншого – вносити зміни в існуюче програмне забезпечення [7-12].

Наявність онтологічних описів процесів моделювання на основі певних методів дає змогу уніфікувати програмне забезпечення для вирішення широкого кола завдань. Це дає можливість, на основі досвіду, створити репозиторій математичних моделей, які можна використовувати для моделювання широкого спектру математично подібних властивостей [13-20].

Позитивним ефектом такого підходу буде значне спрощення процесу створення інструментів як для організації процесів моделювання, так і їх застосування до прикладних завдань. Потреба в автоматизованих, систематичних і багаторазових математичних моделях як середовища для отримання, накопичення та повторного використання знань цілком виправдана в контексті великої кількості інформації про знання, які формуються, зберігаються та постійно накопичуються.

Мета

Метою статті є реалізація схеми поєнання онтологічного підходу та аналізу інтервальних даних в процесі розробки програмних систем з інтелектуальним аналізом даних.

Для досягнення поставленої у роботі мети необхідно розв'язати такі завдання:

- провести аналіз проблем моделювання об'єктів на основі інтервальних даних, розкрити сутність онтологічного підходу;
- запропонувати схему використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів;
- запропонувати схему використання онтології математичного моделювання на основі інтервальних даних та її оновлення;
- здійснити експериментальні дослідження запропонованих в роботі методів, оцінити їх ефективність.
- сформулювати напрямки подальших наукових досліджень, виходячи із отриманих у роботі напрацювань та результатів.

Задачі

1. Аналіз проблем моделювання об'єктів на основі інтервальних даних, та особливостей поєнання інтервального та онтологічного підходу.
2. Реалізація схеми використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів.
3. Реалізація схеми використання онтології математичного моделювання на основі інтервальних даних та її оновлення.
4. Проведення експериментальних досліджень для підтвердження ефективності запропонованих процедур на прикладі системи моделювання на основі інтервального аналізу для моделювання шкідливих викидів оксиду вуглецю на певній території міста.

Розв'язання задач

Проблема моделювання об'єктів на основі інтервальних даних розглянута в роботах [1-3,11,15]. Автори інтервального підходу заявляють, що він має цілу низку переваг перед стохастичним підходом. Серед основних – відсутність вимоги до дослідження статистичних характеристик модельованого об'єкта, що в свою чергу зменшує кількість експериментів (вибірка даних). Тому підхід на основі інтервального аналізу даних є більш корисним для дослідження властивостей об'єкта в умовах обмеженої вибірки. Декларативний підхід до представлення знань про методи моделювання об'єктів на основі інтервального аналізу даних дає змогу розробити інструменти для використання зазначеного підходу як дослідниками, так і практиками. Для розробки онтології даної предметної області та її практичного використання в процесі реалізації відповідного програмного забезпечення, необхідно розглянути основні поняття зазначеного підходу.

По-перше, основна концепція, яка відноситься до методу представлення даних у вигляді інтервалів можливих значень змодельованої характеристики представляється наступним відношенням:

$$\left[z_{i,j,h,k}^-; z_{i,j,h,k}^+ \right], \quad i = 0, \dots, I, \quad j = 0, \dots, J, \quad h = 0, \dots, H, \quad k = 0, \dots, K \quad (1)$$

де $\left[z_{i,j,h,k}^-; z_{i,j,h,k}^+ \right]$ – відповідно нижня і верхня межі інтервалів можливих значень вихідної характеристики в точці з дискретно заданими просторовими координатами $i = 0, \dots, I$, $j = 0, \dots, J$, $h = 0, \dots, H$ (для об'єктів із розподіленими параметрами) і дискретний за часом $k = 0, \dots, K$ (для динамічних об'єктів, наприклад динаміка забруднення повітря від транспортних засобів за дискретний час).

Зауважимо, що в вимірному експерименті нижня та верхня межі можуть бути визначені відносно похибкою вимірального пристрою: $z_{i,j,h,k}^- = z_{i,j,h,k} - z_{i,j,h,k} \cdot \mathcal{E}$ і $z_{i,j,h,k}^+ = z_{i,j,h,k} + z_{i,j,h,k} \cdot \mathcal{E}$, де $z_{i,j,h,k}$ – вимірюване значення характеристики; \mathcal{E} – відносна похибка вимірювання.

Представлення експериментальних даних у інтервальному вигляді (1) доцільно у випадках: коли похибка вимірювання значно перевищує методологічні похибки та похибки моделювання, інтервали (1) встановлюють межі допуску відхилень модельованої характеристики об'єкта від номінальної, під умови відомих максимальних значень експериментальних похибок.

Далі необхідно визначити математичний об'єкт для представлення моделі об'єкта. У цьому випадку він обмежується дискретною лінійною моделлю наступного вигляду

$$v_{i,j,h,k} = \vec{f}^T \left(v_{i-d,j-d,h-d,k-d}, v_{i-d+1,j-d,h-d,k-d}, v_{i-1,j-1,h-1,k-1}, \vec{u}_{i,j,h,0}, \dots, \vec{u}_{i,j,h,k} \right) \cdot \vec{g},$$

$$i = d, \dots, I, \quad j = d, \dots, J, \quad h = d, \dots, H, \quad k = d, \dots, K \quad (2)$$

де $\vec{f}^T(\bullet)$ – вектор нелінійних функцій, за допомогою якого перетворюються значення змодельованої характеристики об'єкта, а також вхідні змінні в дискретних точках простору і за певний дискретний час.

У результаті виконання процедури структурної ідентифікації визначається дискретна модель, зокрема: вектор основних функцій $\vec{f}^T(\bullet)$; множини та розмірність векторів вхідних змінних (контролів) $\vec{u}_{i,j,h,0}, \dots, \vec{u}_{i,j,h,k}$, d – порядок дискретної моделі, який, як відомо, еквівалентний порядку диференціального рівняння, аналогічного дискретній моделі. Для реалізації дискретної моделі необхідно також задати початкові умови, тобто значення кожного елемента в наборі $v_{0,0,0,0}, \dots, v_{d-1,d-1,d-1,d-1}, \vec{u}_{i,j,h,0}, \dots, \vec{u}_{i,j,h,k}$ для певного дискретного, як правило початкового, і задати значення компонентів у векторі параметрів \vec{g} .

Якщо загальна форма дискретної моделі відома, наприклад, з фізичних міркувань, залишається ідентифікувати параметри \vec{g} таким чином, щоб забезпечити максимальну узгодженість змодельованої характеристики об'єкта з експериментально отриманими значеннями цієї характеристики. Це завдання називається задачею параметричної ідентифікації [1-3].

Основною проблемою використання цих методів є відсутність декларативного онтологічного опису, що не дозволяє розробляти програмні середовища як інструмент. З іншого боку, як видно з опису задачі ідентифікації, основною проблемою для її вирішення є формування набору потенційних структурних елементів моделі $F = \{f_1(\vec{v}), f_2(\vec{v}), \dots, f_m(\vec{v})\}$ – різницевого (дискретного) рівняння, яке представляє математичну модель об'єкта. Цю проблему можна вирішити за допомогою онтологічного опису предметної області моделювання, тобто операційної онтології. Тому рішення цих проблем зменшить складність процедури моделювання та отримають адекватні моделі з гарантованими прогностичними властивостями.

Підхід до використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів

На основі загального визначеного опису процесу моделювання на основі інтервального аналізу реалізовано онтологічну модель, особливості реалізації якої представлено у вигляді відповідної схеми (рисунк 1). Загальне представлення онтології включає класичних два типи основних об'єктів:

- 1) представлення, які описують основні сутності;
- 2) представлення, які описують відношення між цими сутностями.

Загалом, немає обмежень для визначення відношень між сутностями в онтології. Відношення можуть мати визначену множину значень або бути нескінченними залежно від ситуації. Різні відношення використовуються для з'єднання загального опису при створенні конкретної онтологічної моделі. На рисунку 1 показано основні поняття онтологічної моделі, яка використовується для опису математичного моделювання на основі інтервального підходу.

Конкретні елементи онтології, зв'язок між якими описано за допомогою відповідних стрілок (властивості об'єкта онтології) між класами домену (верхня стрілка) і класами відповідного діапазону (кінець стрілки), де назва на конкретному рядку зображує тип відношення. Сутності будуть змодельовані як «об'єкти» у відповідних прямокутних. Властивість «is-a» пов'язує поняття з його екземплярами (фізичними інтерпретаціями). У запропонованому онтологічному представленні клас «Модель» – це основний концептуальний клас, а «Опис», «Функція», «Процес», «Математична інтерпретація», «Репозиторій», «Завдання», «Сервіс», «Механізм», «Обмеження», «Об'єкт», «Протокол», «Дані» – це підкласи класу «Модель». Підкласи класу «Модель» були виокремлені в онтологічному представленні, щоб зробити онтологію простою і зрозумілою як для окремих дослідників, так і для розробників програмних систем.

На рисунку 1 представлено схему використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів.

Онтологія предметної області – це онтологія, яка фіксує поняття, відношення та властивості про предметну область. Визначена онтологічна модель буде використана для представлення основних концептів математичного моделювання на основі інтервального аналізу в процесі реалізації програмних інструментаріїв.

Онтологія надає інформацію для розробників програмного забезпечення та архітекторів для полегшення процесу створення екземплярів архітектури програмної системи. Вона описує також компоненти програмної архітектури, які допомагають розробникам програмного забезпечення та архітекторам знайти необхідні компоненти архітектури шляхом відстеження зв'язків між елементами онтології та особливостями їх інтерпретації в конкретній системі.

Онтологія представляє компоненти, відношення та обмеження для конкретної предметної області. Це являє собою концептуальну модель в організованому і структурному представленні. Це допоможе проектувальникам та розробникам програмного забезпечення відстежувати взаємозв'язки між цими компонентами.

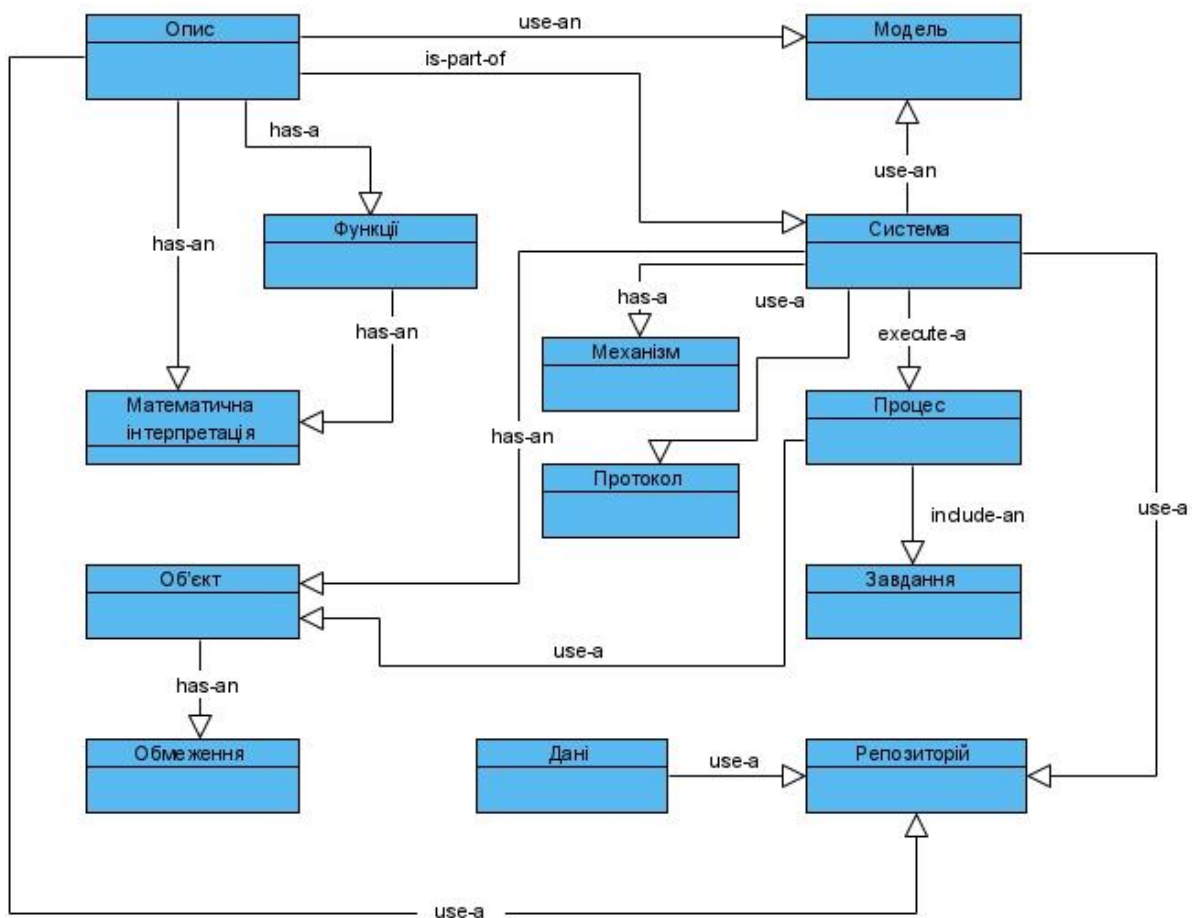


Рисунок 1 – Загальна схема використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів

На рисунку 2 представлено основні етапи процесу розробки програмної системи математичного моделювання з використання онтології математичного моделювання на основі інтервального аналізу.

Процес розробки онто-керованої системи включає наступні кроки:

1) Визначення основних концептів предметної області. Першим кроком у процесі розробки програмного забезпечення з використанням конкретної онтологічної моделі для конкретної предметної області. Існують різні методи, які використовуються для отримання знань з джерел. Ці методи поділяються на три типи: ручні, такі як [7], напівавтоматичні, такі як [7], [8], та автоматичні, такі як [13]. Результатом цього кроку є набір основних понять, які використовуються для опису математичного моделювання на основі інтервальних даних.

2) Визначення понять, які використовуються для опису компонентів предметної області.

3) Визначення екземплярів вилучених понять;

4) визначення зв'язків між поняттями.

5) визначення атрибутів понять.

б) визначення обмежень, які описують умови та обґрунтування.

7) конструкція системи математичного моделювання на основі інтервальних даних з використанням напрацьованої онтологічної моделі.

На останньому кроці детально пояснюється процес побудови системи. Така система є результатом поєднання загальної онтологічної моделі та описів досліджуваної предметної області, які використовуються для опису системи в цілому.

Системний архітектор, який проектує архітектуру, відіграє значну роль у визначенні основних складових. Системний аналітик предметної області має знання та досвід, які використовуються в процесі розробки системи. Однак ці знання та досвід не задокументовані в архітектурі, а вбудовані в її загальну концепцію.

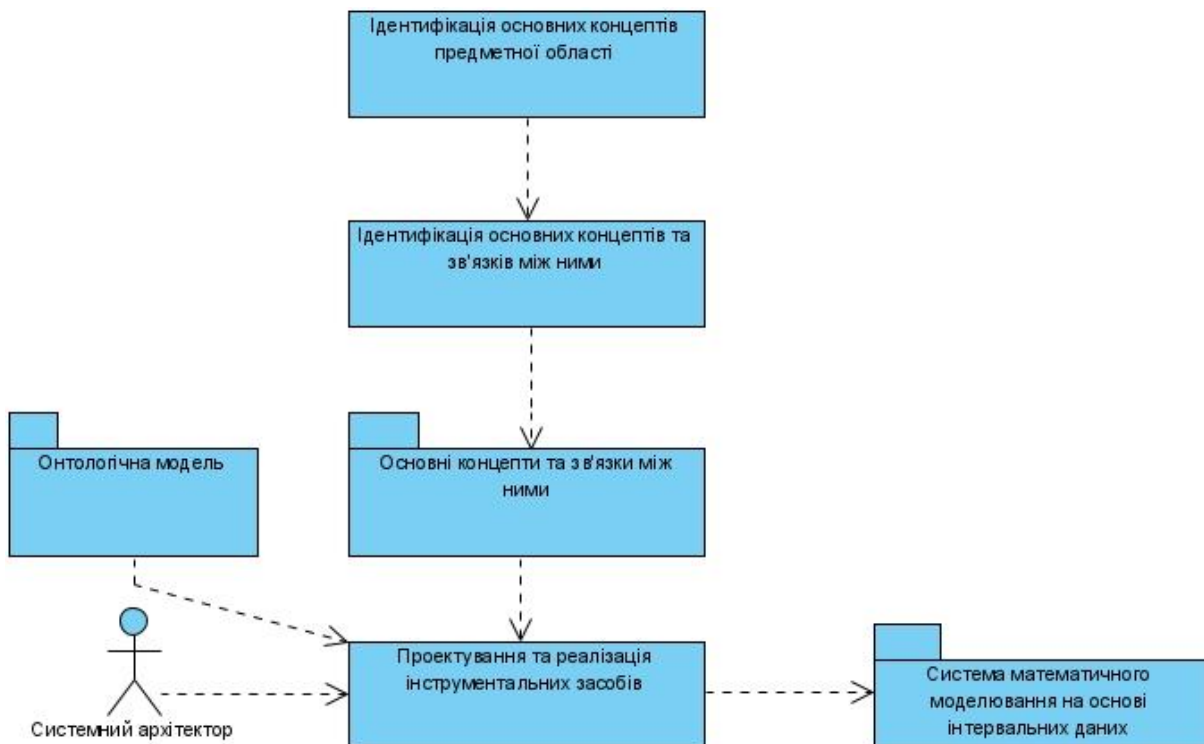


Рисунок 2 – Основні етапи процесу розробки програмної системи математичного моделювання з використанням онтології математичного моделювання на основі інтервального аналізу

Основна мета онтологічного представлення, як надбудови до програмної системи для моделювання на основі інтервального аналізу представляє собою набір множин, які використовуються для опису компонентів, зв'язків і обмежень в рамках досліджуваної предметної області в організований і структурований спосіб. Таке представлення також формує визначений набір понять та їх описових представлень для архітекторів і розробників програмного забезпечення. Онтологічні представлення допомагають архітекторам і розробникам програмного забезпечення, щоб знайти концепції, відстежуючи взаємозв'язки між ними.

Онтологія математичного моделювання на основі інтервальних даних спрямована на полегшення процесу створення екземплярів архітектури програмної системи з онтокерованою взаємодією. На рисунку 3 представлено схему процесу використання розглянутої онтологічної моделі та її оновлення. Розглянемо детальніше кроки, які описують процес використання онтології.

Крок 1: Визначення користувача системи. Це перший крок, який формується виходячи із визначення вимог до розроблюваної системи.

Крок 2: Визначення вимог до системи від користувачів.

Крок 3: Визначення можливої концепції та зв'язку між ними з вимог системи.

Крок 4: Порівняння вилучених понять з основними концепціями онтології.

Якщо концепції онтології відповідають визначеним поняттям, то визначаємо інші концепції, простеживши взаємозв'язки ідентифікованих понять. Для перевірки узгодженості між основними та суміжними поняттями використовується техніка онтологічного міркування [7,10].

Якщо концепції онтології не перекривають досліджувану предметну область, то виконуємо наступну послідовність кроків:

- визначаємо нове поняття;
- визначаємо екземпляри нового поняття, які будуть представлені як індивіди в онтології.
- визначаємо атрибути нових понять, які будуть представлені як властивості даних в онтології.
- визначаємо обмеження для нових понять.
- оновлюємо загальну онтологічну модель, додавши нові концепції до існуючої з її атрибутами, екземплярами, зв'язками та обмеженнями. Розробник онтології оновлює її, додавши нові концепції та визначивши відношення між ними.

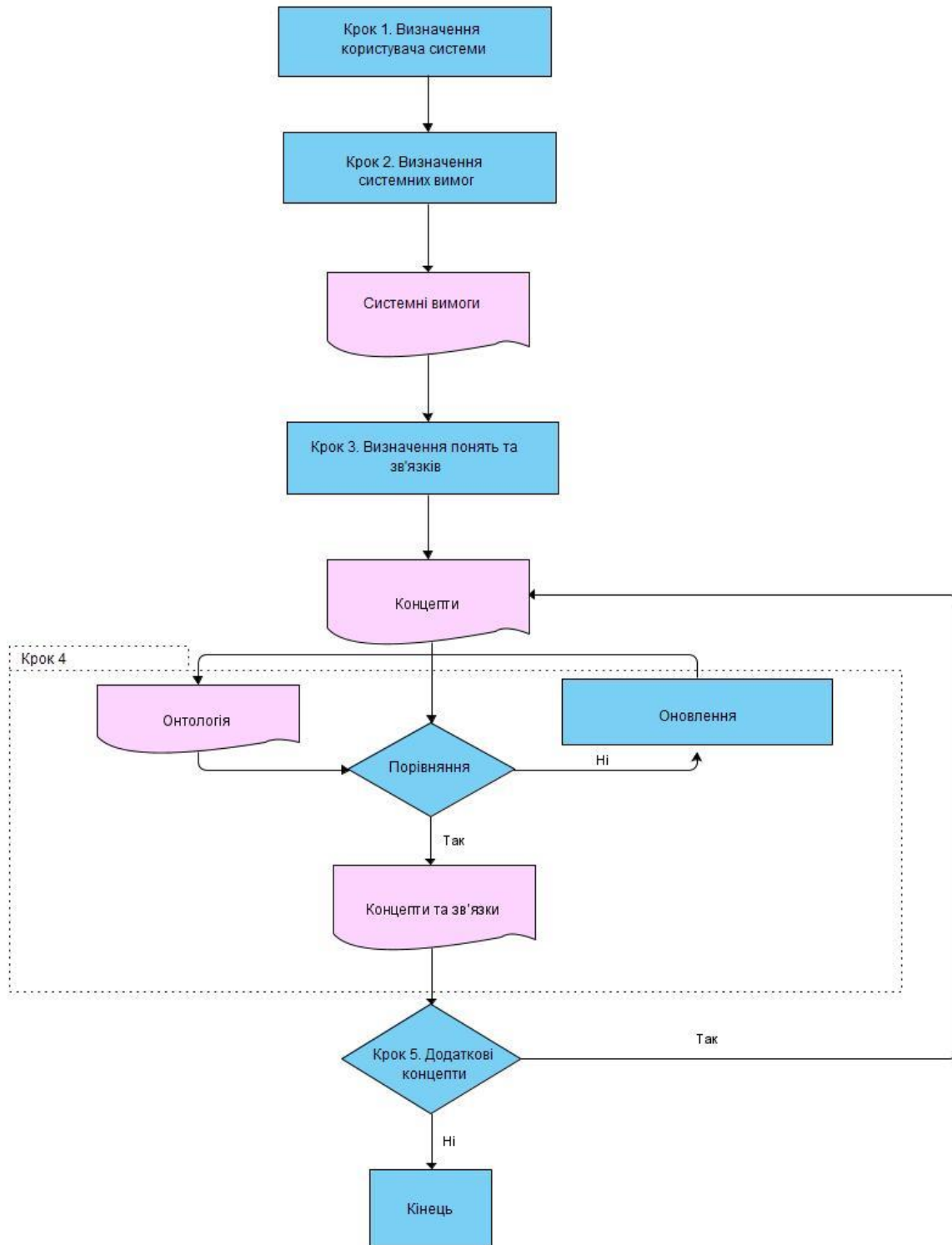


Рисунок 3 – Загальна схема використання онтології математичного моделювання на основі інтервальних даних та її оновлення

Крок 5: Повторюємо крок 4 до того моменту, поки не розглянемо всі поняття, включаючи їх опис та відповідні зв'язки.

Експериментальні дослідження

Розглянемо приклад, який ілюструє процес імплементації онтології математичного моделювання на основі інтервального аналізу для моделювання динаміки концентрацій шкідливих викидів оксиду вуглецю на певній території міста та існуючого сховища подібних моделей, схему застосування методу вибору математичної моделі для моделювання на основі інтервальних даних і те, як онтологія надає опис основних понять досліджуваної предметної області розробникам системи.

Запропонований процес використання онтологічної моделі був апробований для проектування та реалізації веб-орієнтованої програмної системи для моделювання шкідливих викидів, скріншот якої візуально представлено на рисунку 4.

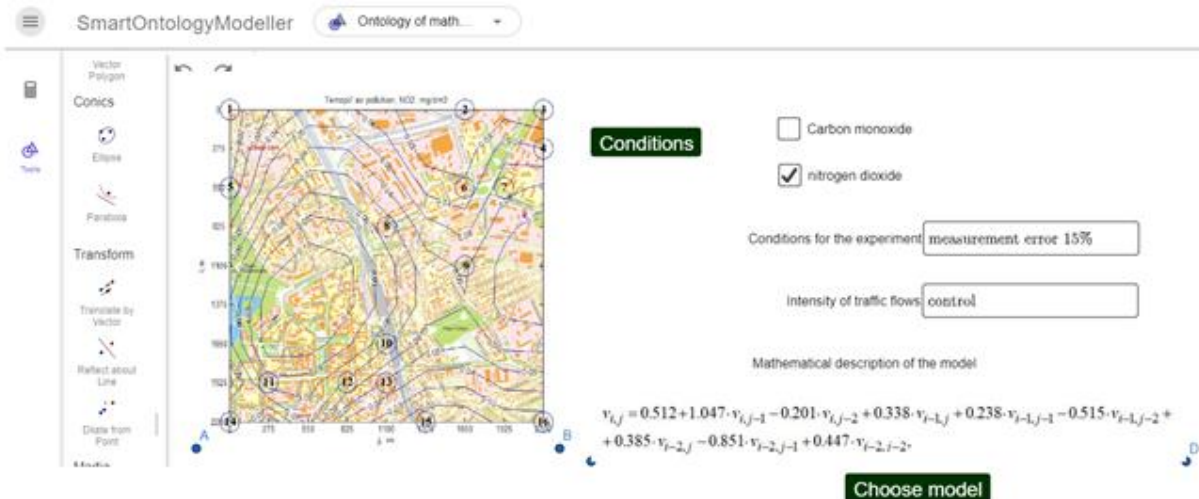


Рисунок 4 – Система для моделювання шкідливих викидів оксиду вуглецю на певній території міста

Дослідник проаналізував предметну область, переглянувши її, щоб виділити основні концепти та зв'язки між ними. Розглянемо цей процес детальніше:

- Система включає вісім основних підсистем, кожна з яких має різні функції. Такими підсистемами є інтерфейс користувача, механізм моделювання, механізм візуалізації, збереження даних, мережа, інтерпретатор математичних команд, семантичний аналізатор і репозиторій математичних моделей. Рисунок 5 ілюструє систему для моделювання шкідливих викидів оксиду вуглецю на певній території міста.

Підсистеми використовують різні ресурси:

- Користувачі запускають систему на різному обладнанні, такому як комп'ютери та мобільні пристрої.

- Користувачі використовують різні протоколи передачі даних для доступу до системи моделювання на основі інтервального аналізу.

- Для представлення архітектури системи використовується багатoshаровий архітектурний стиль.

- Система використовує інтерпретатор математичних команд та семантичний аналізатор для вибору математичних моделей з відповідного репозиторію.

Зв'язок між підсистемами:

А. Підсистема інтерфейсу користувача підключається до підсистеми з репозиторієм математичних моделей, підсистеми моделювання, і підсистеми збереження та візуалізації даних.

В. Підсистема з інтерпретатором математичних команд підключається до репозиторію математичних моделей, механізму моделювання та візуалізації даних.

С. Підсистема семантичний аналізатор підключається до мережі та репозиторію математичних моделей і підсистеми візуалізації результатів.

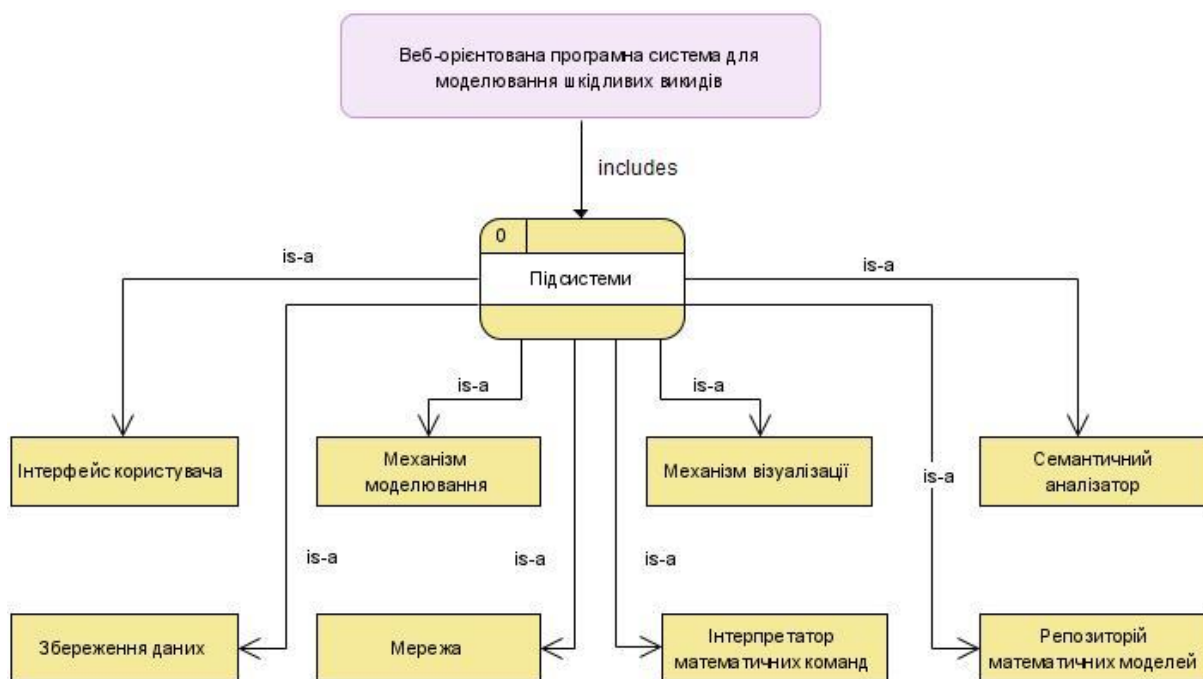


Рисунок 5 – Архітектура програмної системи для моделювання шкідливих викидів оксиду вуглецю на певній території міста

Розглянемо детальніше функції підсистем системи для моделювання шкідливих викидів оксиду вуглецю на певній території міста:

А. Функціями підсистеми «Інтерфейс користувача» (рисунок 6) є:

- 1 – Підключення користувача до підсистеми математичного моделювання.
- 2 – Надає такі функції, як панель інструментів для вибору та налаштування математичних моделей, візуальний прогрес моделювання, візуалізація результатів моделювання, опрацювання та завантаження даних для експериментальних досліджень, налаштування та друк.

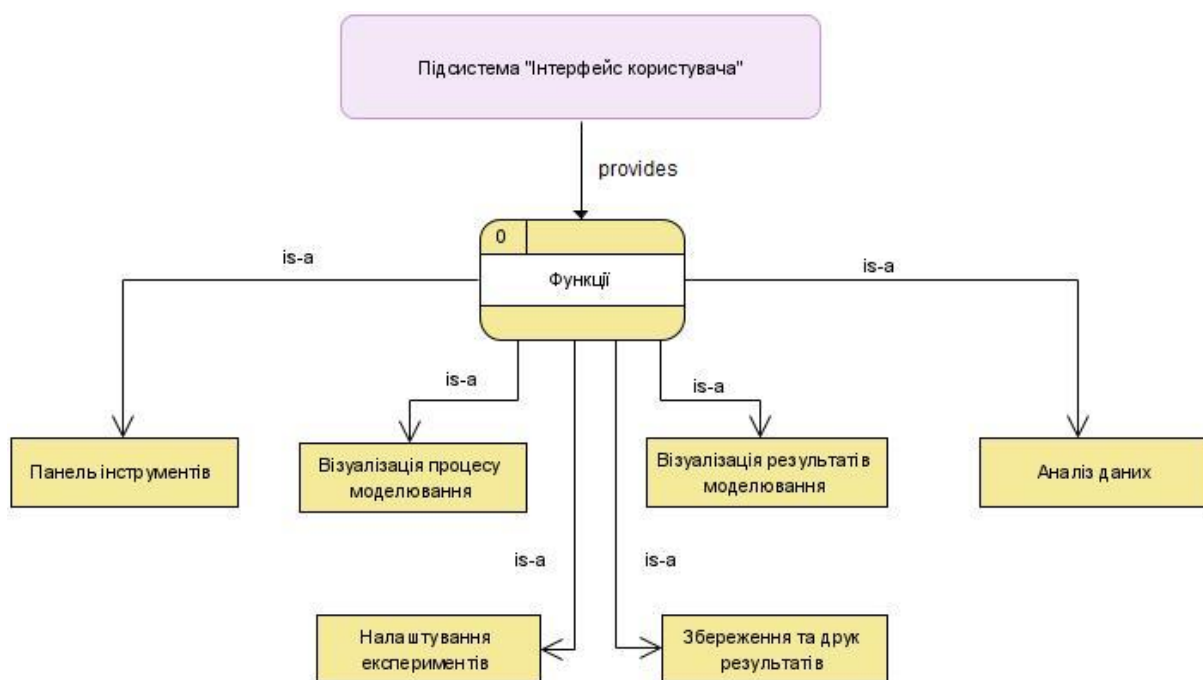


Рисунок 6 – Особливості підсистеми інтерфейсу користувача

В. Функціями підсистеми «Механізм моделювання» є:

- 1 – Забезпечення інтерфейсу високого рівня до підсистеми механізму моделювання.
- 2 – Завантаження репозиторію з математичними моделями.

- 3 – Підтримка процесу налаштування параметрів моделі.
- 4 – Забезпечення перемикачів для перегляду сеансу моделювання.
- 5 – Реалізація запитів та маніпуляції з налаштуваннями механізму моделювання.

C. Функціями підсистеми «Механізм візуалізації»:

1 – Створення візуального представлення вибору параметрів візуалізації процесу та відображення результатів моделювання.

2 – Відображення різноформатних файлів для збереження результатів моделювання.

3 – Розрахунок точного макету результатів моделювання.

D. Функціями підсистеми «Мережі» є:

1 – Реалізація протоколів передачі файлів, такі як HTTP і FTP.

2 – Опрацювання кешу нещодавно отриманих ресурсів.

E. Функція підсистеми «Семантичний аналізатор»:

1 – Інтерпретація семантичних інструкцій в програмні команди.

F. Функція підсистеми «Збереження даних»:

1 – Можливість вибору типів файлів для збереження результатів моделювання.

G. Функціями підсистеми «Репозиторій математичних моделей» є:

1 – Семантично-інтерпретоване відображення множини математичних моделей для вибраної предметної області конкретного об'єкту моделювання.

2 – Вибір моделей.

3 – Інтерпретація моделей в зовнішнє середовище моделювання.

H. Функція підсистеми «Збереження даних»:

1 – Зберігання різних даних, які пов'язані з сеансом моделювання.

Виходячи із наведеного вище аналізу можна отримати онтологічний концептуальний словник системи математичного моделювання на основі інтервальних даних для моделювання шкідливих викидів оксиду вуглецю, фрагмент якого представлений в таблиці 1.

Таблиця 1 – Поняття, які описують об'єкти програмної системи моделювання на основі інтервального аналізу

Словник			
Математичне моделювання	Механізм моделювання	Інтерпретатор математичних команд	Репозиторій математичних моделей
Візуалізація результатів моделювання	Мережа	Семантичний аналізатор	Аналізатор даних
Формат даних	Типи файлів	Інтерпретація семантичних інструкцій	Сеанс моделювання
Збереження даних	Параметри моделі	Методи ідентифікації	Об'єкт моделювання

У таблиці 2 представлено можливі типи зв'язків між цими об'єктами, що дозволяє встановити відповідні залежності для їх подальшого аналізу та використання.

Таблиця 2 – Можливі типи зв'язків між концептами програмної системи моделювання на основі інтервального аналізу

Словник			
Доступ до	Дозволити	Застосувати	Розрахувати
Підключитися до	Показати	Оцінити	Виконати
Має	Реалізує	Включає	Завантажує
Опрацьовує	Виробляє	Надає	Надає функцію для
Представлений як	Зберігає в	Підтримує в	Використовується
Підключений до	Виконати з	Використати з	Зберегти до

Використовуючи дані, які представлені в таблиці 1 та 2 можна побудувати онтологічний граф залежностей між поняттями для досліджуваної предметної області. Таке використання онтології дозволяє зпростити процес використання системи як окремими дослідниками в галузі математичного моделювання, так і розробниками програмного забезпечення, які будуть в подальшому масштабувати та розширювати функціонал системи.

Майбутні дослідження

Подальші дослідження в рамках запропонованих підходів будуть зосереджуватися на розробленні в межах теорії ідентифікації методах структурної та параметричної ідентифікації цих моделей на основі

аналізу інтервальних даних, використання онтологічних описів предметних областей для яких будуються моделі та оптимізаційних процедур на основі інтелектуальних обчислень, що використовують поведінкові моделі штучних бджолиних колоній.

Таке поєднання відомих підходів забезпечить підвищення ефективності обчислювальних процедур ідентифікації моделей складних об'єктів, а також адаптивне використання різнотипних моделей для різних предметних областей в системах підтримки прийняття рішень.

Висновки

В роботі розкрито проблему розроблення методів та засобів побудови дискретних моделей складних об'єктів у вигляді інтервальних різницевих рівнянь на основі поєднання онтологічного підходу та аналізу інтервальних даних для розширення сфери та умов застосування моделей при забезпеченні її заданих прогностичних властивостей, розв'язування якої слугує поштовхом для розвитку прикладних досліджень у сферах оборони країни, охорони довкілля, медицини та інших галузях.

Описано підхід до використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів. Виходячи із запропонованого підходу, реалізовано схему використання онтології математичного моделювання на основі інтервальних даних для розробки та використання програмних засобів. Особливістю запропонованого підходу є те, що він може бути реалізований як програмна надбудова до прикладних систем математичного моделювання на основі інтервального аналізу.

Список літератури

- [1] М. П. Дивак, Н. П. Порплиця, Т. М. Дивак, *Ідентифікація дискретних моделей систем з розподіленими параметрами на основі аналізу інтервальних даних: монографія*. Тернопіль, Україна: Економічна думка ТНЕУ, 2018, 220 с.
- [2] М. П. Дивак, *Задачі математичного моделювання статичних систем з інтервальними даними: монографія*. Тернопіль, Україна: Економічна думка ТНЕУ, 2011, 215 с.
- [3] М. П. Дивак, А. В. Пукас, Н. П. Парплиця, А. М. Мельник, *Прикладні задачі структурної та параметричної ідентифікації інтервальних моделей складних об'єктів: монографія*. Тернопіль, Україна: Університетська думка, 2021, 212 с.
- [4] H. Madala, A. Ivakhnenko, "Inductive Learning Algorithms for Complex Systems Modelling," Boca Raton: CRC Press. 1994.
- [5] A. Ivakhnenko, G. Ivakhnenko, "The Review of Problems Solvable by Algorithms of the Group Method of Data Handling (GMDH)," *Pattern Recognition and Image Analysis*, 5 (4), pp. 527–535. 1995.
- [6] A. Ivakhnenko, V. Lapa, "Cybernetics and Forecasting Techniques," *Modern Analytic and Computational Methods in Science and Mathematics*, v.8 ed. American Elsevier. 1967.
- [7] SW. Tu, H. Eriksson, JH. Gennari, Y. Shahar, MA. Musen, "Ontology-based configuration of problem-solving methods and generation of knowledge-acquisition tools: application of PROTEGE-II to protocol-based decision support," *Artif Intell Med.*, 7(3), pp. 257-89. 1995. doi: 10.1016/0933-3657(95)00006-r. PMID: 7581625.
- [8] A. Sattar, E. Salwana, M. Surin, M. Ahmad, M. Ahmad, A. Mahmood, "Comparative Analysis of Methodologies for Domain Ontology Development: A Systematic Review," *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(5). 2020. doi: 10.14569/IJACSA.2020.0110515.
- [9] M. Musen, "The protégé project. AI Matters," 1, pp. 4-12. 2015. doi: 10.1145/2757001.2757003.
- [10] U. Itziar, M. Nieto, M. García, O. Otaegui, "Design and Implementation of an Ontology for Semantic Labeling and Testing: Automotive Global Ontology (AGO)," *Applied Sciences*, 11, no. 17: 7782. 2021. doi: 10.3390/app11177782.
- [11] M. Dyvak, O. Papa, A. Melnyk, A. Pukas, N. Porplytsya, A. Rot, "Interval Model of the Efficiency of the Functioning of Information Web Resources for Services on Ecological Expertise," *Mathematics*, 8, 2116. 2020. doi: 10.3390/math8122116
- [12] O. Androshchuk, R. Berezenskyi, O. Lemeshko, A. Melnyk, O. Huhul, "Model of Explicit Knowledge Management in Organizational and Technical Systems," *International Journal of Computing*, 20(2), pp. 28-36. 2021.
- [13] A. Melnyk, R. Pasichnyk, "System of semantic classes for test's generation," in *2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2010, pp. 206-206.
- [14] R. Pigazzi, C. Confalonieri, M. Rossoni, E. Gariboldi, G. Colombo, "Ontologies As a Tool for Design and Material Engineers," in *Proceedings of the ASME 2020 International Mechanical Engineering Congress and Exposition*. Vol. 6: Design, Systems, and Complexity. Virtual, Online. <https://doi.org/10.1115/IMECE2020-24042>, 2020.

- [15] A. Kovbasisty, A. Melnyk, M. Dyvak, V. Brych and I. Spivak, "Method for detection of non-relevant and wrong information based on content analysis of web resources," *2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, 2017, pp. 154-156, doi: 10.1109/MEMSTECH.2017.7937555.
- [16] M. Dyvak, A. Melnyk and Y. Kedrin, "Interval model of the user reactions to messages in thematic groups of social networks," *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 837-840, doi: 10.1109/TCSET55632.2022.9766857.
- [17] M. Dyvak, A. Pukas, A. Melnyk, I. Voytyuk, S. Valchyshyn and I. Romanets, "Software Architecture for Modeling the Interval Static and Dynamic Objects," *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 2021, pp. 572-575, doi: 10.1109/ACIT52158.2021.9548577.
- [18] S. Mazepa, S. Banakh, A. Melnyk, S. Pugach, O. Yavorska and N. Golota, "An Ontological Approach to Detecting Fake News in Online Media," *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 2021, pp. 531-535, doi: 10.1109/ACIT52158.2021.9548394.
- [19] М. П. Дивак, А. М. Мельник, О. А. Папа, "Математичне та програмне забезпечення інтелектуального модуля прикладних програмних систем для надання адміністративних послуг щодо проведення екологічної експертизи," *Інформаційні технології та комп'ютерна інженерія*, 49(3), с. 66–76. 2020.
- [20] М. П. Дивак, А. М. Мельник, А. В. Ковбасистий, О. А. Папа, "Підхід до математичного моделювання ефективності web-ресурсів," *Оптико-електронні інформаційно-енергетичні технології*, 38, 2 (Бер 2020), с. 29–37. 2020.

Стаття надійшла: 22.05.2022.

References

- [1] М. Р. Dyvak, N. Р. Porplytsia, Т. М. Dyvak, *Identyfikatsiia dyskretnykh modelei system z rozpodilenyu parametramy na osnovi analizu intervalnykh danykh: monohrafiia*. Ternopil, Ukraina: Ekonomichna dumka TNEU, 2018, 220 s. [in Ukrainian].
- [2] М. Р. Dyvak, *Zadachi matematychnoho modeliuвання statychnykh system z intervalnyu danymy: monohrafiia*. Ternopil, Ukraina: Ekonomichna dumka TNEU, 2011, 215 s. [in Ukrainian].
- [3] М. Р. Dyvak, А. V. Pukas, N. Р. Parplytsia, А. М. Melnyk, *Prykladni zadachi strukturnoi ta parametrychnoi identyfikatsii intervalnykh modelei skladnykh ob'ektiv: monohrafiia*. Ternopil, Ukraina: Universytetska dumka, 2021, 212 s. [in Ukrainian].
- [4] H. Madala, A. Ivakhnenko, "Inductive Learning Algorithms for Complex Systems Modelling," Boca Raton: CRC Press. 1994.
- [5] A. Ivakhnenko, G. Ivakhnenko, "The Review of Problems Solvable by Algorithms of the Group Method of Data Handling (GMDH)," *Pattern Recognition and Image Analysis*, 5 (4), pp. 527–535. 1995.
- [6] A. Ivakhnenko, V. Lapa, "Cybernetics and Forecasting Techniques," *Modern Analytic and Computational Methods in Science and Mathematics*, v.8 ed. American Elsevier. 1967.
- [7] SW. Tu, H. Eriksson, JH. Gennari, Y. Shahar, MA. Musen, "Ontology-based configuration of problem-solving methods and generation of knowledge-acquisition tools: application of PROTEGE-II to protocol-based decision support," *Artif Intell Med.*, 7(3), pp. 257-89. 1995. doi: 10.1016/0933-3657(95)00006-r. PMID: 7581625.
- [8] A. Sattar, E. Salwana, M. Surin, M. Ahmad, M. Ahmad, A. Mahmood, "Comparative Analysis of Methodologies for Domain Ontology Development: A Systematic Review," *International Journal of Advanced Computer Science and Applications (IJACSA)*, 11(5). 2020. doi: 10.14569/IJACSA.2020.0110515.
- [9] M. Musen, "The protégé project. AI Matters," 1, pp. 4-12. 2015. doi: 10.1145/2757001.2757003.
- [10] U. Itziar, M. Nieto, M. García, O. Otaegui, "Design and Implementation of an Ontology for Semantic Labeling and Testing: Automotive Global Ontology (AGO)," *Applied Sciences*, 11, no. 17: 7782. 2021. doi: 10.3390/app11177782.
- [11] M. Dyvak, O. Papa, A. Melnyk, A. Pukas, N. Porplytsya, A. Rot, "Interval Model of the Efficiency of the Functioning of Information Web Resources for Services on Ecological Expertise," *Mathematics*, 8, 2116. 2020. doi: 10.3390/math8122116
- [12] O. Androshchuk, R. Berezenskyi, O. Lemeshko, A. Melnyk, O. Huhul, "Model of Explicit Knowledge Management in Organizational and Technical Systems," *International Journal of Computing*, 20(2), pp. 28-36. 2021.
- [13] A. Melnyk, R. Pasichnyk, "System of semantic classes for test's generation," in *2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2010, pp. 206-206.

- [14] R. Pigazzi, C. Confalonieri, M. Rossoni, E. Gariboldi, G. Colombo, "Ontologies As a Tool for Design and Material Engineers," in *Proceedings of the ASME 2020 International Mechanical Engineering Congress and Exposition*. Vol. 6: Design, Systems, and Complexity. Virtual, Online. <https://doi.org/10.1115/IMECE2020-24042>, 2020.
- [15] A. Kovbasisty, A. Melnyk, M. Dyvak, V. Brych and I. Spivak, "Method for detection of non-relevant and wrong information based on content analysis of web resources," *2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, 2017, pp. 154-156, doi: 10.1109/MEMSTECH.2017.7937555.
- [16] M. Dyvak, A. Melnyk and Y. Kedrin, "Interval model of the user reactions to messages in thematic groups of social networks," *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 837-840, doi: 10.1109/TCSET55632.2022.9766857.
- [17] M. Dyvak, A. Pukas, A. Melnyk, I. Voytyuk, S. Valchyshyn and I. Romanets, "Software Architecture for Modeling the Interval Static and Dynamic Objects," *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 2021, pp. 572-575, doi: 10.1109/ACIT52158.2021.9548577.
- [18] S. Mazepa, S. Banakh, A. Melnyk, S. Pugach, O. Yavorska and N. Golota, "An Ontological Approach to Detecting Fake News in Online Media," *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 2021, pp. 531-535, doi: 10.1109/ACIT52158.2021.9548394.
- [19] M. P. Dyvak, A. M. Melnyk, O. A. Papa, "Matematychno ta prohramne zabezpechennia intelektualnoho moduliu prykladnykh prohramnykh system dlia nadannia administratyvnykh posluh shchodo provedennia ekolohichnoi ekspertyzy," *Informatsiini tekhnolohii ta kompiuterna inzheneriia*, 49(3), s. 66–76. 2020 [in Ukrainian].
- [20] M. P. Dyvak, A. M. Melnyk, A. V. Kovbasisty, O. A. Papa, "Pidkhid do matematychnoho modeliuвання efektyvnosti web-resursiv," *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, 38, 2 (Ber 2020), s. 29–37. 2020 [in Ukrainian].

Відомості про авторів

Мельник Андрій Миколайович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук.

A. M. Melnyk

ONTOLOGY AS A SOFTWARE ADDITION TO THE SYSTEM FOR MATHEMATICAL MODELING ON THE BASIS OF INTERVAL DATA

West Ukrainian National University, Ternopil

УДК 004.652

С. В. Осієвський, О. Ю. Несміян

СИНТЕЗ СИСТЕМИ КЕРУВАННЯ АЛОФОННИМИ БАЗАМИ ДАНИХ ДЛЯ ОРГАНІЗАЦІЇ ВЗАЄМОДІЇ ОПЕРАТОРА АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ ПОВІТРЯНИМ РУХОМ (АС КПр) З КОМПЛЕКСОМ ЗАСОБІВ АВТОМАТИЗАЦІЇ (КЗА)

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

Анотація. У статті розглянуті особливості реалізації сховищ даних і їх обмеження, а також описана послідовність представлення даних в абстрактній предметній області, які дозволяють запропонувати деякий альтернативний підхід до організації сховищ даних, орієнтований на використання контейнерів. Даний підхід поєднує в собі переваги реляційних баз даних з їх можливістю забезпечення консистентності даних в будь-який момент часу, а також особливості безструктурного зберігання даних, характерних в цілому для NoSQL систем. Також запропоновані шляхи вирішення задачі синтезу системи керування алофонними базами даних для організації взаємодії оператора АС КПр з КЗА. В основу організації покладено ряд правил, що дозволяють побудувати схему неструктурованих даних, організувати взаємодію бази даних NoSQL з існуючими реляційними рішеннями в основу якої покладено положення теорії категорій. Розроблені правила забезпечують можливість здійснення фізичного та логічного моделювання баз даних NoSQL. Також розроблено стандарти кардинальності для моделювання баз даних NoSQL та введено класифікацію з визначенням пріоритетів класів і настанов щодо моделювання NoSQL. Перевірку запропонованих рішень було здійснено шляхом моделювання та порівняння отриманих результатів з теоретичними положеннями. Розроблено SO-model та обґрунтовано її властивості. Особливістю SO-model являється те, що кожен об'єкт має свій глобальний унікальний ідентифікатор U_{unqid} , що дозволяє зберігати об'єкти одного типу на різних комп'ютерах за рахунок чого підвищити масштабованість сховища даних. Отримані результати свідчать про значне вдосконалення схеми даних неструктурованих та слабоструктурованих баз даних. Запропоновану модель сховища даних за рахунок її властивості уніфікації структури, яка враховує динаміку даних і їх зв'язків, можна розвивати в різних напрямках, використовуючи NoSQL рішення.

Ключові слова: бази даних NoSQL, моделювання баз даних, схеми великих даних, бази даних зберігання документів.

Abstract. The article describes data warehouses implementation peculiarities and their limitations, as well as describing the sequence of data presentation in an abstract subject area, which allows us to propose some alternative approach to the organization of data warehouses, focused on containers usage. This approach combines the advantages of relational databases with their ability to ensure data consistency at any point in time, as well as features of unstructured data storage, typical of NoSQL systems in general. Also, the article proposes ways to solve the problem of synthesis of allophone database management system for organization of interaction between AC ACS operator and ACM. The method is based on a number of rules that allow to build a scheme of unstructured data, to organize the interaction of the NoSQL database with existing relational solutions, which is based on the provisions of the category theory. The developed rules provide the possibility of physical and logical modeling of NoSQL databases. Cardinality standards for NoSQL database modeling have also been developed and a classification has been introduced to prioritize classes and guidelines for NoSQL modeling. The verification of the proposed solutions was carried out by modeling and comparing the obtained results with theoretical positions. The SO-model was developed and its properties were substantiated. A feature of the SO-model is that each object has its own global unique identifier U_{unqid} , which allows you to store objects of the same type on different computers, thereby increasing the scalability of the data store. Obtained results indicate a significant improvement of the data scheme of unstructured and poorly structured databases. The proposed model of data storage, due to its property of unifying the structure, which takes into account the dynamics of data and their connections, can be developed in various directions using NoSQL solutions.

Keywords: NoSQL databases, database modeling, big data schemes, document storage databases.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-39-46>.

Вступ

В даний час, в науковому середовищі, виникає досить велика кількість диспутів щодо питання зберігання та обробки різнорідних (неструктурованих) даних.

При цьому, якщо вести мову про структуровані дані, то традиційні бази даних, в даний час, забезпечують реалізацію всіх технічних рішень в КЗА, це підтверджується роботами [7-11]. Зокрема вони забезпечують централізований контроль даних, усунення невідповідностей та надмірність контролю [1]. Поява великих та неструктурованих даних з їх нетрадиційними характеристиками та слабоструктурованих даних, що вимагають спільного зберігання та обробки зумовили необхідність створення гнучких, масштабованих та прихованих баз даних – NoSQL [2-4].

Термін NoSQL не введено як повноцінну заміну SQL та традиційних баз даних, він призначений заповнити прогалини, що утворилися внаслідок постійного розширення розміру, складності, різноманітності та мінливості даних.

Актуальність теми

З метою отримання адекватних рішень, щодо забезпечення вимог до обробки та використання даних, проведено аналіз існуючих рішень та провідних наукових досліджень, зокрема: в роботі [5] запропоновано використання нових позначень та стилів кардинальності, в роботі [6] розроблені та запропоновані до використання пропозиції щодо моделювання баз даних та особливостей зберігання документів

NoSQL. Результати цих досліджень дають можливість провести поточне дослідження в аспекті дослідження семантичного відображення сутностей та пріоритетності відношень.

Рішення, які пропонуються, відображені в моделі, що віддзеркалює структури схеми для баз даних зберігання документів NoSQL. Ця модель спрямована на подальше спрощення процесу моделювання NoSQL.

Першим рішенням вищезгаданої задачі було встановлення стандартів кардинальності для моделювання баз даних NoSQL. Другим рішенням являється класифікація та визначення пріоритетів класів та настанов щодо моделювання NoSQL. Ці рішення вимагають значно високого рівня знань, тим самим мотивуючи використання положень, що запропоновані для вирішення задачі синтезу системи керування алофонними базами даних для організації взаємодії оператора АС КПП з КЗА.

Мета

Грунтуючись на завданнях, що потребують вирішення визначено за мету розробку науково – теоретичного апарату, що дозволить досягти підтримання темпоральності на рівні зв'язків між сутностями ER-моделі за рахунок відсутності обмеження на підтримання такої цілісності даних в базовому функціоналі SO-model. Досягнення зазначеної мети дозволить знайти рішення задачі синтезу системи керування алофонними базами даних для організації взаємодії оператора АС КПП з КЗА.

Задачі

Виходячи з вищезазначених існуючих рішень та теоретичних положень теорії побудови БД, рішення основної задачі вбачається в послідовній реалізації наступних етапів:

- розробка правил локалізації характеристик об'єктів алофонної БД;
- розробка конструкторів об'єктів алофонної БД;
- розробка SO-моделі реалізації керуючих функцій алофонних БД для організації керування алофонними БД.

Розв'язання задач

В сучасному світі швидкість доступу до інформації стає вкрай важливим фактором. Задля підвищення швидкості доступу до інформації було розроблено низку нових підходів до зберігання даних, у тому числі NoSQL БД, які зарекомендували себе як надійні, швидкі БД які легко масштабуються [12]. Проте, такі рішення мають один суттєвий недолік – відсутність контролю консистентності даних.

Для отримання кращого результату по швидкості і консистентності пропонується використання ER-моделей у NoSQL рішеннях. Доведемо, що будь-яка ER-модель може бути реалізована в SO-модель.

Можливі два варіанти первинного ключа однієї сутності. Вони представлені на рисунку 1. Сформуємо правила роботи з первинними ключами таких сутностей

Правило 1. Первинний ключ сутності (Entity₁) є простим (рисунок 1(a)). Така сутність відповідає множині об'єктів в SO-model. Кожен екземпляр сутності відображається в відповідний об'єкт SO-model. Всі об'єкти цього множини мають однаковий тип – ім'я сутності. Атрибут (Attribute₁) – первинний ключ задає ім'я об'єкта, всі інші атрибути задають властивості об'єкта.

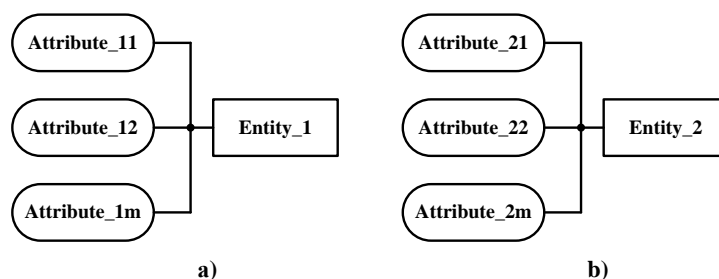


Рисунок 1 – Одна сутність

Позначимо:

Entity_j.Name – ім'я j -ї сутності (Entity _{j} , $j = 1, 2$), відповідає типу об'єкта;

Attribute_{jk}.Name – ім'я k -го атрибута j -ї сутності;

Attribute_{jk}.Value – значення k -го атрибута j -ї сутності;

time_j – момент часу початку існування сутності і її властивостей;

m – кількість атрибутів сутності, а також кількість властивостей об'єктів відповідного типу;

n – кількість примірників сутності, а також кількість об'єктів відповідного типу;

$U_{unqID_{obji}}$ – унікальний ідентифікатор i -го об'єкта;

$U_{unqID_{p,ik}}$ – унікальний ідентифікатор k -ї властивості i -го об'єкта.

Тоді множина об'єктів SO-model будується наступним чином:

$$\left\{ \left\langle U_{unqID_{obji}}, Entity_j.Name, P_i, \langle Attribute_{jk}.Value, time_j \rangle \right\rangle_{i=1, \dots, n} \right\}$$

$$\forall i: P_i = \left\{ \left\langle U_{unqID_{p,1k}}, Attribute_{1k}.Name, \left\{ \langle Attribute_{1k}.Value, null, time_1 \rangle \right\} \right\rangle_{k=2..m} \right\}$$

Правило 2. Є одна сутність (Entity_2), первинний ключ якої є складовим – наприклад, складається з атрибутів Attribute_21, Attribute_22 (рисунок 1 (b)). В цьому випадку відображення будується аналогічно попередньому випадку, за винятком імені об'єкта, яке можна побудувати з'єднанням частин складеного ключа, крім цього, кожна частина складеного первинного ключа додається як окрема властивість об'єкта.

$$\left\{ \left\langle U_{unqID_{obji}}, Entity_2.Name, P_i \left\langle Attribute_{21}.Value : Attribute_{22}.Value, time_1 \right\rangle \right\rangle_{i=1, \dots, n} \right\}$$

$$\forall i: P_i = \left\{ \left\langle U_{unqID_{p,ik}}, Attribute_{2k}.Name, \left\{ \langle Attribute_{2k}.Value, null, time_1 \rangle \right\} \right\rangle_{k=1..m} \right\}$$

Зауважимо, що якщо розглядати статичну SO-модель (значення $time_i$ не змінюється у імені об'єктів і їх властивостей), то побудоване відображення примірників сутностей ER-моделі в об'єкти SO-моделі є бієктивне, тобто можливе взаємно однозначне відображення об'єктів SO-моделі по сутності і екземпляри сутностей ER-моделі.

Правило 3. Рекурсивне відношення ER-моделі даних може бути реалізовано в SO-model.

Можливі види рекурсивних відносин в ER-моделі показані на рисунку 2.

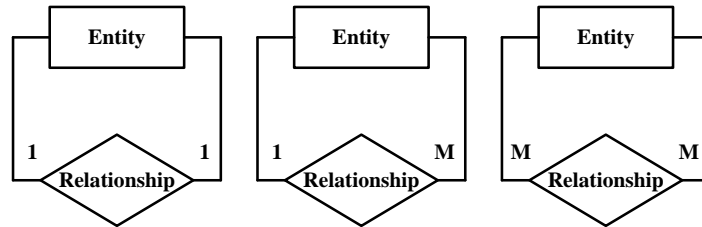


Рисунок 2 – Рекурсивні зв'язки

В базовому функціоналі SO-model відсутній механізм фіксації виду відносин – один до одного, один до багатьох, багато до багатьох. Дане розмежування виду відносин може бути перенесено на програмні додатки по взаємодії зі сховищем. Тому для доказу досить розглянути тільки один вид відносин: багато до багатьох, вважаючи інші види окремими випадками цих відносин з накладеними певними обмеженнями.

Для реалізації рекурсивних відносин багато до багатьох в SO-model в об'єкти, які відповідають екземплярам сутності, крім атрибутів сутності, додається властивість з типом об'єкта. Причому значення цієї властивості, що має посилання, вказує на U_{unqID} об'єкта, який відповідає структурі відносин:

$$\left\{ \left\langle U_{unqID_{obji}}, Entity.Name, P_i \left(Attribute_1.Value, time_1 \right) \right\rangle_{i=1..n} \right\}$$

$$\forall i: P_i = \left\{ \left\langle U_{unqID_{p,ik}}, Attribute_k.Name, \left\{ \langle Attribute_k.Value, null, time_1 \rangle \right\} \right\rangle_{k=1..m} \right\}$$

$$\left\langle \left\langle U_{uniqID_p, i(m+1)}, Entity.Name, \begin{cases} null, \\ U_{uniqIDobj} \\ time_1 \end{cases} \mid T_{obj}(\bar{U}_{obj}(U_{uniqIDobj})) = Entity.Name \right\rangle \right\rangle$$

Правило 4. Зв'язки сутностей ER-моделі даних можуть відобразитися в зв'язку об'єктів в SO-model.

На рисунках 3 – 5 показані можливі види зв'язків між сутностями в ER-моделі даних та модальність зв'язків: подвійна лінія зв'язку – «повинен», одинарна лінія зв'язку – «можливо». Введення обмежень на створення нових об'єктів певного типу, додавання і зміни властивостей об'єктів дозволяють реалізувати всі види зв'язків ER-моделі даних (причому реалізація цих обмежень може бути винесена за рамки базового функціоналу SO-model).

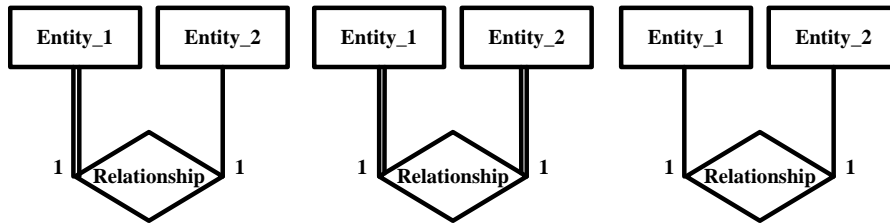


Рисунок 3 – Види зв'язків сутності один до одного

1. Нехай екземпляри сутності «Entity_1» при простому первинному ключі «Attribute_11» відображаються в об'єкти SO-model:

$$\left\langle \left\langle U_{uniqID_{obj}}, Entity_1.Name, P_i \langle Attribute_{11}.Value, time_1 \rangle \right\rangle_{i=1..n} \right\rangle$$

$$P_i = \left\langle \left\langle U_{uniqID_{pk}}, Attribute_{1k}.Name \left\langle \left\langle Attribute_{1k}.Value, null, time_1 \right\rangle \right\rangle_{k=1..m} \right\rangle \right\rangle$$

$F(Object_{ji})$ – зовнішнє правило, що задає наявність зв'язку один до одного для об'єкта, відповідного i -му примірнику j -ї сутності. В цьому випадку об'єкти, відповідні екземплярам «Entity_2», можна виділити із значень первинного ключа примірників «Entity_1» наступним чином:

$$A \Leftarrow Object.Type(Entity_1.Name)$$

$$B \Leftarrow red(Ind[x], if(F(x), x, NULL), X)$$

$$C \Leftarrow Ind[x], Get.Name(x, Attribute_{11}.Name), B$$

$$D \Leftarrow Ind([x], Object.Create(GenU_{uniqID}, Attribute_{11}.Name, Property.Value.Values.Time(x, time)time), C)$$

$$Ind([x, x^*], mod(x \Leftarrow x^*), B, ind([x_1, x_2, x_3], Property.Link.Change(x_1, x_2, x_3, time), B, C, ind([z], z.U_{uniqID}, D)))$$

2. Нехай екземпляри сутності «Entity_1» при складеному первинному ключі «Attribute_11», «Attribute_12» відображаються в об'єкти SO-model:

$$\left\langle \left\langle U_{uniqID_{obj}}, Entity_1Name, P_i \langle Attribute_{11}.Value : Attribute_{12}.Value, time_1 \rangle \right\rangle_{i=1..n} \right\rangle$$

$$P_i = \left\{ \left\langle U_{\text{uniqID}_{pk}}, \text{Attribute}_{1k}.\text{Name} \left\{ \left\langle \text{Attribute}_{1k}.\text{Value}, \text{null}, \text{time}_1 \right\rangle \right\}_{k=1\dots m} \right\rangle \right\}$$

У цьому випадку порядок дій може бути аналогічний попередньому пункту, відмінність полягає в тому, що об'єкти виділяються з кожного атрибута складеного первинного ключа «Entity_1»:

$$A \leftarrow \text{Object.Type}(\text{Entity}_1.\text{Name})$$

$$B \leftarrow \text{red}(\text{Ind}[x], \text{if}(F(x), x, \text{NULL}), X))$$

$$C \leftarrow \text{Ind}[x], \text{Get.Name}(x, \text{Attribute}_{11}.\text{Name}), B$$

$$D \leftarrow \text{Ind}[x], \text{Get.Name}(x, \text{Attribute}_{12}.\text{Name}), B$$

$$E \leftarrow \text{Ind}([x], \text{Object.Create}(\text{GenU}_{\text{uniqID}}, \text{Attribute}_{11}.\text{Name}, \text{Property.Value.Values.Time}(x, \text{time})\text{time}), C)$$

$$F \leftarrow \text{Ind}([x], \text{Object.Create}(\text{GenU}_{\text{uniqID}}, \text{Attribute}_{12}.\text{Name}, \text{Property.Value.Values.Time}(x, \text{time})\text{time}), D)$$

$$\text{Ind}([x, x^*].\text{mod}(x \leftarrow x^*), B, \text{ind}([x_1, x_2, x_3], \text{Property.Link.Change}(x_1, x_2, x_3, \text{time}), B, C, \text{ind}([z], z.U_{\text{uniqID}}, E)))$$

$$\text{Ind}([x, x^*].\text{mod}(x \leftarrow x^*), B, \text{ind}([x_1, x_2, x_3], \text{Property.Link.Change}(x_1, x_2, x_3, \text{time}), B, C, \text{ind}([z], z.U_{\text{uniqID}}, F)))$$

Модальність зв'язків: «Entity_1» – «повинен»; «Entity_2» – «можливо». Надалі дозволяється додавати нові об'єкти в множину об'єктів типу «Entity_2», а також забороняється додавати об'єкти «Entity_1» без виділення нового об'єкта зі значення первинного ключа і додавання його в множину «Entity_2».

Модальність зв'язків: «Entity_1» – «повинен»; «Entity_2» – «повинен».

Порядок дій збігається з попереднім випадком. Однак після виділення об'єктів забороняється додавати нові об'єкти в множину об'єктів типу «Entity_2», а також забороняється додавати об'єкти «Entity_1» без виділення нового об'єкта зі значення первинного ключа і додавання його в множину «Entity_2».

Реалізація зв'язків один до багатьох.

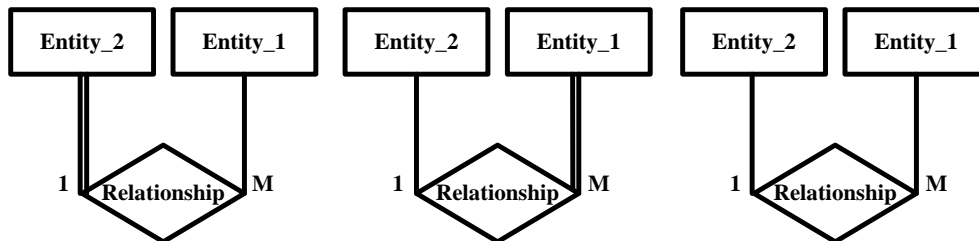


Рисунок 4 – Види зв'язків сутності один до багатьох

Для доказу аналогічно попередньому випадку прийемо угоду про завдання зовнішньої функції $F(\text{Object } j_i)$, що визначає наявність зв'язку для об'єкта. На відміну від зв'язку один до одного в даному випадку різні об'єкти сутності «Entity_1» можуть бути пов'язані з однаковим об'єктом сутності «Entity_2». Тому об'єкти сутності «Entity_2» повинні створюватися в одному екземплярі.

1. У разі простого первинного ключа такий зв'язок може бути реалізований наступним чином (вводиться допоміжна функція $Name_{UnqID}$, яка для заданої множини об'єктів X і заданого імені $name$ на момент часу $time$ формує підмножину унікальних ідентифікаторів об'єктів, які в даний момент часу мають ім'я $name$):

$$A \Leftarrow Object.Type(Entity_1.Name)$$

$$B \Leftarrow red(Ind[x], if(F(x), x, NULL), X)$$

$$Name_{UnqID}(X, name, time) = red\left(ind\left([x] \text{ if } \left(\begin{array}{l} mem(name, xTimeToName(time)), \\ x.U_{unqID}, NULL \end{array} \right), X \right) \right)$$

$$C \Leftarrow Ind([x], Get.Name(x, Attribute_{11}.Name), B)$$

$$\begin{aligned} F \Leftarrow & Object.Type(Attribute_{11}.Name, Property.Value.Values.Time(x, time)time), map[x^*], \\ & mod(Object.U_{unqID}(Property.Object(x)) \leftarrow Property.Link.Change(Property.Object(x), \\ & x, x^*, time)), Name.U_{unqID}(D, Property.Value.Values.Time(x, time))), mod(G \Leftarrow \\ & \Leftarrow Object.Create(Gen.U_{unqID}, Attribute_{11}.Name, \\ & Property.Value.Values.Time(x/time, time), Object.U_{unqID}(Property.Object(x)) \leftarrow \\ & \leftarrow Property.Link.Change(Object(x), x, G.U_{unqID}, time))), C \end{aligned}$$

2. Для реалізації відносини один до багатьох зі складовим первинним ключем «Attribute_11.Name» і «Attribute_12.Name» порядок дій повністю збігається з попереднім пунктом, але зазначена там процедура виконується окремо для кожного атрибута «Attribute_11.Name» і «Attribute_12.Name».

Для реалізації модальності зв'язків необхідно ввести такі обмеження.

Модальність зв'язків: «Entity_1» – «можливо»; «Entity_2» – «повинен».

Дозволяється додавати нові об'єкти в множину об'єктів типу «Entity_1», а також забороняється безпосередньо додавати об'єкти типу «Entity_2». Об'єкти типу «Entity_2» можна додавати лише шляхом їх виділення з об'єктів типу «Entity_1».

Модальність зв'язків: «Entity_1» – «повинен»; «Entity_2» – «можливо».

Після виділення об'єктів типу «Entity_2» з властивості об'єктів «Entity_1» дозволяється додавання нових об'єктів типу «Entity_2», забороняється додавання нових об'єктів типу «Entity_1» без виділення нових об'єктів типу «Entity_2» з відповідних властивостей.

Модальність зв'язків: «Entity_1» – «можливо»; «Entity_2» – «можливо».

Після виділення об'єктів типу «Entity_2» з властивості об'єктів «Entity_1» дозволяється додавання як нових об'єктів типу «Entity_1», так і типу «Entity_2».

Реалізація зв'язків багато до багатьох.

Даний вид зв'язку може бути зведений до двостороннього використання відносин один до багатьох.

Модальність зв'язків: «Entity_1» – «можливо»; «Entity_2» – «можливо».

Дозволяється додавання нових об'єктів як типу «Entity_1», так і типу «Entity_2».

Модальність зв'язків: «Entity_1» – «необхідно»; «Entity_2» – «можливо».

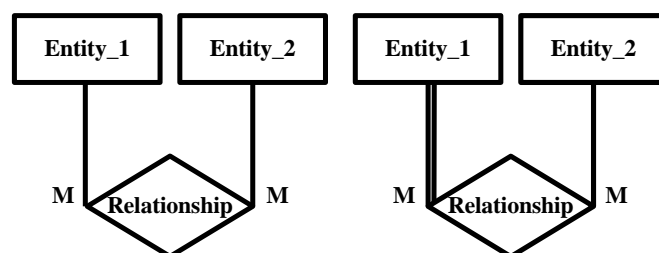


Рисунок 5 – Види зв'язків сутності багато до багатьох

Дозволяється додавання нових об'єктів типу «Entity_2», однак при додаванні нових об'єктів типу «Entity_1» потрібно додавати довідкові значення відповідних властивостей в об'єкти типу «Entity_2» на доданий об'єкт типу «Entity_1».

Правило 5. Будь-яка ER-модель даних відображається в SO-model.

Використовуємо принцип математичної індукції: припустимо, що n сутностей з можливими зв'язками між ними вже реалізовані в SO-model. Доведемо, що, виходячи з цього припущення, додавання ще однієї сутності з можливими зв'язками її з іншими сутностями з n вже існуючих також піддається реалізації в SO-model. Можливі наступні варіанти:

1. Додавання нової сутності без зв'язків зводиться до випадків, розглянутих в правилі 1;
2. Додавання рекурсивного зв'язку для деякої сутності зводиться до випадків, розглянутих у правилі 2;
3. Додавання нової сутності X і її зв'язку з уже існуючою сутністю B щодо один до одного, один до багатьох, багато до багатьох зводяться до випадків, розглянутих у правилі 3.

Таким чином, виходячи з припущення можливості ER-моделі даних бути реалізованою в SO-model для n сутностей, слідує її реалізуємість для $n+1$ сутностей, а оскільки реалізація ER-моделі даних в SO-model для однієї або двох пов'язаних сутностей була показана в правилах 1, 2, 3, то тим самим доведена можливість реалізувати ER-моделі даних в SO-model для будь-якої кількості сутностей і зв'язків між ними.

Акцентуємо увагу на необхідних порівняннях між ER-моделлю і SO-model:

- 1) сутність ER-моделі (в реляційному підході – це таблиця) відповідає типу об'єкта в SO-model;
- 2) атрибут сутності ER-моделі (в реляційному підході – стовпець таблиці) відповідає властивості об'єкта SO-model;
- 3) екземпляр сутності Entity в ER-моделі (в реляційному підході – рядок таблиці) відповідає об'єкту SO-model типу Entity;
- 4) зв'язок між сутностями Entity_1, Entity_2 по атрибуту первинний ключ Attr1 ER-моделі (в реляційному підході – зв'язок між таблицями в співвідношенні 1:1, 1:Б, Б:Б) відповідає зв'язку об'єктів типу Entity_1 з об'єктами типу Entity_2 за властивістю з ім'ям Attr1 у об'єктів типу Entity2.

Правило 6. В рамках зіставлення ER-моделі і SO-model в запропонованій SO-model підтримується темпоральність сутностей, атрибутів сутності ER-моделі даних, темпоральність зв'язків між сутностями ER-моделі даних.

Підтримка темпоральності на рівні сутностей ER-моделі даних пов'язана з можливістю додавання нових таблиць в базу даних без зв'язків їх з уже існуючими таблицями. Така можливість може бути реалізована в рамках реляційного підходу. Однак виникає неузгодженість між SQL- запитами до бази даних і програмними додатками, що обслуговують її (Impedance Mismatch). Програмні додатки доводиться переробляти. В SO-model темпоральність на рівні сутностей ER-моделі підтримується можливістю додавання об'єктів нового типу.

Підтримка темпоральності на рівні атрибутів сутності ER моделі даних пов'язана з можливістю створення таблиць зі змінним у часі складом стовпців або підтримки для кожного рядка таблиці свого переліку стовпців. Така можливість очевидно відсутня в рамках реляційного підходу. В SO-model така можливість підтримується: для виключення необхідного атрибуту на заданий момент часу достатньо записати в значення заданої властивості, що містить та не містить посилань, «порожньо» (null); для додавання необхідного атрибуту на заданий момент часу $time_p$ необхідно виконати функцію додавання нової властивості у вибраного об'єкту $X_p(Obj_j, i_p, n_p)$, а також додати значення цієї властивості, що не містить посилань, за допомогою $PPVt(Obj_j, n_p, v_p, d_p)$.

Оскільки в SO-model рядки таблиці зберігаються окремо у вигляді об'єктів, існує можливість підтримки для кожного об'єкта свого складу атрибутів-властивостей.

Підтримка темпоральності на рівні зв'язків між сутностями ER-моделі даних означає можливість змінювати тип і модальність зв'язків між таблицями бази даних у часі, а також додавати або виключати ці зв'язки. Для реляційного підходу зміна типу або модальності зв'язку призводить до порушення цілісності даних. Якщо такі зміни виконуються, то вони призводять до необхідності суттєвої переробки програмних додатків по роботі з базою даних. Крім того, такі зміни є незворотними, тобто інформація, що раніше цей зв'язок мав інший тип або модальність, втрачається. Додавання або виключення зв'язків, як правило, також призводять до порушення цілісності даних і втрати інформації про структуру бази даних до моменту зміни.

Висновки

В рамках запропонованої SO-model підтримка темпоральності на рівні зв'язків між сутностями ER-моделі даних здійснюється за рахунок відсутності обмеження на підтримання такої цілісності даних в базовому функціоналі SO-model (як було показано, будь-який зв'язок з часом може стати зв'язком багато до багатьох з модальністю «можливо» з обох кінців зв'язку), причому за рахунок фіксації моментів часу в

моделі даних існує можливість збереження історії про вид та модальності зв'язку фактичних даних в будь-який момент часу.

Як було відзначено, реалізація ER-моделі даних в рамках реляційного підходу призводить до проблем масштабування при кластерному, хмарному зберіганні даних. В SO-model кожен об'єкт має свій глобальний унікальний ідентифікатор U_{uniqID} . Це дозволяє зберігати об'єкти одного типу на різних комп'ютерах і підвищує масштабованість сховища даних. Також слід зазначити навмисну надмірність: значення кожної властивості може зберігатися з посиланням та без посилання. Відповідно до прийнятого протоколу можна реалізувати різні схеми узгодження цих значень, наприклад: завжди намагатися отримувати значення, що містить посилання, а при недоступності вузла видавати значення, що не містить посилання, при кожному успішному отриманні значення, що містить посилання, синхронізувати значення, що не містить посилання; завжди видавати значення, що не містить посилання, і до визначеного регламенту проводити синхронізацію цього значення зі значенням, що містить посилання. Все це дозволить підвищити доступність системи.

Таким чином, запропоновану модель сховища даних за рахунок її властивості уніфікації структури, яка враховує динаміку даних і їх зв'язків, можна розвивати в різних напрямках, використовуючи NoSQL рішення.

References

- [1] H. Garcia-Molina, J.D. Uman, J. Widom, M. Ozsu, P. Valduriez, T. Connolly, C. Begg, R. Elmasri, S. B. Navathe, M. Lin, M. Tsuchiya, S. Member, M. P. Mariani, M. Sharma, G. Singh, R. Virk, "Database systems: a practical approach to design, implementation, and management," *Int. J. Comput. Appl. Technol.* 49(4), 2010, pp. 90-107.
- [2] M. L. Chouder, S. Rizzi, R. Chalal, "Enabling self-service BI on document stores," *Workshop Proceedings EDBT/ICDT. Joint Conference Venice, Italy*, 2017.
- [3] P. Atzeni, F. Bugiotti, L. Rossi, "Uniform access to NoSQL systems," *Inf. Syst.* 43, 2014, pp. 117-133.
- [4] J. G. Enriquez, F. J. Dominguez-Mayo, M. J. Escalona, M. Ross, G. Staples, "Entity reconciliation in big data sources: a systematic mapping study," *Expert Syst. Appl.* 80, 2017, pp. 14-27.
- [5] A. A. Imam, S. Basri, R. Ahmad, N. Abdulaziz, M. T. Gonzalez-Aparicio, "New cardinality notations and styles for modeling NoSQL document-stores databases," *IEEE Region 10 Conference (TENCON)*, Penang, Malaysia, 2017.
- [6] A. Imam, S. Basri, R. Ahmad, N. Aziz, M.T. Gonzalez-Aparicio, J. Watada, S. Member, "Data modeling guidelines for NoSQL document-store databases," *Computer Science Education. SI on Advancing Theory About the Novice Programmer*. Taylor & Francis, 2018.
- [7] Pramod J. Sadalage, Martin Fowler, *NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence*, Addison-Wesley, 2012, 192 p.
- [8] C. J. Date, *Database Design and Relational Theory: Normal Forms and All That Jazz*, O'Reilly, 2012, 260 p. ISBN: 978-1-449-32801-6.
- [9] Jan L. Harrington, *Relational Database Design and Implementation*, Morgan Kaufmann, 2016, 935 p.
- [10] Louis Davidson, Jessica Moss, *Pro SQL Server Relational Database Design and Implementation*, Apress, 2016, 791 p. ISBN-13 (pbk): 978-1-4842-1972-0.
- [11] Ramez Elmasri, Shamkant B. Navathe, *Fundamentals of Database Systems, 7th Edition*, Pearson, 2015, 1242 p.
- [12] Hector Garcia-Molina, Jeffrey D. Ullman, Jennifer Widom, *Database Systems: The Complete Book, 2nd Edition*, Prentice Hall, 2009, 1248 p. ISBN-10: 0-13-187325-3; ISBN-13: 978-0-13-187325-4.

Стаття надійшла: 20.05.2022.

Відомості про авторів

Осієвський Сергій Валерійович – кандидат технічних наук, доцент, начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба.

Несміян Олексій Юрійович – кандидат технічних наук, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба.

S. Osiiievskiy, O. Nesmiian

ALLOPHONE DATABASE CONTROL SYSTEMS SYNTHESIS FOR INTERACTION ORGANIZATION BETWEEN THE AIRCRAFT AUTOMATED CONTROL SYSTEMS (AC ACS) OPERATOR AND AUTOMATION COMPLEX MEANS (ACM)

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv

УДК 004.95

О. Н. Романюк¹, О. В. Романюк¹, С. В. Котлик², А. В. Снігур¹, Л. Г. Коваль¹РОЗРОБКА МОДЕЛІ ВІДБИВНОЇ ЗДАНОСТІ ПОВЕРХНІ З
ВИКОРИСТАННЯМ ПОЛІНОМІВ ЧЕБИШЕВА¹Вінницький національний технічний університет, Вінниця²Одеська національний технологічний університет, Одеса

Анотація. На даному етапі розвитку комп'ютерної графіки важливою задачею є забезпечення високої продуктивності формування графічних сцен, достатньої для забезпечення реального часу та інтерактивного режиму, коли передбачається, що траєкторії руху об'єктів не задані заздалегідь, а визначаються діями користувача в процесі взаємодії із системою. Для таких режимів висуваються жорсткі вимоги до часу формування тривимірних графічних сцен. При формуванні тривимірних зображень за оптичними властивості поверхні відповідає двопротена дистрибутивна функція відбивної здатності (ДФВЗ). Вона є моделлю освітлення та визначає, яку частку випромінювання, що надійшло в точку з напрямку джерела світла, буде відбито в напрямку спостерігача. Принциповою вимогою до ДФВЗ є її розрахунок через косинус кута між відповідними векторами нормалей, який легко знайти через скалярний добуток векторів. При розробці моделі важливо, щоб зображення відблиску відносно еталонної реалізації не мало візуальних відмінностей. Проста апаратна реалізація функції можлива при використанні поліномів низького степеня за умови, що при розрахунку не використовують складні функції та довготривалі операції, які мають місце для відомих підходів. При формуванні відблисків важливо з достатньою точністю відтворити його епіцентр. Для периферійних областей, які характеризують затухання інтенсивності світла до мінімального значення, необхідно забезпечити монотонність зміни інтенсивності кольору, яка виключає появу артефактів. У роботі розроблено нову модель відбивної здатності поверхні з використанням поліномів Чебишева, яка має другу степінь і просту апаратну реалізацію та задовольняє наведеним вимогам. Отримано формули для розрахунку складових коефіцієнтів. Розроблена модель з високою точністю відтворює епіцентр відблиску. Отримано оцінки точності апроксимації. Розроблено структурну схему пристрою для формування двопротенової дистрибутивної функції відбивної здатності. Розроблена модель відбивної здатності поверхні може бути використана в системах динамічної тривимірної графіки.

Ключові слова: рендеринг, модель відбивної здатності поверхні, дистрибутивна функція відбивної здатності, модель Фонга, модель Бліна, спекулярна складова кольору.

Abstract. At this stage of computer graphics development, an important task is to ensure high productivity of graphic scenes, sufficient for real-time and interactive mode, when it is assumed that the trajectories of objects are not set in advance, but determined by user actions in interaction with the system. For such modes there are strict requirements for the time of formation of three-dimensional graphic scenes. In the formation of three-dimensional images for the optical properties of the surface is responsible for the two-beam distributive function of reflectivity (DFVZ). It is a model of illumination and determines what proportion of the radiation received at a point from the direction of the light source will be reflected in the direction of the observer. A fundamental requirement for DFVZ is its calculation through the cosine of the angle between the corresponding vectors of normals, which is easy to find through the scalar product of vectors. When developing the model, it is important that the image of the reflection relative to the reference implementation has no visual differences. Simple hardware implementation of the function is possible when using low-degree polynomials, provided that the calculation does not use complex functions and long-term operations that take place for known approaches. When forming glare, it is important to reproduce its epicenter with sufficient accuracy. For peripheral areas, which characterize the attenuation of light intensity to a minimum value, it is necessary to ensure the monotony of color intensity change, which eliminates the appearance of artifacts. The paper develops a new model of surface reflectivity using Chebyshev polynomials, which has a second degree and a simple hardware implementation and satisfies the above requirements. Formulas for calculating the component coefficients are obtained. The developed model reproduces the epicenter of the glare with high accuracy. Estimates of the accuracy of the approximation are obtained. The structural scheme of the device for formation of a two-beam distributive function of reflectivity is developed. The developed model of surface reflectivity can be used in systems of dynamic three-dimensional graphics.

Key words: rendering, surface reflectivity model, reflective distributive function, Fong model, Pancake model, specular color component.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-47-54>.

Вступ

При формуванні тривимірних зображень за оптичні властивості поверхні відповідає двопротена дистрибутивна функція відбивної здатності ДФВЗ (BRDF – Bidirectional Reflectance Distributive Function) [1-8]. Вона є моделлю освітлення та визначає, яку частку випромінювання, що надійшло в точку з напрямку джерела світла, буде відбито в напрямку спостерігача.

Для відтворення рефлекторних властивостей поверхні бажано розробити таку модель, обчислювальна складність якої не залежала б від коефіцієнта спекулярності поверхні. Проста апаратна реалізація ДФВЗ можлива при використанні поліномів низького степеня за умови, що при розрахунку не використовують складні функції та довготривалі операції, які мають місце для відомих підходів. При формуванні відблисків важливо з достатньою точністю відтворити його епіцентр. Для периферійних областей, які характеризують затухання інтенсивності світла до мінімального значення, необхідно забезпечити монотонність зміни інтенсивності кольору, яка виключає появу артефактів [1, 4].

Тому актуальною задачею є розробка моделі відбивної здатності поверхні, яка має просту обчислювальну складність і просту апаратну реалізацію.

Аналіз літератури

При апаратній реалізації важливо досягти високої реалістичності при використанні простих, з апаратної точки зору, операцій при їх мінімальній кількості та мінімальній розгалуженості обчислювального процесу.

Принциповою вимогою до ДФВЗ [1-8] є її розрахунок через косинус кута між відповідними векторами нормалей, який легко знайти через скалярний добуток векторів. При визначенні ж дистрибутивної функції через кут між векторами необхідно виконання трудомісткої операції арккосинуса.

Бажано, щоб дистрибутивна функція була додатною, оскільки в іншому випадку необхідний додатковий аналіз для виконання процедур відсікання. При розробці моделі важливо, щоб зображення відблиску відносно еталонної реалізації не мало візуальних відмінностей.

Локальні моделі освітлення [4] можна розділити на дві групи. Перша містить ті ДФВЗ поверхні, які отримано експериментальним шляхом. Вони найбільш поширені, оскільки достатньо прості та забезпечують прийнятну реалістичність відтворення об'єктів, для яких не вимагається точна фізична інформація про освітлення. До другої групи [4] відносять більш точні моделі, які, як правило, враховують як корпускулярну, так і хвильову природу світлового потоку. В таких моделях поверхня розглядається у вигляді мікроскопічних ділянок.

ДФВЗ можна розділити на ізотропні та анізотропні [4]. Ізотропні функції інваріантні відносно повороту навколо вектора нормалі до поверхні. Навпаки, в анізотропних дистрибутивних функціях відбивні властивості матеріалу змінюються при повороті навколо вектора нормалі.

У комп'ютерній графіці найчастіше використовують модель визначення спекулярної складової кольору Б. Фонга [1-8], що має вигляд

$$I_s = I \cdot \varpi(\varphi, \lambda) \cdot \cos^n \psi,$$

де $\varpi(\varphi, \lambda)$ – крива відбиття, що визначає відношення дзеркально відбитого світла до падаючого як функцію кута падіння θ і довжини хвилі λ , n – коефіцієнт спекулярності поверхні.

Функція $\varpi(\varphi, \lambda)$ складна, тому її у більшості випадків заміняють константою k_s , яку визначають експериментально або вибирають з естетичних міркувань. У ДФВЗ Фонга [1, 4] $\cos \psi = \vec{V} \cdot \vec{R}$, де $\vec{R} = 2 \cdot (\vec{L} \cdot \vec{N}) \cdot \vec{N} - \vec{L}$, де \vec{L} – вектор до джонла світла, \vec{N} – вектор нормалі. Вектор \vec{R} називають вектором дзеркального відбиття [1, 4]. У дистрибутивній функції Бліна [227], яка історично з'явилася пізніше ДФВЗ Фонга, замість $\cos \psi$ використовують $\cos \gamma = \vec{N} \cdot \vec{H}$, де $\vec{H} = (\vec{L} + \vec{V}) / |\vec{L} + \vec{V}|$, \vec{V} – вектор до спостерігача.

Серед ДФВЗ найбільшого поширення отримали моделі освітлення Фонга та Бліна. Це пояснюється їх простотою, достатньо високою точністю та використанням в якості аргумента – косинуса кута між векторами, який легко знайти через їх скалярний добуток. Саме ці моделі доцільно використовувати в системах динамічної графіки. Фізично точні моделі, які враховують фасетну структуру поверхні та хвильову теорію світла, доцільно використовувати при жорстких вимогах до реалістичності, оскільки їх розрахунок вимагає великих затрат часу.

Мета статті – розробка моделі відбивної зданості поверхні з використанням поліномів Чебишева, яка має просту обчислювальну складність та просту апаратну реалізацію.

Розробка нової моделі відбивної зданості поверхні

Розглянемо графік функції $\cos^n x$ для різних n (рис. 1).

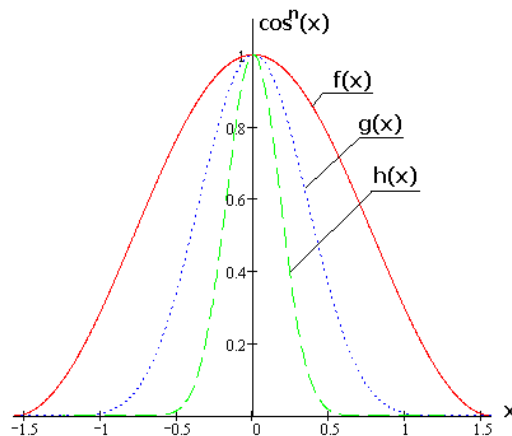


Рисунок 1 – Графіки функції $\cos^n(x)$ при різних n

$$f(x) = \cos^2(x), \quad g(x) = \cos^8(x), \quad h(x) = \cos^{32}(x)$$

Аналізуючи дані графіки видно, що верхня частина графіка подібна до перевернутої параболи. Тому пропонується замінити $\cos^n(x)$ на параболу – $f(x) = A \cdot x^2 + B \cdot x + C$. Така заміна обгрунтована тим, що при відтворенні спекулярної складової кольору жорсткі вимоги ставляться саме до відображення епіцентру відблиску (рис. 2).

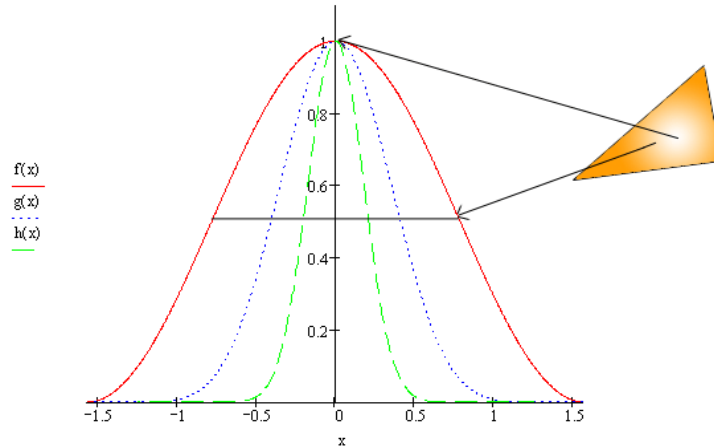


Рисунок 2 – Епіцентр відблиску

Для заміни $\cos^n x$ на $A \cdot x^2 + B \cdot x + C$ потрібно знайти відповідні коефіцієнти A , B , C . Щоб знайти ці коефіцієнти розкладемо $\cos^n x$ в ряд Чебішева [9], виконавши такі перевороння:

$$Na := 3$$

$$a := 0$$

$$b := 0.6$$

$$c(j) := \frac{2}{Na} \cdot \sum_{k=1}^{Na} \left[f \left[\cos \left[\pi \cdot \frac{\left(k - \frac{1}{2} \right)}{Na} \right] \cdot \frac{(b-a)}{2} + \frac{(b+a)}{2} \right] \cdot \cos \left[\pi \cdot j \cdot \frac{\left(k - \frac{1}{2} \right)}{Na} \right] \right], \quad (3.5)$$

$$T(n, x) := \cos(n \cdot \arccos(x))$$

$$ap(x) := \left[\sum_{k=0}^{Na-1} c(k) \cdot T \left[k, \frac{x - \frac{(b+a)}{2}}{\frac{(b-a)}{2}} \right] \right] - \frac{c(0)}{2}$$

$$T_m := \frac{(b-a)}{2} \quad T_p := \frac{(b+a)}{2}$$

$$C := \frac{(2 \cdot c(2) \cdot T_p^2) - (c(1) \cdot T_p \cdot T_m)}{T_m^2} + \frac{c(0)}{2} - c(2)$$

$$B := \frac{c(1) T_m - 4c(2) T_p}{T_m^2}$$

$$A := \frac{2c(2)}{Tm^2}$$

$$fa(x) := A \cdot x^2 + B \cdot x + C.$$

У наведених формулах використано локальні змінні, які не корельовані з раніше прийнятими.

Вибір для апроксимації полінома Чебишева має таке обґрунтування. Поліноми П. Л. Чебишева [9] відомі своєю властивістю найменше відхилятися від нуля на заданому проміжку, і відповідно, вносять найменший внесок у похибку інтерполяції. Для апроксимації $\cos^n x$ використовується тригонометрична форма запису полінома Чебишева $T_n(x) = \cos(n \arccos x), |x| \leq 1$, яка визначається через $\cos x$, що, безумовно, впливає на зменшення похибки.

У даному випадку було взято три перших члени ряду Чебишева. Для визначення коефіцієнтів A, B, C як видно з формул, потрібно задати інтервал, на якому виконується апроксимація. Для цього задамо задати рівень відносної похибки та визначити, до якого значення верхньої межі b похибка апроксимації не буде перевищувати задану відносну похибку.

Взявши за максимальну відносну похибку 2%, отримуємо коефіцієнти A, B, C для всіх значень n . Для наочності представимо графіки коефіцієнтів залежно від значення n (рис. 3-4).

Проаналізувавши дані графіки можна зробити такі висновки: значення коефіцієнта A змінюється за лінійним законом:

$$fra(n) = -0,272 \cdot n - 0,16$$

для коефіцієнта B значення змінюється по нелінійному закону. Для спрощення знаходження цього коефіцієнта пропонується використати кусково-лінійну апроксимацію.

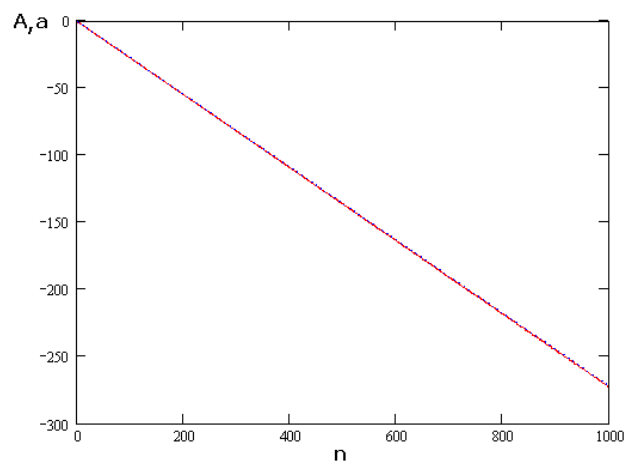
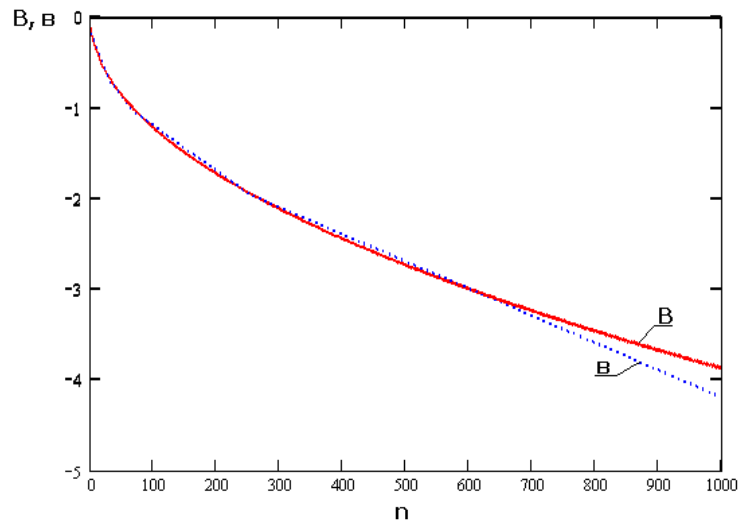


Рисунок 3 – Графік значень коефіцієнтів a при різних n

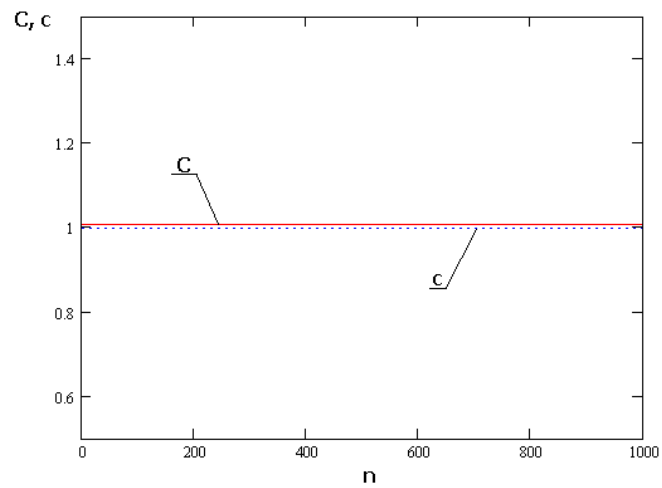
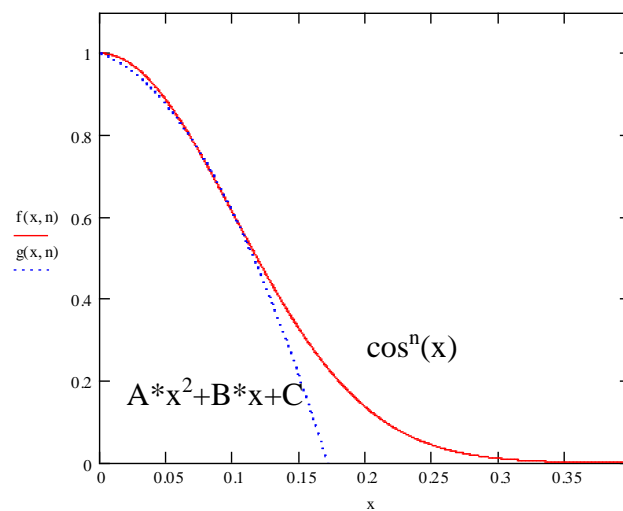
Пропонується здійснити розбиття на чотири інтервали з відповідними коефіцієнтами лінійних функцій (рис. 4 – штрихована лінія):

$$b = \left(\begin{array}{ll} -0,018 \cdot n - 0,158 & \text{при } 1 \leq n \leq 31, \\ -0,01 \cdot n - 0,38 & \text{при } 32 \leq n \leq 63, \\ -0,005 \cdot n - 0,7 & \text{при } 64 \leq n \leq 255, \\ -0,003 \cdot n - 1,2 & \text{при } 256 \leq n \leq 1000. \end{array} \right);$$

Значення коефіцієнта C не змінюється та дорівнює 1.

Рисунок 4 – Графік значень коефіцієнтів B при різних n

Графік функції $A \cdot x^2 + B \cdot x + C$ зображено на рисунку 5. При використанні даної BRDF отримаємо такий графік відносної похибки апроксимації (рис. 6).

Рисунок 5 – Графік значень коефіцієнтів C при різних n Рисунок 6 – Порівняння графіків функцій $A \cdot x^2 + B \cdot x + C$ і $\cos^n x$

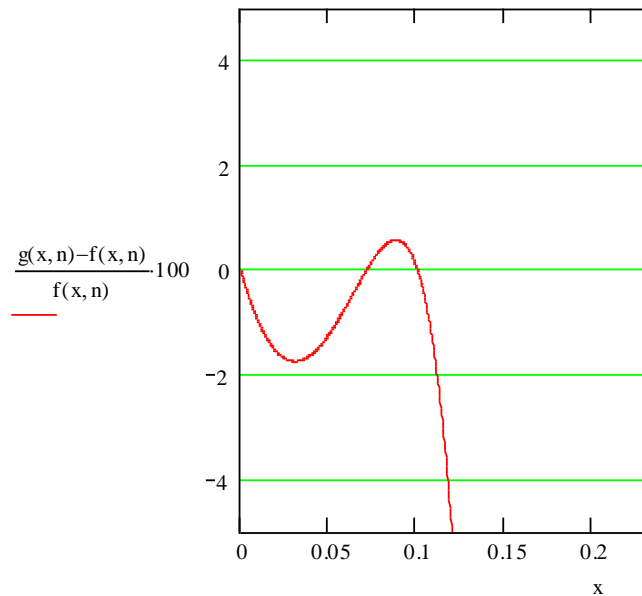


Рисунок 7 – Відносна похибка апроксимації функції $\cos^n x$ функцією $A \cdot x^2 + B \cdot x + C$

На рисунку 8 зображено структурну схему пристрою для апроксимації $\cos^n x$.

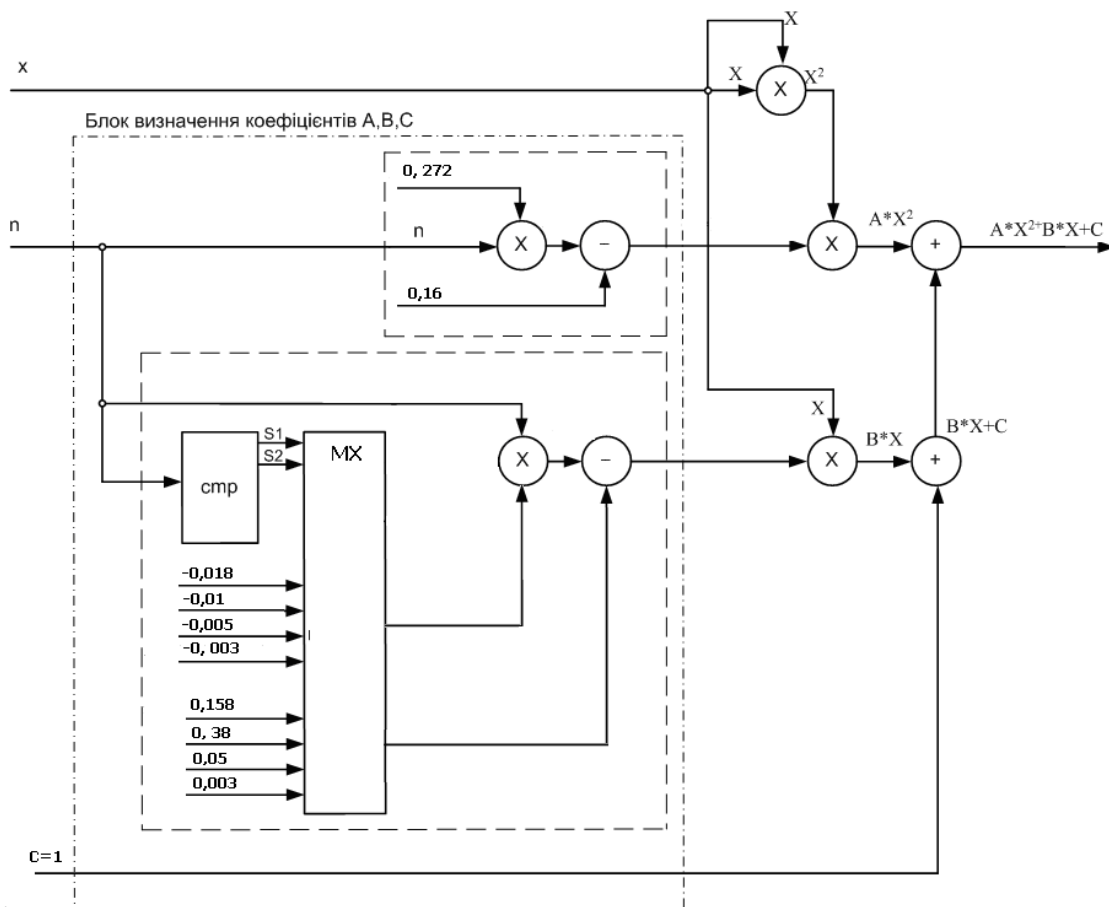


Рисунок 8 – Структурна схема обчислення BRDF

Висновки

Розроблено модель відбивної зданості поверхні з використанням поліномів Чебишева, яка має просту обчислювальну складність та просту апаратну реалізацію. ДФВЗ має другу степінь для всього діапа-

зону n і високою точністю відтворює епіцентр відблиску. Розроблена модель відбивної здатності поверхні може бути використана в системах динамічної тривимірної графіки.

Список літератури

- [1] О. Н. Романюк, та А. В. Чорний, *Високопродуктивні методи та засоби зафарбовування тривимірних графічних об'єктів*, Вінниця, Україна: УНІВЕСУМ-Вінниця, 2006.
- [2] О. Н. Романюк, "Метод підвищення реалістичності відтворення тривимірних графічних об'єктів", *Інформаційні технології та комп'ютерна інженерія*, №1 (8), с. 269-272. 2016.
- [3] О. Н. Романюк, *Комп'ютерна графіка. Навчальний посібник*. Вінниця, Україна: УНІВЕСУМ-Вінниця, 2001.
- [4] О. Н. Романюк, "Класифікація дистрибутивних функцій відбивної здатності поверхні", *Наукові праці Донецького національного технічного університету. Сер.: Інформатика, кібернетика та обчислювальна техніка*, вип. 9, с. 145-151. 2008.
- [5] О. Н. Романюк, Ю. Р. Довгалюк, та С. В. Олійник, "Класифікація графічних відеоадаптерів", *Наукові праці Донецького національного технічного університету. Сер.: Інформатика, кібернетика та обчислювальна техніка*, вип. 14, с. 211-215. 2011.
- [6] Романюк О. Н., "Альтернативна реалізація дистрибутивної двопрореєвої функції для моделей освітлення Бліна та Фонга", *Наукові праці Донецького національного технічного університету. Серія «Обчислювальна техніка та автоматизація»*, випуск 106, с. 151-156. 2006.
- [7] O. Romanuyk, "Approximation of Bidirectional Reflectance Distribution Function with 3-Degree Polynomial", *IEEE Workshop on Control and Communications*, 2007. SIBCON apos; 07. Siberian Conference on Volume, Issue, 20-21 April 2007, pp. 158-164. 2007.
- [8] O. Romanuyk, and A. Chernij, "Methods for Specular Color Component Accelerate Calculation", *IEEE Workshop on Intelligent Data Acquisition and Advanced Computing systems: Technology and Applications*. Sofia, pp. 615-619. 2005.
- [9] А. В. Примак, та І. О. Шевчук, *Теорія наблизень, Навчальний посібник*, Київський національний університет ім. Т. Г. Шевченко, 2011.

Стаття надійшла: 16.05.2022.

References

- [1] O. N. Romanyuk, ta A. V. Chorny, *Vysokoproduktyvni metody ta zasoby zafarbovuvannya tryvymirnykh hrafichnykh obyektiv*, Vinnytsya, Ukrayina: UNIVESUM-Vinnytsya, 2006 [in Ukrainian].
- [2] O. N. Romanyuk, "Metod pidvyshchennya realistychnosti vidtvorennya tryvymirnykh hrafichnykh ob'yektiv", *Informatsiyini tekhnolohiyi ta komp'yuterna inzheneriya*, №1 (8), s. 269-272. 2016 [in Ukrainian].
- [3] O. N. Romanyuk, *Kompyuterna hrafika. Navchannyu posibnyk*. Vinnytsya, Ukrayina: UNIVESUM-Vinnytsya, 2001 [in Ukrainian].
- [4] O. N. Romanyuk, "Klasyfikatsiya dystributyvnykh funktsiy vidbyvnoyi zdadnosti poverkhni", *Naukovi pratsi Donetskoho natsionalnoho tekhnichnoho universytetu. Ser.: Informatyka, kiberne-tyka ta obchyslyval na tekhnika*, vyp. 9, s. 145-151. 2008 [in Ukrainian].
- [5] O. N. Romanyuk, YU. R. Dovhalyuk, ta S. V. Oliynyk, "Klasyfikatsiya hrafichnykh videoadapteriv", *Naukovi pratsi Donetskoho natsionalnoho tekhnichnoho universytetu. Ser.: Informatyka, kiber-nyta ta obchyslyval na tekhnika*, vyp. 14, s. 211-215. 2011 [in Ukrainian].
- [6] O. N. Romanyuk, "Alternatyvna realizatsiya dystributyvnoyi dvopromenevoyi funktsiyi dlya modeley osviltlennya Blina ta Fonha", *Naukovi pratsi Donetskoho natsionalnoho tekhnichnoho universytetu. Seriya «Obchyslyvalna tekhnika ta avtomatyzatsiya»*, vypusk 106, s. 151-156. 2006 [in Ukrainian].
- [7] O. Romanuyk, "Approximation of Bidirectional Reflectance Distribution Function with 3-Degree Polynomial", *IEEE Workshop on Control and Communications*, 2007. SIBCON apos; 07. Siberian Conference on Volume, Issue, 20-21 April 2007, pp. 158-164. 2007.
- [8] O. Romanuyk, and A. Chernij, "Methods for Specular Color Component Accelerate Calculation", *IEEE Workshop on Intelligent Data Acquisition and Advanced Computing systems: Technology and Applications*. Sofia, pp. 615-619. 2005.
- [9] A. V. Prymak, ta I. O. Shevchuk, *Teoriya nablyzhen, Navchalnyu posibnyk*, Kyuyivskyyu natsionalnyu universytet im. T.H. Shevchenko, 2011 [in Ukrainian].

Відомості про авторів

Романюк Олександр Никифорович – доктор технічних наук, професор, завідувач кафедри програмного забезпечення.

Романюк Оксана Володимирівна – кандидат технічних наук, доцент кафедри програмного забезпечення.

Котлик Сергій Валентинович – кандидат технічних наук, доцент.

Снігур Анатолій Васильович – кандидат технічних наук, доцент кафедри обчислювальної техніки.

Коваль Леонід Григорович – кандидат технічних наук, доцент кафедри біомедичної інженерії та оптико-електронних систем.

O. N. Romanyuk¹, O. V. Romanyuk¹, S. V. Kotlyk², A. V. Snigur¹, L. G. Koval¹

DEVELOPMENT OF A MODEL OF REFLECTIVE SURFACE CAPACITY USING CHEBYSHEV POLYNOMES

¹Vinnitsia National Technical University, Vinnitsia

²Odessa National Technological University, Odessa

УДК 004.9: 004.032.26

М. А. Солоний, А. А. Яровий, Я. В. Іванчук, В. С. Озеранский

ПЕРСПЕКТИВИ НЕЙРОМЕРЕЖЕВОГО ПІДХОДУ ДЛЯ ЗАДАЧІ ВІДТВОРЕННЯ ПОШКОДЖЕНИХ ПАПЕРІВ

Вінницький національний технічний університет, Вінниця

Анотація. У наш час, задача відтворення пошкоджених паперів є достатньо актуальною, експерти витрачають години, дні або навіть тижні, на те, щоб відтворити пошкоджені документи, рисунки або інші матеріали, які можуть відіграти роль ключового доказу в кримінальній справі. Автоматизація даного процесу значно підвищить швидкість та якість вирішення даної задачі, тим самим підвищить ефективність роботи експертів-криміналістів. Під час пошуку існуючих рішень, в ході дослідження прямих аналогів виявлено не було, проте знайдено декілька непрямих аналогів, які вирішують досить близькі задачі. Перший аналог – технологія, запропонована вченими Хайфського університету для відтворення пошкоджених археологічних знахідок. Дану технологію успішно випробувано на реальних артефактах Британського музею, що довело її ефективність при відтворенні пошкоджених фресок. Дані результати є перспективними для подальшої розробки інформаційної технології відтворення цілісності пошкодженого документа, зокрема, в контексті повного відтворення структури паперу на основі його мікрорельєфу. Другий аналог – технологія редагування зображень за допомогою карт Кохонена. Дана технологія ефективно виконує базові завдання ретушування зображень, зокрема, видалення об'єктів, відновлення цілісності після видалення. Оскільки дана технологія використовується для обробки зображень, її можна використати як основу для відтворення пошкодженого вмісту документа після його фізичної збірки. Адже під час відновлення структури паперу цілісність вмісту може бути частково втрачена. В даній статті детально проаналізовано кожну з наведених технологій, в тому числі й на рівні математичних моделей, виокремлено їх переваги та недоліки, наведено приклади їх реального застосування. На основі переваг кожної з проаналізованих технологій, запропоновано підхід до вирішення задачі відтворення пошкоджених паперів.

Ключові слова: нейронні мережі, відтворення пошкоджених паперів, криміналістика.

Abstract. Nowadays, the damaged papers restoration task is quite urgent, experts spend hours, days or even weeks to restore damaged documents, drawings or other materials that can play the key role evidence in a criminal case. Automation of this process will significantly increase the speed and quality of solving this problem, thereby increasing the efficiency of the work of forensic experts. During the search for existing solutions, no direct analogs were found, but several indirect analogs were found that solve quite similar problems. The first analog is a technology proposed by Haifa University scientists to restore damaged archaeological finds. This technology was successfully tested on real artifacts of the British Museum, which proved its effectiveness in restoring damaged frescoes. These results are promising for the further development of information technology for restoring the integrity of a damaged document, in particular, in the context of the complete restoration of the paper structure based on its microrelief. The second analog is image editing technology using Kohonen maps. This technology effectively performs the basic tasks of retouching images, in particular, removing objects, restoring integrity after removal. Since this technology is used for image processing, it can be used as a basis for restoration of the damaged content of a document after its physical assembly. After all, during the paper structure restoration, the integrity of the content may be partially lost. In this article, each of the above technologies is analyzed in detail, including at the level of mathematical models, their advantages and disadvantages are highlighted, and examples of their real application are given. Based on the advantages of each of the analyzed technologies, an approach to solving the problem of damaged papers restoration is proposed.

Keywords: neural networks, damaged papers restoration, criminalistics.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-55-60>.

Вступ та актуальність

Із розвитком інформаційних технологій активується розвиток різних професійних сфер, в тому числі й сфери криміналістики. Працюючи в цій сфері, фахівці стикаються з різними неординарними задачами, такими як балістичні дослідження, пошук відбитків пальців, відтворення розірваних та пошкоджених паперів. Однією з актуальних задач, що потребують активнішого застосування інтелектуальних інформаційних технологій та автоматизації, є задача відтворення пошкоджених паперів [1]. За результатами спілкування з експертами-криміналістами встановлено, що наразі проблема відтворення пошкоджених паперів вирішується переважно вручну, що займає надто багато часу. Експерти годинами співставляють елементи паперу, співставляючи текстуру, розмір, символи. Автоматизувавши даний процес, можна оптимізувати велику кількість часу та зусиль, збільшити точність відтворення, а також підвищити ефективність роботи експертів-криміналістів [2].

Мета

Метою статті є аналіз сучасних досліджень і підходів до вирішення задачі відтворення пошкоджених паперів та визначення перспектив застосування нейромережевого підходу.

Задачі

1. Проаналізувати існуючі моделі, методи та технології вирішення задачі відтворення пошкоджених об'єктів (паперів).
2. Запропонувати підхід до вирішення задачі відтворення пошкоджених паперів на основі поєднання ключових аспектів проаналізованих технологій.

Аналіз існуючих аналогів

В ході проведеного аналізу літературних та інформаційних джерел прямих аналогів чи досліджень щодо задачі відтворення пошкоджених паперів виявлено не було. Разом з тим, знайдено та проаналізова-

но подібні дослідження, що стосуються задачі відтворення в інших предметних областях (непрямі аналогії). Їх аналіз буде корисним з точки зору доцільності та перспектив застосування нейромережевого підходу у задачі відтворення об'єктів.

Зокрема, учені Хайфського університету, розробили алгоритм відтворення археологічних артефактів за допомогою нейронних мереж. Описаний ними алгоритм базується на чотирьох таких основних підходах [3].

По-перше, щоб вирішити проблему застарілих фрагментів археологічних артефактів, розробники пропонують екстраполювати кожен фрагмент перед повторною збіркою. Цей процес реалізується шляхом створення широкої смуги k -пікселів навколо фрагмента, який включає не лише область, що постраждала від ерозії, але й продовження до наступного фрагмента.

По-друге, пропонується метод вибірки набору реальних перетворень. Мета полягає в тому, щоб екстрапольовані фрагменти були близькі один до одного (щоб ймовірність суміжності була високою), але не перекривалися. Існування збігу (подібності) між двома фрагментами визначається в тому випадку, якщо пікселі вихідних фрагментів не перекриваються після їх накладання. Учені показують, що набір таких перетворень можна описати як простір конфігурації завдань, що, наприклад, часто використовується в робототехніці.

По-третє, – пошук збігів. Розробники намагаються обчислити параметр несхожості для даного перетворення між парою фрагментів. На першому етапі проблема безперервності простору при порівнянні була зведена до узгодження екстрапольованої області частини фрагменту на інший вихідний фрагмент у зоні перекриття. Головна особливість полягає в тому, що колір країв одного фрагмента має збігатися з кольором країв іншого.

По-четверте, – розміщення. Аналізуються проблеми, що стосуються безперервності простору трансформації та загальної форми фрагментів, які в подальшому ефективно усуваються. Крім того, щоб вирішити проблему неточності перетворення (за допомогою вибірки), вибране перетворення уточнюють на невеликій ділянці навколо нього.

Описаний алгоритм учених Хайфського університету було перевірено на реальних об'єктах із колекцій Британського музею та на фресках різних церков по всьому світу. На рис. 1 зображено поетапну візуалізацію роботи алгоритму [3].

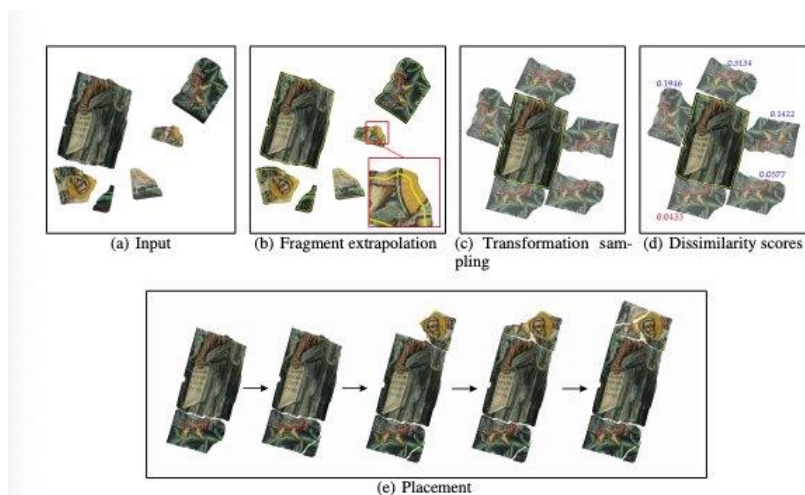


Рисунок 1 – Візуальний приклад роботи алгоритму відтворення археологічних артефактів [3]

Даний алгоритм досить ефективно вирішує задачу відтворення об'єктів, так як містить вирішення багатьох підзадач, включаючи нерівності країв, ерозію та інші можливі пошкодження елементів (в контексті ж задачі відтворення пошкоджених паперів, дуже важливо зберегти максимальну якість контенту, так як навіть деякі маленькі елементи паперів, можуть бути значним речовим доказом).

Інший приклад подібних досліджень є редагування та відтворення пошкоджених зображень. У даних дослідженнях було проаналізовано модель редагування та відновлення зображень за допомогою карти Кохонена [4].

Карта Кохонена є двовимірною мережею $N \times N$, що складається з нейронів. Кожен нейрон у мережі є квадратом $S \times S$ – вектор ваги, значення якого рівні коду кольору відповідного пікселя [4-7].

Для навчання в мережу подаються фрагменти зображення $S \times S$, після чого мережа шукає найбільш схожий на фрагмент нейрон, так званий ВМУ (best matching unit), і коригує його вагові коефіцієнти таким чином, щоб він ще більше був схожий на поданий фрагмент. А потім ще тренує сусідів, але вже із меншою інтенсивністю. Що далі знаходиться нейрон від ВМУ, то менший внесок у нього робить пода-

ний фрагмент. Таким чином мережа навчається доти, доки відхилення ВМУ кожного поданого фрагмента досягне встановленої мінімальної величини.

Алгоритм навчання здійснюється за ітераціями. Нехай t – номер ітерації. Припустимо, що ініціалізація має номер ітерації 0. Далі виконуються такі операції:

1. Обираємо випадковий вектор $x(t)$ із набору вхідних значень.

2. Знаходимо відстань до всіх векторів ваг усіх нейронів карти Кохонена. Для даної операції обирається відповідна міра, в загальному випадку – середньоквадратичне відхилення. Шукаємо нейрон, найбільш близький до вхідного значення [5]:

$$d(x(t), m_c(t)) \leq d(x(t), m_i(t)),$$

де $m_c(t)$ – вектор ваги нейрона “переможця” $M_c(t)$,

$m_i(t)$ – вектор ваги i -го вузла в карті,

$d(x(t), m_i(t))$ – міра відхилення.

В разі, якщо вищевказаному виразу задовольняє декілька нейронів, ВМУ обирається випадковим чином.

3. Визначення міри сусідства нейронів та зміна ваг нейронів у карті Кохонена.

3.1. Обираємо міру сусідства – функцію $h_{ci}(t)$. Дана функція визначає міру сусідства між нейронами M_i та M_c . Зазвичай, в якості функції $h_{ci}(t)$ використовується гаусова функція [5]:

$$h_{ci}(t) = a(t) * \exp\left(-\frac{\|r_c - r_i\|^2}{2\delta^2(t)}\right),$$

де $(0 < a(t) < 1)$ – навчальний співмножник, монотонно спадаючий з кожною наступною ітерацією (тобто, визначається наближення значення векторів ваг ВМУ та їх сусідів, що більше крок, то менше уточнення);

r_i, r_c – координати вузлів $M_i(t)$ та $M_c(t)$ на карті Кохонена;

$\delta(t)$ – множник, що поступово зменшує кількість сусідів з ітераціями (монотонно зменшується).

Параметри a, δ та їх характер зменшення задаються аналітиком.

Більш простий спосіб задання функції сусідства [4-7]:

$$h_{ci}(t) = a(t),$$

якщо $M_i(t)$ знаходиться в околі $M_c(t)$ заздалегідь заданого аналітиком радіусу (в іншому разі – рівна 0).

Функція $h(t)$ дорівнює $a(t)$ для ВМУ та зменшується з віддаленням від ВМУ.

3.2. Обчислення помилки карти

Змінюємо вектор ваг за виразом [4-7]:

$$m_i(t) = m_i(t-1) + h_{ci}(t)(x(t) - m_i(t-1)),$$

Таким чином, усі вузли, що є сусідами ВМУ, наближаються до розгляду.

4. Вибір зупинки.

Для визначення критерію зупинки в більшості випадків використовується помилка карти, наприклад, як середня арифметична відстань між спостереженнями та векторами ваги відповідних їм ВМУ [6]:

$$\frac{1}{N} \sum_{i=1}^N \|x_i - m_c\|,$$

де N – кількість елементів набору вхідних даних.

Виходячи з описаного вище, можна виділити такі елементи для моделювання системи відновлення мультимедійних даних:

1) X – вектор спостережуваних даних. У відновленні мультимедійної інформації це може бути певний набір пікселів (семплів, набір блоків стиснення зображень), згрупованих за певним правилом.

2) m – вектор ваги нейрона. За визначенням, має бути однієї розмірності c^x .

3) $h_{ci}(t)$ – міра сусідства нейронів. Деяка функція, що повертає відстань між нейронами і залежить від номера ітерації t . За певних умов може визначати і топологію поверхні.

4) $d(x(t), m_c(t))$ – міра відхилення, що вказує наскільки вектор $x(t)$ "не схожий" на вектор $m_i(t)$.

Таким чином, якщо в моделі визначені вищезазначені елементи, то в цій моделі можна використовувати карти Кохонена, що самоорганізуються, для відновлення пошкоджених ділянок даних. Для підвищення якості редагування зображень, також учені пропонують використовувати попередню сегментацію. Сегментація кольорового зображення організована як кластеризація за допомогою самоорганізованих карт, функцій з нечіткими мірами або за допомогою самоорганізованих карт R-дерева. Зображення як набір пікселів або інші структурні елементи зазвичай не можуть бути представлені як вхідний вектор у саморганізованих картах. Геометричні варіації, такі як переходи, обертання, масштабування за різних умов освітлення, є надзвичайно широкими та різноманітними. На рис. 2 зображено приклад роботи даної технології [7].

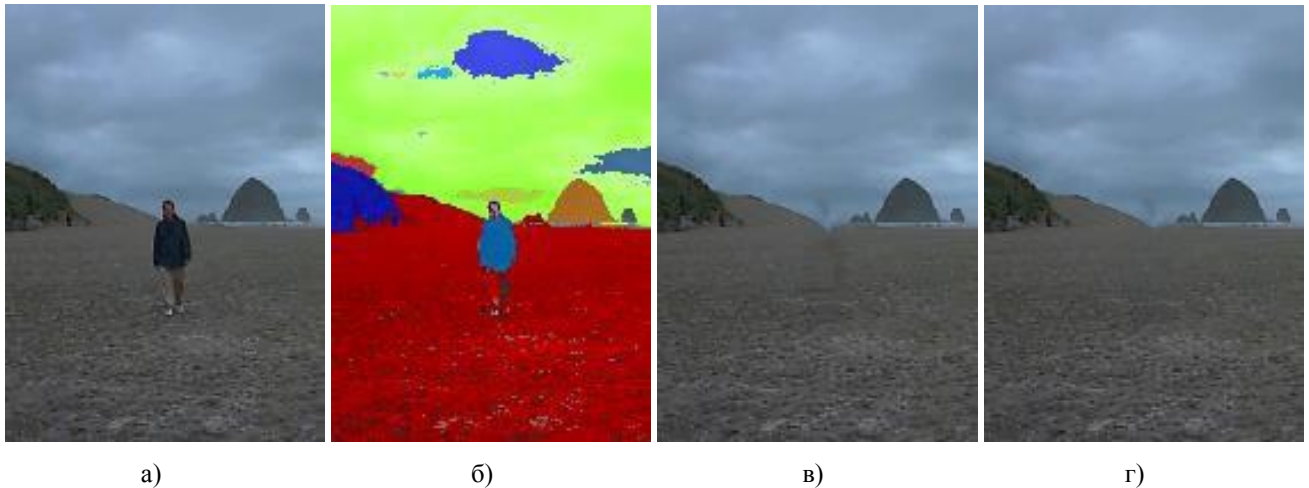


Рисунок 2 – (а) початкове зображення; (б) сегментоване зображення; (в) відредатоване зображення за допомогою карт Кохонена; (г) відредатоване зображення за допомогою карт Кохонена з попередньою сегментацією [7]

Висновок

На основі аналізу результатів досліджень задачі відтворення в інших предметних областях виділено декілька важливих аспектів, які певною мірою є актуальними при вирішенні задачі відтворення пошкоджених паперів.

По перше, стосовно технології відтворення пошкоджених археологічних знахідок. Застосовані тут рішення вирішують задачу знаходження співпадінь частин об'єктів навіть при умові, що фрагменти об'єкта так чи інакше пошкоджені ерозією, вицвітанням та іншими природними факторами. Використання області k -пікселів з подальшим екстраполюванням та пошуком співпадінь на основі кольору та неперервності країв є перспективним при вирішенні задачі відтворення цілісності форми паперу. Проте, залишається проблема втрати цілісності вмісту, що відображений на папері, а також проблема затертості, пошкодження мікрорель'єфу поверхні паперу, що може зробити текст нечитабельним.

По друге, для вирішення задачі втрати цілісності та якості вмісту паперу, є перспективним використання карт Кохонена, що розглядається на прикладі задачі відтворення та редагування зображень. Так як нейромережа на основі карт Кохонена шукає нейрони, які найбільше схожі до шуканого фрагмента, – це дозволяє максимально точно відтворити контент, що постраждав внаслідок пошкодження паперу. Використання карт Кохонена є перспективним для відтворення пошкодженого контенту документа після його збірки, що може забезпечити експертам краще опрацювати отриманий матеріал в подальшому.

Таким чином, об'єднавши ключові аспекти проаналізованих досліджень задачі відтворення в інших предметних областях, зроблено висновки щодо подальших досліджень в контексті розробки інформаційної технології задачі відтворення пошкоджених паперів. Перспективою застосування такого інтегрованого підходу є важливі переваги, а саме – не тільки відтворення пошкодженої структури паперу, але й збереження контенту, що може бути спотворений в результаті порушення цілісності текстури матеріалу паперу.

Список літератури

- [1] М. А. Солоний, А. А. Яровий, "Перспективи застосування технологій нейронних мереж для задачі відтворення пошкоджених паперів," у *Збірник матеріалів Всеукраїнської науково-практичної конференції "Молодь в науці: дослідження, проблеми, перспективи (МН-2021)"*, (Вінниця, 01–14 травня 2021 р.). Вінниця, Україна: ВНТУ, 2021, с. 1-2. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/mn/mn2021/paper/viewFile/13252/11113>. Дата звернення: Травень 10, 2022.
- [2] М. А. Солоний, А. А. Яровий, "Аналіз інтелектуальних технологій в контексті задачі відтворення пошкоджених паперів," у *Збірник матеріалів Всеукраїнської науково-практичної конференції "Молодь в науці: дослідження, проблеми, перспективи (МН-2022)"*. Вінниця, Україна: ВНТУ, 2022, с. 1-3. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/16337/13751>. Дата звернення: Травень 10, 2022.
- [3] SOLVING ARCHAEOLOGICAL PUZZLES. [Електронний ресурс]. Режим доступу: <https://arxiv.org/pdf/1812.10553.pdf>. Дата звернення: Травень 10, 2022.
- [4] KOHONEN SELF-ORGANIZING MAPS. [Електронний ресурс]. Режим доступу: <https://towardsdatascience.com/kohonen-self-organizing-maps-a29040d688da>. Дата звернення: Травень 10, 2022.
- [5] Self Organizing Maps – Kohonen Maps. [Електронний ресурс]. Режим доступу: <https://www.geeksforgeeks.org/self-organising-maps-kohonen-maps/>. Дата звернення: Травень 10, 2022.
- [6] A multiscale neural network method for image restoration. [Електронний ресурс]. Режим доступу: <https://tema.sbmacc.org.br/tema/article/download/179/118>. Дата звернення: Травень 10, 2022.
- [7] Image inpainting based on self-organizing maps by using multi-agent implementation. [Електронний ресурс]. Режим доступу: <https://www.sciencedirect.com/science/article/pii/S1877050914012186>. Дата звернення: Травень 10, 2022.

Стаття надійшла: 18.05.2022.

References

- [1] M. A. Soloniy, A. A. Yaroviy, "Perspektyvy zastosuvannya tekhnolohii neironnykh merezh dlia zadachi vidtvorennia poshkodzhennykh paperiv," u *Zbirnyk materialiv Vseukrainskoi naukovo-praktychnoi konferentsii "Molod v nauksi: doslidzhennia, problemy, perspektyvy (MN-2021)"*, (Vinnytsia, 01–14 travnia 2021 r.). Vinnytsia, Ukraina: VNTU, 2021, s. 1-2. [Online]. Available: <https://conferences.vntu.edu.ua/index.php/mn/mn2021/paper/viewFile/13252/11113>. Accessed on: May 10, 2022 [in Ukrainian].
- [2] M. A. Soloniy, A. A. Yaroviy, "Analiz intelektualnykh tekhnolohii v konteksti zadachi vidtvorennia poshkodzhennykh paperiv," u *Zbirnyk materialiv Vseukrainskoi naukovo-praktychnoi konferentsii "Molod v nauksi: doslidzhennia, problemy, perspektyvy (MN-2022)"*. Vinnytsia, Ukraina: VNTU, 2022, s. 1-3. [Online]. Available: <https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/16337/13751>. Accessed on: May 10, 2022 [in Ukrainian].
- [3] SOLVING ARCHAEOLOGICAL PUZZLES. [Online]. Available: <https://arxiv.org/pdf/1812.10553.pdf>. Accessed on: May 10, 2022.
- [4] KOHONEN SELF-ORGANIZING MAPS. [Online]. Available: <https://towardsdatascience.com/kohonen-self-organizing-maps-a29040d688da>. Accessed on: May 10, 2022.
- [5] Self Organizing Maps – Kohonen Maps. [Online]. Available: <https://www.geeksforgeeks.org/self-organising-maps-kohonen-maps/>. Accessed on: May 10, 2022.

- [6] A multiscale neural network method for image restoration. [Online]. Available: <https://tema.sbmac.org.br/tema/article/download/179/118>. Accessed on: May 10, 2022.
- [7] Image inpainting based on self-organizing maps by using multi-agent implementation. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050914012186>. Accessed on: May 10, 2022.

Відомості про авторів

Солоний Максим Андрійович – аспірант кафедри комп'ютерних наук.

Яровий Андрій Анатолійович – доктор технічних наук, професор, завідувач кафедри комп'ютерних наук.

Іванчук Ярослав Володимирович – доктор технічних наук, доцент, професор кафедри комп'ютерних наук.

Озеранський Володимир Сергійович – кандидат технічних наук, старший викладач кафедри комп'ютерних наук.

M. A. Solonyi, A. A. Yarovy, Y. V. Ivanchuk, V. S. Ozeranskyi

PROSPECTS OF NEURAL NETWORK APPROACH TO THE PROBLEM OF DAMAGED PAPERS RESTORATION

Vinnitsia National Technical University, Vinnitsia

УДК 004.772

В. І. Чистов, К. С. Васюта

АНАЛІЗ МЕТОДІВ СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ДАНИХ В ІНФОРМАЦІЙНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

Анотація. Для маскування факту передачі інформації в інформаційно-телекомунікаційних мережах, останнім часом широко застосовуються методи мережевої стеганографії, які засновані на використанні структурних властивостей протоколів моделі OSI (Open System Interconnection - мережевої взаємодії відкритих систем). Це дозволяє приховано передавати, на основі фонового трафіку, важливі дані без істотного зниження швидкості передачі даних в базовому (відкритому) каналі. При адекватному виборі властивості (групи властивостей) протоколу (протоколів) моделі OSI, методи мережевої стеганографії не дозволяють стеганоаналітику виявити факт наявності прихованої передачі даних. Стосовно до мережевої стеганографії, процес виявлення прихованої передачі даних заснований на аналізі протокольних характеристик використовуваних протоколів моделі OSI на предмет відповідності стандартам. При використанні протоколів каналного та мережевого рівнів моделі OSI, як технологічної основи для організації прихованого каналу передачі даних, приховування здійснюється за рахунок розміщення даних, факт передачі яких повинен бути прихований, в видимих полях заголовків відповідних протоколів, тобто у відкритому вигляді. У зв'язку з тим, що технологія IP-шифрування охоплює лише корисне навантаження протоколів мережевого рівня, то доцільним є використання протоколів транспортного рівня моделі OSI. На даному рівні найпоширенішим є протокол TCP, при цьому він стандартизований і використовується протиборчими сторонами, в тому числі й у військовій сфері. В роботі проведено аналіз сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування та методів стеганографічної передачі даних в інформаційно-телекомунікаційних мережах. Також проаналізовано мережеві протоколи, які використовуються в інформаційних телекомунікаційних мережах розкрито поняття "мережева стеганографія", основним завданням якої є приховування самого факту передачі повідомлення в каналах передачі даних.

Ключові слова: інформаційно-телекомунікаційні мережі, мережева стеганографія, протокол, дейтаграма, стек TCP/IP.

Abstract. Recently, network steganography methods based on the use of structural properties of OSI (Open System Interconnection) protocols have been widely used to mask the fact of information transmission in information and telecommunication networks. This allows to covertly transmit important data based on background traffic, without significantly reducing the data rate in the base (open) channel. With the correct choice of properties (groups of properties) of the protocol (protocols) of the OSI model, the methods of network steganography do not allow the stegananalyst to detect the fact of hidden data transmission. In network steganography, the process of detecting hidden data transmission is based on the analysis of the protocol characteristics of the used protocols of the OSI model for compliance with standards. When using protocols of channel and network levels of the OSI model, as a technological basis for organizing a hidden data transmission channel, concealment is carried out by placing data, the fact of transmission of which must be hidden, in the visible fields of the headers of the corresponding protocols, i.e. in open form. Due to the fact that the IP encryption technology covers only the payload of network layer protocols, it is advisable to use transport layer protocols of the OSI model. At this level, the TCP protocol is the most common, and it is standardized and used by opposing parties, including the military. The paper analyzes the current state of hidden data transmission in public information telecommunication networks and methods of steganographic data transmission in information and telecommunication networks. The network protocols used in information telecommunication networks were also analyzed, the concept of "network steganography" was revealed, the main task of which is to hide the very fact of message transmission in data transmission channels.

Key words: information and telecommunication networks, network steganography, protocol, datagram, TCP/IP stack.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-61-67>.

Вступ

Останнім часом, методи прихованої передачі даних в інформаційно-телекомунікаційних мережах (ІТКМ), що використовують особливості протоколів моделі OSI, набули широкої популярності. Всі протоколи моделі OSI виконані у вигляді стандартів RFC (Request For Comments) і носять рекомендаційний характер, не примушуючи до реалізації протоколів у всіх тонкощах, але основний акцент ставиться на обов'язковій наявності можливості сумісного використання усіх розроблених версій.

Множину таких методів об'єднує в собі "мережева стеганографія", основним завданням якої є приховування самого факту передачі повідомлення, що підсилює систему захисту інформації ще одним рівнем.

Мережева стеганографія – напрям комп'ютерної стеганографії, об'єктом вивчення якої, є виявлення властивостей (особливостей) протоколів моделі OSI, придатних для організації прихованих каналів передачі даних.

WLAN (Wireless Local Area Networks) стеганографія ґрунтується на методах, які використовуються для передачі стеганограм в бездротових мережах. Практичний приклад WLAN стеганографії – це система Hidden Communication System for Corrupted Networks (HICCUPS) [2]. Основою цих методів є недоліки, властиві бездротовим мережам. Ці недоліки іноді викликають викривлення енергетичних характеристик сигналів. В результаті цих викривлень час від часу з'являються "некоректні" пакети, контрольна сума яких не збігається з заявленою. Для реалізації такого роду методів, необхідно володіти актуальною статистикою активності в мережі в використовуємому середовищі, для запобігання виникненню аномальної активності в цій самій мережі.

Lost Audio Packets Steganography стеганографія або LACK стеганографія являє собою маскування повідомлень під час розмов із застосуванням IP-телефонії. Прикладом є застосування пакетів що затри-

муються (навмисно пошкоджуються, ігноруються) приймачем або прикладною програмою, але не додатком для стеганографії [3].

У зв'язку із тим, що найпоширенішим в інтернеті є стек протоколів TCP/IP, то доречним є побудова стеганографічних каналів на його базі.

Під мережевою стеганографією на мережевому рівні моделі OSI (далі IP - стеганографія), розуміється група методів мережевої стеганографії, в яких основою стегоконтейнеру є невикористані (зарезервовані) місця в заголовках і полях даних IP - дейтаграм.

Відповідно моделі OSI і принципам стеганографічної передачі даних, необхідно проаналізувати можливість використання методів IP-стеганографії для досягнення мети дослідження.

Актуальність

Актуальність роботи обумовлена необхідністю забезпечення надійного прихованого обміну інформації в умовах можливих атак на стеганографічні системи передачі даних.

Мета

Аналіз сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування та методів стеганографічної передачі даних в інформаційних телекомунікаційних мережах.

Задачі

1. Аналіз сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування.
2. Аналіз мережевих протоколів, які використовувалися в інформаційних телекомунікаційних мережах.
3. Аналіз методів стеганографічної передачі даних в інформаційних телекомунікаційних мережах.
4. Аналіз методів побудови мережевих стеганографічних каналів та можливих атак на стеганографічні системи передачі даних.

Розв'язання задач

Призначенням мережевого рівня моделі OSI є організація зв'язку станцій, що з'єднані з різними логічними каналами та/або роз'єднані другими логічними каналами. Функцією даного рівня в першу є вибір оптимальної черговості каналів між станціями у процесі передачі пакету (протокольного блоку даних на рівні мережі). Історично склалося, що перші мережеві протоколи розроблялися з метою використання їх в глобальних мережах (ГМ). Це можна обґрунтувати великою кількістю вузлів в ГМ – однією з найсуттєвіших проблем в роботі є досягнення ефективної маршрутизації. Одночасно з'явився термін стратегій передачі – данограма віртуальних каналів. Данограмна транспортна мережа – це мережа що передає незалежні пакети даних – данограми. Принцип роботи такої мережі схожий на роботу звичайної пошти – листи ніяк не пов'язані один з одним і можуть загубитися.

Перед тим, як почати передачу даних в мережі віртуальних каналів між процесами налагоджується віртуальний канал, який функціонує впродовж усього сеансу зв'язку. Роботу мережі віртуальних каналів можна порівняти з роботою міської телефонної мережі. Насамперед налагоджується канал зв'язку, послідовність інформації, яка передається, зберігається. Данограмна транспортна мережа відправляє пакети набагато швидше за мережу віртуальних каналів, але не забезпечує гарантії того, що пакет дійде до адресата (черговість надходження пакетів випадкова; є ймовірність втрати певних пакетів та перенасичення буферів). Мережа віртуальних каналів повільніша, але дає гарантія того, що пакет дійде до адресату (зберігається черговість надходження пакетів; відбувається припинення надходження пакетів від джерела якщо вузол перенасичений).

Одним із прикладів використання полів заголовків протоколу IP є метод, заснований на модифікації полів "identification" і "fragmentoffset" [4] – [7] при встановленому прапорі "DF" (do not fragment – НЕ фрагментувати). Якщо встановлений прапор DF, модуль IP не стане фрагментувати дейтаграму. Замість цього дейтаграма відкидається і по протоколу ICMP генерується повідомлення про помилку – "необхідна фрагментація, але встановлений прапор заборони фрагментації", яке посилається відправнику пакета. Якщо IP-дейтаграма була фрагментована, то кожен фрагмент стає окремим пакетом зі своїм власним IP-заголовком. Такі пакети маршрутизуються незалежно і, як наслідок, фрагменти дейтаграми можуть приходити в точку призначення з порушенням їх черговості. Однак в IP-заголовках фрагментів міститься вся необхідна інформація для їх правильного складання в пункті призначення.

Фрагментація в IP виконується незалежно від транспортного рівня моделі OSI. Не дивлячись на таку прозорість, фрагментація може привести до небажаних наслідків, які позначаються на рівнях вище IP.

Справа в тому, що через втрату одного фрагмента потрібно передати повторно всю дейтаграму, а оскільки в самому протоколі IP не передбачені таймаут і повторна передача, то ці функції повинні бути покладені на вищі рівні. Протокол TCP здійснює повторну передачу з таймаут, а UDP – ні [8]. Якщо виявиться, що втрачено певну частину сегмента TCP, то з таймаут буде повторено передачу всього сегменту TCP. Повторна передача окремого фрагмента IP-дейтаграми неможлива в принципі. Дійсно, якщо

фрагментацію зробив не хост-джерело дейтаграми, а один з проміжних маршрутизаторів, то джерело не може знати, яким саме чином було виконано розбиття на фрагменти. Вже з однієї цієї причини бажано вживати заходів для запобігання фрагментації. Фрагментація пакетів в IP є штатною ситуацією, тому використання раніше зазначених полів заголовків IP-пакетів як стежоконтейнер є цілком доцільним методом для організації прихованого каналу зв'язку. При правильному виборі розміру пакету можна домогтися виконання наступної умови:

$$L \leq PMTU, \quad (1)$$

де L – довжина пакету;

MTU – maximum transmission unit (максимальний розмір корисного блоку даних);

$PMTU$ – MTU траси від джерела до кінцевого адресата пакета.

$$PMTU = \min MTU_i, \quad (2)$$

де $\min MTU_i$ – мінімальне значення MTU серед інтерфейсів маршруту, по якому пройде пакет.

При виконанні умови (1) необхідність фрагментації пакетів на інтерфейсах маршруту відсутня. Це означає, що поля "identification", "flags", "fragmentoffset" оброблятися проміжними маршрутизаторами не будуть. В такому випадку, при використанні цих полів як стежоконтейнер, інформація вбудована в нього буде передана без змін. Ємність такого стежоконтейнер може становити до 32 біт.

Використання даного методу для досягнення мети дослідження недоцільно, так як порушується стандартні вимоги до протоколу IP, а приховувані дані розташовуються в заголовках IP-пакетів в явному вигляді.

На сучасному етапі метод "DF", є єдиним описаним методом мережевий стеганографії, застосовуваний на мережевому рівні моделі OSI. Але слід зазначити, що можуть існувати й інші поля заголовка IP-дейтаграми, які можливо використовувати для організації прихованих каналів обміну інформацією в інформаційно-телекомунікаційних мережах (ІТКМ). До таких поліф відносяться опції IPv4, розмір яких може досягати 40 байт (рис. 1).

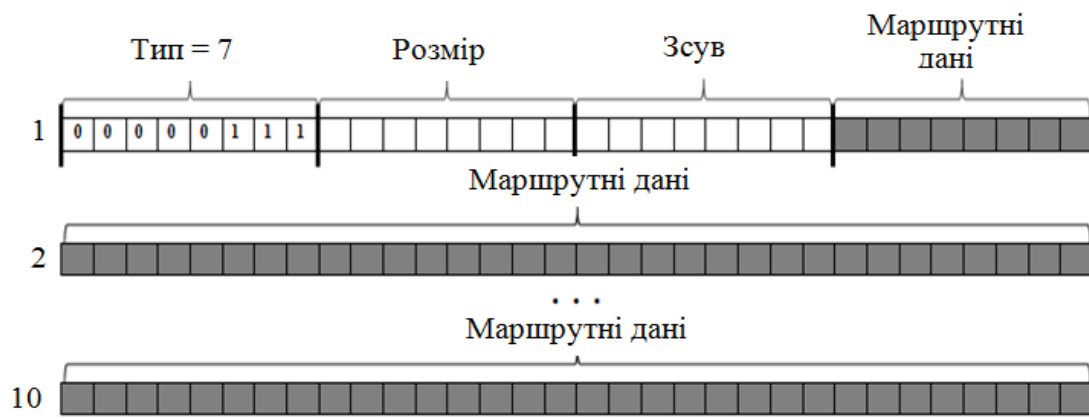


Рисунок 1 – Вид поля опції "Запис маршруту"

До опцій, які можна використовувати з метою прихованої передачі даних можна віднести наступні: "запис маршруту", "часовий штамп", "маршрутизація від джерела". Спільною рисою перерахованих опцій є виділення достатнього (до 40 октетів) місця в заголовку IP-пакету для їх реалізації. Поле опцій є обов'язковим, а їх підтримка повинна реалізуватися у всіх модулях IP (на хостах і шлюзах). Використання опцій визначається для окремої дейтаграми, а не для реалізації модуля. Теоретична основа "методу опцій" описана на прикладі опцій "запис маршруту" і "часовий штамп". При використанні в якості стежоконтейнера поля для запису проміжних вузлових пристроїв (опція "запис маршруту" або Record Route (RR)), можливо досягти розміру контейнера до 37 байт. Опція RR призначена для запису в заголовок дейтаграми IP-адрес вихідних інтерфейсів маршрутизаторів, що пересилали дану дейтаграму. При використанні даної опції представляється можливим записати до 9 IP-адрес. Це пов'язано із тим, що в IP-дейтаграми відведено до 40 байтів для опису опцій, 3 з яких - заголовок опції RR.

Опція починається з поля типу опції, за яким слід поле довжини, що враховує Type = 7 повний розмір опції (тип, розмір, зсув, маршрутні дані). Третій октет містить покажчик на октет, з якого починається наступна область запису маршруту. Зсув відраховується від початку опції, тому значення покажчика

не може бути менше 4. Хост, що відправляє дейтаграму, повинен забезпечити достатній простір (розмір опції) для запису адрес на шляху до одержувача. У вихідній дейтаграмі поля адрес повинні мати нульові значення.

Якщо поле маршрутних даних вже заповнено (значення покажчика перевищує розмір опції), дейтаграма пересилається без подальшого запису маршруту. Якщо простір, що залишився для запису маршрутних даних недостатньо для включення адреси, дейтаграма розглядається як помилкова та відкидається. У таких випадках відправник дейтаграм може бути переданий ICMP повідомлення про помилку в параметрах. Тому, якщо на передаючій стороні записати приховану інформацію в поля, призначені для запису IP-адрес вихідних інтерфейсів, а для полів "зсув" та "розмір" буде виконано умова (1), то ця дейтаграма буде доставлена без змін.

$$L_p < L_1, \quad (3)$$

де L_p – октет маршрутних даних, починаючи з якого буде оброблятися наступний параметр, який застосовується в опорній опції;

L_1 – значення розміру опції (в октетах), з урахуванням полів типу та розміру опції, а також октету покажчика та власне опції.

Для реалізації описаного способу, необхідно мати встановлене програмне забезпечення на стороні відправника та одержувача інформації, що приховується. Ситуація при якій поточний маршрутизатор не зможе записати необхідну в опції інформацію, є штатною для протоколу IP [9]. Подібний підхід можливо застосувати й до решти опцій IP – SR (source route – маршрутизація від джерела), TS (time stamp – часовий штамп), при виконанні умови (3). Для запису, необхідних даних для опцій "маршрутизація від джерела" і "запис маршруту" відводиться 37 байт, а для опції "часовий штамп" – 36 байт в кожній IP-дейтаграмі, що є ємністю такого стежоконтейнеру. Менша ємність стежоконтейнера, при використанні в якості опорної, опції "часовий штамп" (рис. 2), обумовлена тим, що в четвертому октеті поля опції зберігається інформація, необхідна для виконання призначення опції.

Поле "надлишок" показує кількість маршрутизаторів, які не змогли виконати необхідну операцію. Поле "прапор" може набувати таких значень:

- 0 – проміжні маршрутизатори повинні записувати тільки часові мітки, які зберігаються в послідовності 32-бітових слів;
- 1 – перед кожною позначкою поміщається IP-адреса, яка реєструє мітку модуля;
- 3 – поля адрес вказуються задалегідь і модуль IP поміщає часову мітку тільки в тому випадку, коли адреса цього модуля вказана наступною у списку адрес опції.

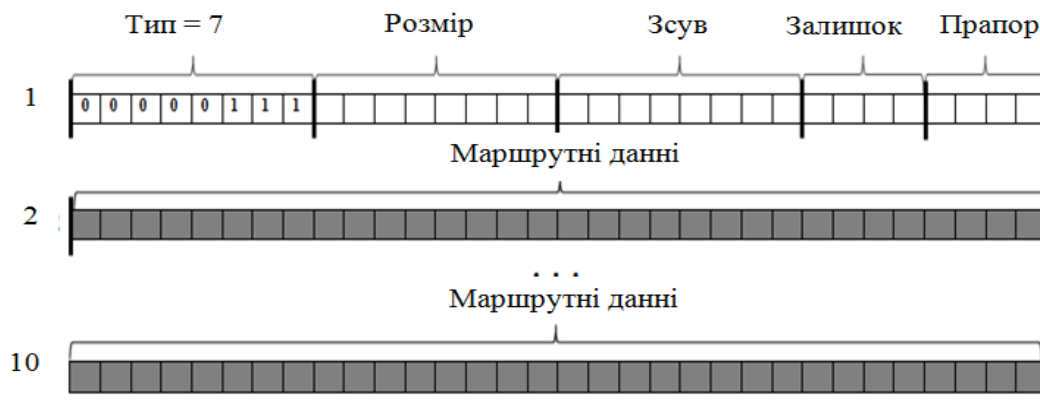


Рисунок 2 – Вид поля опції "Часовий штамп"

Використання даного методу для досягнення мети дослідження недоцільно з огляду на те, що приховувані дані розташовуються в полі опцій заголовків IP-пакетів в явному вигляді.

Під мережевою стеганографією на транспортному рівні моделі OSI (далі TCP – стеганографія), розуміється група методів мережевої стеганографії, в яких основою стежоконтейнер є технологічні особливості протоколів транспортного рівня моделі OSI.

Одним з представників методів TCP – стеганографії, є метод на основі управління довжиною поля корисного навантаження протоколу TCP.

Суть методу DL (DataLength) полягає в тому, що секретний текст представляють у вигляді послідовності біт, яку передають одержувачу частинами. Це пов'язано з тим, ємність такого стежоконтейнера

обмежена і в разі необхідності передачі великої кількості інформації, що приховується, її необхідно розбивати на порції. Стегоконтейнером є довжина поля даних кожного інформаційного TCP-сегмента, представлена в двійковій формі обчислення. В [10] задекларовано, що у випадку хендшейку, на початку TCP-сесії, сторони заздалегідь не домовляються про допустиме максимальне значення MSS (Maximum Segment Size – максимальний розмір сегменту), то його значення приймається за замовчуванням рівним 536 байтам. В роботі [11] автор пропонує приховано передавати інформацію, представлену у вигляді тексту, де кожній букві відповідає двійкова послідовність з прийнятною таблицею кодування. Для даного методу це може бути кодування windows-1251 (таблиця CP1251). Це кодування є 8-розрядною. Довжина поля даних TCP-сегмента наступна:

$$DL = MSS - L_4 = 536 - 20 = 516, \quad (4)$$

де L_4 – довжина заголовку TCP-сегмента без опцій.

В цьому випадку, кількість розрядів двійкового значення довжини відкритого тексту (ДВТ) відповідає

$$L_{OT} = L_m - 1, \quad (5)$$

де $L_m = \log_2(DL) \approx 9,07$, при округленні до найближчого більшого відповідає 10 розрядів.

TCP-дамп процесу передачі даних, заснованому на методі DL, зображений на рис.3. У методі закладена необхідність отримання підтверджень про доставку кожного сегмента до відправки наступного. Для цього використовується прапор PUSH (прапор проштовхування даних).

```
TCP: 50240 > scp-config [SYN] Seq=0 Win=32792 Len=0 MSS=16369 TSV=528243
TSER=0 WS=6
TCP: scp-config > 50240 [SYN, ACK] Seq=0 ACK=1 Win=32768 Len=0 MSS=16369
TSV=528243
TSER=528243
TCP: 50240 > scp-config [ACK] Seq=1 Ack=1 Win=32832 Len=0 TSV=528243
TSER=528243
TCP: 50240 > scp-config [PSH, ACK] Seq=1 Ack=1 Win=32832 Len=116 TSV=529497
TSER=528243
TCP: scp-config > 50240 [ACK] Seq=1 ACK=117 Win=32768 Len=0 TSV=529497
TSER=529497
TCP: 50240 > scp-config [PSH, ACK] Seq=117 Ack=1 Win=32832 Len=101 TSV=529523
TSER=528497
```

Рисунок 3 – TCP-дамп при передачі даних по методу DL

Для досягнення більшої стійкості до виділення прихованої інформації автор використовує криптографію. А саме, використання шифрування самого приховуваного тексту, розсіювання приховуваного тексту в двійкових значеннях довжини полів даних TCP-сегментів, задіяння секретної маски, що представляє собою двійкову послідовність, поодинокі значення яких відповідає інформаційним, а нульові – сегментам, що камуфлюють. Даний метод має можливість передавати будь-які дані, які можливо уявити 8 розрядами в двійковій системі числення. Це може бути: текст, зображення, аудіозапис, відеозапис.

В [5] запропоновано метод, який дозволяє передавати приховувані дані всередині пакетів TCP, що відправляються нібито для виправлення невдало переданих даних. Цей алгоритм отримав назву RSTEG (Retransmission Steganography – стеганографія в повторній передачі).

Описаний метод прихованої передачі даних для досягнення мети дослідження непридатний, тому що порушуються стандартні вимоги до протоколу TCP, в частині оптимального використання каналних ресурсів, і знижується більш ніж в два рази швидкість передачі даних в базовому віртуальному каналі передачі даних.

Також, викликає інтерес метод TCP-стеганографії заснований на управлінні ретрансляції фрагментів протоколу TCP – RSTEG.

Одержувач приймає початковий пакет і відправляє повідомлення про успішний прийом. Замість того, щоб передати наступний пакет, відправник ігнорує повідомлення про успішний прийом і відправляє

пакет з прихованим змістом, але цей пакет має такий же ідентифікатор, що і попередній, а системи аналізу мережевого трафіку вже не перевіряють повторний пакет.

Для всіх систем мережевого захисту новий пакет з секретним вмістом не відрізняється від початкового пакету, в якому не містилося нічого підозрілого. Коли повторно переданий пакет досягає приймаючої сторони, з нього витягується прихована інформація.

Висновки

В даній роботі основну увагу приділено аналізу сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування та методів стеганографічної передачі даних в інформаційно-телекомунікаційних мережах.

Проведено аналіз мережевих протоколів, які використовуються в інформаційних телекомунікаційних мережах розкрито поняття "мережева стеганографія", основним завданням якої є приховування самого факту передачі повідомлення в каналах передачі даних.

Окремого розгляду вимагають питання дослідження можливих атак на стеганографічні системи (СГС) передачі даних та розробки пропозицій щодо покращення показників ефективності щодо прихованості управління при передачі даних в інформаційній телекомунікаційній мережі, що і буде напрямком подальших досліджень.

Список літератури

- [1] W. Mazurczyk, K. Szczypiorski, "Steganography of VoIP Streams," Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications. [Online]. Available: <http://arxiv.org/pdf/0805.2938v1/>. Accessed on: May 14, 2022.
- [2] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks," Warsaw University of Technology, Institute of Telecommunications. [Online]. Available: <https://goo.gl/ZU9tDM>. Accessed on: May 4, 2022.
- [3] D. Kundur, K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," Proc. Texas Wksp. Securit of Information Systems, Apr. 2003. [Online]. Available: <http://arxiv.org/pdf/1207.0917.pdf>. Accessed on: October 10, 2021.
- [4] E. Cauich, R. Gómez Cárdenas, R. Watanabe, "Data Hiding in Identification and Offset IP Fields," in *Proceedings of 5th International School and Symposium of Advanced Distributed Systems (ISSADS)*, Jan. 2005, pp. 118-125. [Online]. Available: <https://goo.gl/2bjjXZ>. Accessed on: October 29, 2021.
- [5] Theodore G. Handel, Maxwell T. Sandford II, *Hiding data in the OSI network model*. [Online]. Available: <https://goo.gl/hz8X1m>. Accessed on: September 20, 2021.
- [6] О. Ю. Пескова, Г. Ю. Халабурда, "Применение сетевой стеганографии для защиты данных, которые передаются по открытым каналам Интернет," *Объединённая конференция "Интернет и современное общество"*. [Електроний ресурс]. Режим доступу: <https://goo.gl/qtC7D3>. Дата звернення: Серп. 19.2021.
- [7] Е. О. Саватєєв, "Построение стеганографической системы на базе протокола IPv4". [Електроний ресурс]. Режим доступу: <https://goo.gl/wUogUB>. Дата звернення: Серп. 30.2021.
- [8] "Internet protocol – DARPA Internet Program Protocol Specification". RFC-768. User Datagram Protocol, 28 August 1980. [Online]. Available: <https://tools.ietf.org/html/rfc768>. Accessed on: October 22, 2021.
- [9] "Internetprotocol – DARPA Internet Program Protocol Specification" RFC-791 USC / Information Sciences Institute, September 1981 [Online]. Available: <http://www.rfc-base.org/txt/rfc-791.txt>. Accessed on: October 21, 2021.
- [10] "Internet protocol – DARPA Internet Program Protocol Specification" RFC-793 USC / Transmission control protocol, September 1981 [Online]. Available: <https://tools.ietf.org/html/rfc793>. Accessed on: October 21, 2021.
- [11] В. П. Орлов, "Методы скрытой передачи информации в телекоммуникационных сетях," дис. канд. техн. наук: 05.12.13. Самара, 2012.

Стаття надійшла: 20.05.2022.

References

- [1] W. Mazurczyk, K. Szczypiorski, "Steganography of VoIP Streams," Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications. [Online]. Available: <http://arxiv.org/pdf/0805.2938v1/>. Accessed on: May 14, 2022.
- [2] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks," Warsaw University of Technology, Institute of Telecommunications. [Online]. Available: <https://goo.gl/ZU9tDM>. Accessed on: May 4, 2022.
- [3] D. Kundur, K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," Proc. Texas Wksp. Securit of Information Systems, Apr. 2003. [Online]. Available: <http://arxiv.org/pdf/1207.0917.pdf>. Accessed on: October 10, 2021.

- [4] E. Cauich, R. Gómez Cárdenas, R. Watanabe, "Data Hiding in Identification and Offset IP Fields," in *Proceedings of 5th International School and Symposium of Advanced Distributed Systems (ISSADS)*, jan. 2005, pp. 118-125. [Online]. Available: <https://goo.gl/2bjjXZ>. Accessed on: October 29, 2021.
- [5] Theodore G. Handel, Maxwell T. Sandford II, *Hiding data in the OSI network model*. [Online]. Available: <https://goo.gl/hz8X1m>. Accessed on: September 20, 2021.
- [6] O. Y. Peskova, G. Y. Halaburda, "Primenenie setevoy steganografii dlya zashchity dannyh, kotorye peredayutsya po otkrytym kanalam Internet," *Conference "Internet i sovremennoe obshchestvo"*. [Online]. Available: <https://goo.gl/qtC7D3>. Accessed on: Aug. 19.2021 [in Russian].
- [7] E. O. Savateev, "Postroenie steganograficheskoy sistemy na baze protokola IPv4," [Online]. Available: <https://goo.gl/wUogUB>. Accessed on: Aug. 30.2021 [in Russian].
- [8] "Internet protocol – DARPA Internet Program Protocol Specification". RFC-768. User Datagram Protocol, 28 August 1980. [Online]. Available: <https://tools.ietf.org/html/rfc768>. Accessed on: October 22, 2021.
- [9] "Internetprotocol – DARPA Internet Program Protocol Specification" RFC-791 USC / Information Sciences Institute, September 1981 [Online]. Available: <http://www.rfc-base.org/txt/rfc-791.txt>. Accessed on: October 21, 2021.
- [10] "Internet protocol – DARPA Internet Program Protocol Specification" RFC-793 USC / Transmission control protocol, September 1981 [Online]. Available: <https://tools.ietf.org/html/rfc793>. Accessed on: October 21, 2021.
- [11] V. P. Orlov, "Metody skrytoy peredachi informacii v telekomunikacionnyh setyah", cand. of technical sciences thesis: 05.12.13. Samara, 2012 [in Russian].

Відомості про авторів

Чистов Валерій Ігорович – ад'юнкт науково-організаційного відділу Харківського національного університету Повітряних Сил імені Івана Кожедуба.

Васюга Костянтин Станіславович – доктор технічних наук, професор, заступник начальника Харківського національного університету Повітряних Сил імені Івана Кожедуба з навчальної роботи.

V. I. Chystov, K. S. Vasiuta

ANALYSIS OF THE CURRENT STATE OF HIDDEN DATA TRANSMISSION IN THE PUBLIC INFORMATION TELECOMMUNICATIONS NETWORK

Ivan Kozhedub Kharkiv National University of the Air Force, Kharkiv

КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 621.3

О. Д. Азаров, А. С. Фігас

ВИСОКОЛІНІЙНА СИСТЕМА АНАЛОГ-КОД-АНАЛОГ З
ВАГОВОЮ НАДЛИШКОВІСТЮ НА БАЗІ
ПЕРЕТВОРЮВАЧІВ СТРУМІВ

Вінницький національний технічний університет, Вінниця

Анотація. В теперішній час аналого-цифрові- і цифроаналогові- перетворювачі широко застосовуються для операцій з сигналами і дозволяють проводити запис і зберігання сигналів, виведення сигналу в аналоговій формі, виконання операцій з сигналами, генерування сигналів довільної форми. В ряді застосувань аналого-цифрові- і цифроаналогові- перетворювачів для обробки сигналів потрібна висока роздільна здатність, низькі шуми та висока лінійність передатної характеристики перетворення аналог-цифра-аналог для забезпечення низьких нелінійних, частотних, фазових спотворень сигналів й високого відношення сигнал/шум. Розглянуто метод побудови високолінійної системи аналог-код-аналог з ваговою надлишковістю на базі перетворювачів струмів. Розглянуті особливості застосування надлишкових позиційних систем числення в аналого-цифровому та цифроаналоговому перетворенні. Вказана здатність надлишкових позиційних систем числення забезпечувати відсутність «розривів» у перетворювальній характеристиці, викликаних відхиленнями реальних ваг розрядів від їхніх розрахункових значень, а також здатність істотно коригувати вихідні похибки цифроаналогових перетворювачів, а саме лінійність перетворювальної характеристики. Вказана здатність надлишкових позиційних систем числення забезпечувати незважаючи на подовження розрядної сітки, істотне збільшення швидкодії. Наведена схема перетворювача аналог-код-аналог на основі надлишкових позиційних систем числення з буферним накопиченням відліків сигналів в пам'яті. Наведений розрахунок похибок відтвореного перетворювачем аналог-код-аналог сигналу. Обґрунтована актуальність і практична доцільність застосування надлишкових систем числення для отримання високої розрядності та швидкодії систем аналого-код-аналог при використанні неточних компонентів.

Ключові слова: перетворення сигналів, вагова надлишковість, АЦП, ЦАП.

Abstract. At present, analog-to-digital and digital-to-analog converters are widely used for operations with signals and allow recording and storing signals, outputting a signal in analog form, performing operations with signals, and generating arbitrary waveforms. In a number of applications of analog-to-digital and digital-to-analog converters for signal processing, high resolution, low noise and high linearity of the analog-to-digital-to-analog transfer characteristic are required to provide low non-linear, frequency, phase distortion of signals and a high signal-to-noise ratio. A method for constructing a high-linear analog-code-analog system with weight redundancy based on current converters is considered. The features of the use of redundant positional number systems in analog-to-digital and digital-to-analog conversion are considered. The ability of redundant positional number systems to ensure the absence of «gaps» in the conversion characteristic caused by deviations of the real weights of digits from their calculated values, as well as the ability to significantly correct the initial errors of digital-to-analog converters, namely the linearity of the conversion characteristic, is indicated. The ability of redundant positional number systems to provide, despite the lengthening of the bit grid, a significant increase in performance is indicated. The scheme of analog-code-analog converter based on redundant positional number systems with accumulation of buffer samples of signals in memory is presented. Calculation of errors of the analog-code-analog signal reproduced by the converter is given. The relevance and practical expediency of using redundant number systems to obtain high bit capacity and speed of analog-code-analog systems using inaccurate components is substantiated.

Key words: signal conversion, weight redundancy, ADC, DAC.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-68-73>.

Вступ

В теперішній час АЦ- і ЦА- перетворювачі широко застосовуються для операцій з сигналами [1-3]. Такі системи дозволяють проводити: запис і зберігання сигналів – проводитися фіксація значень сигналу і забезпечується можливість їх тривалого зберігання в цифровій формі без втрати інформації; виведення сигналу в аналоговій формі – проводиться зворотне перетворення збереженого сигналу в аналогову форму в необхідний час; виконання операцій з сигналами – додавання, віднімання, множення, інтегрування і більш складні їх похідні, такі як знаходження кореляційних залежностей, перетворення Фур'є, фільтрація; генерування сигналів довільної форми – будь-яка математично визначена і розрахована в цифровій формі функція може бути перетворена в аналоговий сигнал [1-3]. В ряді застосувань АЦ- і ЦА- перетворювачів для обробки сигналів потрібна висока роздільна здатність, низькі шуми та висока лінійність передатної характеристики перетворення аналог-цифра-аналог. Ці параметри в наскрізному тракту перетворення й опрацювання сигналів повинні забезпечити низькі нелінійні, частотні, фазові спотворення сигналів й високе відношення сигнал/шум.

Актуальність

В багатьох сучасних застосуваннях систем обробки низькочастотних сигналів (вимірювання, звукові процесори) виникає необхідність в таких функціональних можливостях, як :

1) затримка аналогового сигналу на заданий чи змінюваний в процесі роботи час (декілька секунд). Наприклад, в радіо та телевізійному мовленні прямого ефіру такі пристрої повинні забезпечити попадання в ефір нетактичних висловлювань гостей студії або телефонних дозвонювачів. Також актуальна задача синхронізації відео і аудіосигналів, якщо один з них запізнюється через цифрове ущільнення й передавання по цифровим лініям зв'язку;

2) запам'ятовування фрагменту вимірюваного аналогового сигналу з метою наступного багатократного відтворення або аналізу, – наприклад, при діагностуванні автомобільних двигунів за акустичними параметрами їх роботи. Інший приклад – в медицині;

3) відтворення сигналу в зворотньому напрямку, або з іншою частотою дискретизації (пришвидшення або уповільнення сигналу). Прикладом можуть слугувати спеціальні методи шифрування аналогових сигналів.

Тому забезпечення високої роздільної здатності, низьких нелінійних, частотних, фазових спотворень сигналів й високого відношення сигнал/шум в системах аналог-код-аналог, в тому числі за рахунок застосування вагової надлишковості є важливою та актуальною задачею.

Мета

Створення високолінійної системи аналог-код-аналог з ваговою надлишковістю з використанням ЦАП на неточних компонентах.

Задачі досліджень

1. Проаналізувати існуючі методи побудови систем запису, запам'ятовування, обробки, відновлення та генерування сигналів на базі перетворювачів аналог-цифра-аналог.

2. Проаналізувати методи використання надлишковості при аналого-цифровому та цифро аналоговому перетворенні та їх переваги.

3. Розглянути методи побудови високолінійних швидкодіючих перетворювачів аналог-цифра-аналог з можливістю запам'ятовування та відтворення сигналів.

Розв'язання задач досліджень

Блок схема типової системи АЦА зображена на рисунку 1. Аналоговий вхідний фільтр (ФНЧ1) використовується для обмеження полоси частот вхідного аналогового сигналу, щоб забезпечити виконання умов теореми Котельникова. Аналого-цифровий перетворювач (АЦП) переводить сигнал в цифрову форму. Після цифрової обробки чи зберігання в цифровому пристрої (ЦП) сигнал за допомогою цифроаналогового перетворювача (ЦАП) знову переводиться в аналогову форму. Вихідний фільтр (ФНЧ2) згладжує вихідний сигнал і усуває небажані високочастотні компоненти, які виникають в наслідок шуму квантування. Створення систем такого типу з високою розрядністю та швидкодією потребує значного ускладнення та подорожчання АЦП та ЦАП і використання в цьому випадку надлишковості може дати значні переваги.

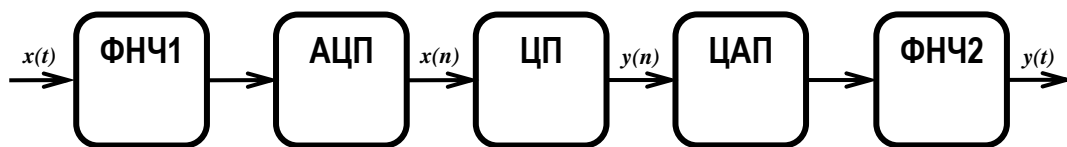


Рисунок 1 – Схема спрощеної АЦА системи.

Перспективним напрямком розвитку АЦП порозрядного наближення є їхня побудова з використанням надлишкових позиційних систем числення (НПСЧ) [4-6]. Проаналізуємо особливості САЦП на основі НПСЧ.

У НПСЧ використовується недвійкова основа системи числення $1 < \alpha < 2$, а ваги розрядів представляються у вигляді

$$Q_i = q \cdot \alpha^i, \quad (1.1)$$

де q – вага молодшого розряду.

Будь-яке дійсне число може бути представлено в НПСЧ у вигляді суми ваг розрядів

$$X = \sum_{i=0}^N a_i \cdot q \cdot \alpha^i, \quad (1.2)$$

де $a_i = \overline{0, 1}$ – двійковий i -ий біт N -розрядного результату перетворення.

Основна перевага НПСЧ, реалізована при аналого-цифровому перетворенні складається у відсутності «розривів» у перетворювальній характеристиці, викликаних відхиленнями реальних ваг розрядів від

їхніх розрахункових значень, рисунок 2. Для «двійкових» АЦП ці відхилення не повинні перевищувати половини молодшого розряду. Для АЦП на основі «золотої пропорції» відносна похибка ваг розряду за рахунок технологічних, температурних, часових факторів може досягати до 23,6%, що не приведе до пропусків кодів.

Як видно з викладеного, у САЦП на основі НПСЧ надлишковість виявляється тільки у співвідношенні між вагами розрядів ЦАП. Проте, теоретично обґрунтована, підтверджена результатами моделювання й практично перевірена в численних розробках [5,6] здатність САЦП істотно коригувати вихідні похибки ЦАП. Так, при вихідних відхиленнях ваг розрядів «надлишкового» ЦАП на рівні 5-10% вдається одержати після самокалібрування САЦП похибка лінійності 0.003%. Причому, самокалібрування може бути проведено в будь-який момент часу роботи САЦП, наприклад, при змінненні температури навколишнього середовища.

Очевидно, що описаний спосіб коригування ваг розрядів САЦП поряд з очевидними перевагами накладає також і певні обмеження. Так, при підсумовуванні ваг розрядів ЦАП повинен виконуватися принцип суперпозиції, що передбачає незалежність ваги розряду від станів («включене» або «виключене») інших розрядів. Необхідно також забезпечити й досить малий температурний і часовий дрейф ваг розрядів, якщо за умовами експлуатації АЦП у складі системи неможливо досить часто здійснювати самокалібрування.

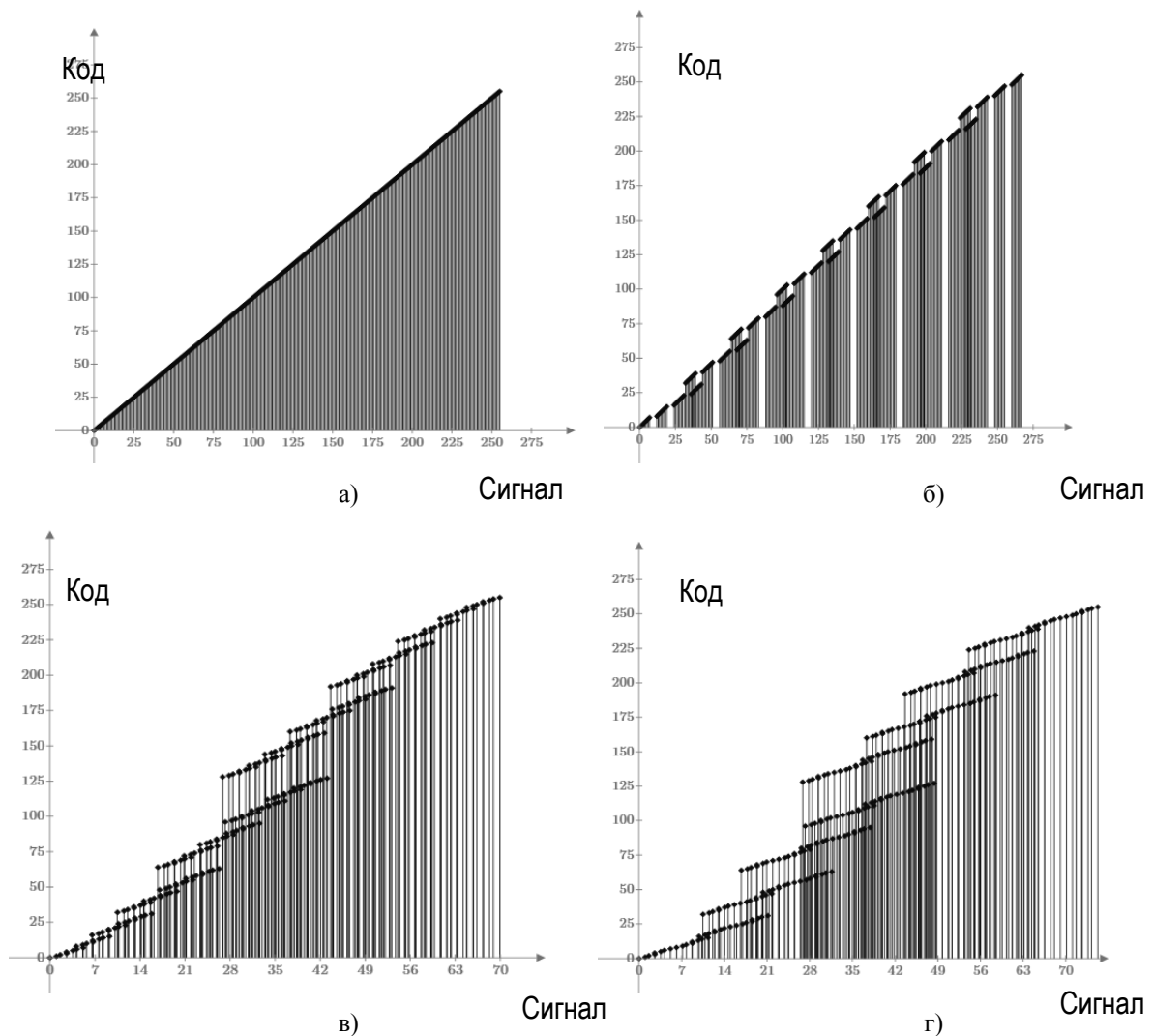


Рисунок 2 – Характеристики перетворення АЦП для різних систем числення: а) двійкова $\alpha=2$ без спотворень; б) двійкова $\alpha=2$ зі спотвореннями; в) надлишкова $\alpha=1,6$ без спотворень; г) надлишкова $\alpha=1,6$ зі спотвореннями

Число розрядів N_α , задіяних у надлишковому ЦАП, природно, більше ніж у двійковому N_2 й визначається зі співвідношення:

$$\alpha^{N_\alpha} = 2^{N_2} \Rightarrow N_\alpha = N_2 \cdot \log_\alpha 2 \quad (1.3)$$

Так, для побудови АЦП 16-ти розрядної точності ($N_2=16$) при $\alpha=1,618$ потрібен ЦАП на $N_\alpha=24$ розряду коду «золотої пропорції». Незважаючи на збільшення розрядної сітки, швидкодія АЦП на основі НПСЧ не зменшується, а навпаки, може бути істотно збільшена. Зазначений ефект виникає внаслідок витрати частини надмірності ваг розрядів на автокомпенсацію динамічних похибок із сигналу, що компенсує [5-6].

Відомо, що наявність при аналого-цифровому перетворенні динамічних похибок може призвести до появи розривів кодувальної характеристики. При правильному ж аналого-цифровому перетворенні наприкінці врівноважування похибка недовстановлення не повинна перевищувати половини молодшого розряду:

$$\Delta_g(t_{np}) = \left| A_{BX} - \sum_{i=0}^N Q_i(t-t_i) \right| \leq q/2, \quad (1.4)$$

де Δ_g – динамічна похибка квантування;

$Q_i(t-t_i)$ – вага i -го розряду, як функція від часу його включення t_i ;

$t_{np} = \Delta t \cdot N$ – сумарний час перетворення;

Δt – тривалість такту зрівноважування.

Наявність похибки на кожному з тактів врівноваження може привести або до невключення необхідного розряду, або до помилкового включення розряду, що перевищує по своїй вазі некомпенсований сигнал. У двійкових АЦП зазначені помилки не можуть бути виправлені на наступних тактах зрівноважування й приводять до похибок зрівноважування, що проявляються в розривах передатної характеристики. Мінімальна тривалість такту у двійковому АЦП визначається значенням [5]:

$$t_2 = \tau \cdot (N_2 + 1) \cdot \ln 2, \quad (1.5)$$

де τ – постійна часу перехідних процесів.

В АЦП на основі НПСЧ поява помилок типу «невключення» розряду компенсується на наступних тактах перетворення за рахунок включення групи більш молодших розрядів. Таким чином в АЦП на основі НПСЧ, вдається, незважаючи на подовження розрядної сітки, істотно збільшити швидкодію. Потенційні можливості розглянутих способів збільшення швидкодії можуть бути досягнуті тільки з урахуванням ряду факторів, пов'язаних з динамічними характеристиками ЦАП і схеми порівняння. Так, при перемиканні розряду важливим виявляється форма різницевого сигналу. Оптимальною є одноекспонентна форма залежності сигналу від часу, для якої й отримані наведені вище оцінки збільшення швидкодії. У реальних пристроях перехідні процеси відбуваються складніше: позначаються затримки включення розрядів, комутаційні перешкоди, перерегулювання, «затягування» і т.д. Вплив зазначених ефектів може бути зменшене за рахунок переходу на струмовий принцип побудови пристрою квантування й розробкою відповідних схемних рішень [7].

На рисунку 3 наведено запропоновану структурну схему АЦА-перетворювача на основі НПСЧ з буферним накопиченням відліків сигналів в пам'яті.

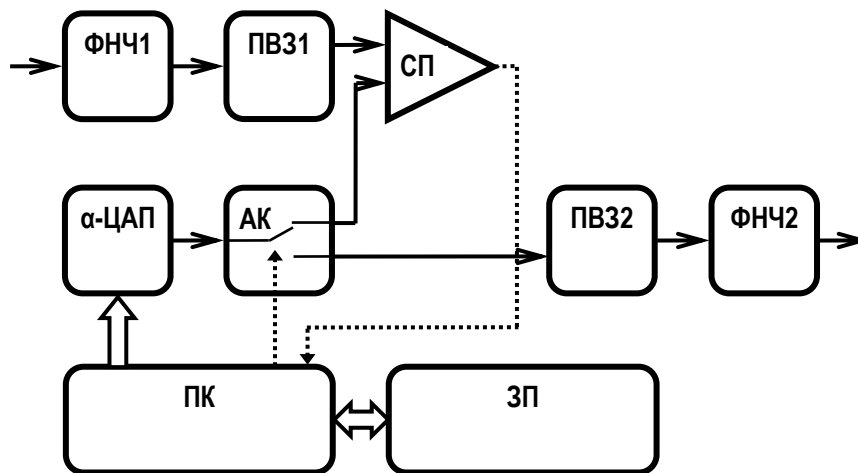


Рисунок 3 – Схема АЦА-перетворювача на основі НПСЧ з буферним накопиченням відліків сигналів в пам'яті

Надлишковий ЦАП на основі НПСЧ працює по чергово – в АЦП порозрядного врівноваження, та (або) в ЦАП. При цьому перетворення з НПСЧ в двійкову систему числення не здійснюється, в цифровій пам'яті зберігаються коди, отримані при АЦ-перетворення. За умови відсутності «розривів» характеристики зберігається задана якість АЦ-перетворення. Пристрої вибірки-зберігання потрібні для збереження аналогового сигналу на час перетворення. Процедури самокорекції для АЦП і ЦАП не потрібні.

Як було зазначено раніше передавальна характеристика (код-сигнал) для надлишкових систем числення залишається нерозривною навіть при істотній похибці ваг розрядів ЦАП або при значному скороченні часу встановлення сигналу на виході внутрішнього ЦАП в процесі порозрядного врівноваження в АЦП. Тобто для будь-якого значення вхідного сигналу $U_{X.BX}$ (в АЦП) існує така кодова комбінація K_X на вході внутрішнього ЦАП, що:

$$U_{X.BX} + \delta U_{BX.T} - U_{CAP}(K_X) < 1 MЗР, \quad (1.6)$$

де $\delta U_{BX.T}$ – похибка вхідного тракту. Якщо потім в якийсь інший момент часу подати отриману кодову комбінацію K_X на вхід того ж внутрішнього ЦАП, і використовувати аналоговий сигнал з його виходу в якості вихідного $U_{X.VIX}$, то він буде дорівнювати:

$$U_{X.VIX} = \delta U_{VIX.T} + U_{CAP}(K_X), \quad (1.7)$$

де $\delta U_{VIX.T}$ – похибка вихідного тракту. Звідки збережений вхідний сигнал і відновлений вихідний будуть пов'язані співвідношенням:

$$U_{X.VIX} = U_{X.BX} + \delta U_{BX.T} + \delta U_{VIX.T} + \delta U_{KB}, \quad (1.8)$$

де δU_{KB} – похибка квантування. Як можна бачити похибка відновленого сигналу не залежить від конкретних значень похибок внутрішнього ЦАП, єдина умова, яка до останнього висувається – це нерозривність його передатної характеристики (код-сигнал), тобто його похибки не повинні бути досить великими. В даному випадку є неважливою конкретна відповідність надлишкового коду його двійковому еквіваленту.

У зазначених раніше завданнях роботи з нестационарними сигналами операції запису і зберігання сигналів, операції відновлення сигналів і виконання операцій над сигналами в аналоговій формі не вимагають здійснення будь-якої математичної обробки їх цифрових еквівалентів, коди в надлишковій формі потрібно просто зберігати і використовувати для зворотного перетворення в необхідний час. Тобто також є неважливим конкретна відповідність надлишкового коду його двійковому еквіваленту. Таким чином створення систем аналого-код-аналог з високою розрядністю та швидкодією при використанні надлишковості не потребує значного ускладнення та подорожчання АЦП та ЦАП і має значні переваги. Також для підвищення швидкодії ЦАП може бути запропоновано використання при їх побудові принципу перетворення струмів [8].

Використання АЦП порозрядного врівноваження з ваговою надлишковістю у складі систем реєстрації аналогових сигналів має певні переваги порівняно з АЦП на основі двійкових систем числення, а саме:

- більшу швидкодію, що дозволяє збільшити кількість відліків на однакових проміжках часу, це в свою чергу знижує вимоги до ФНЧ на виході ЦАП;
- реалізація ЦАП з ваговою надлишковістю дозволяє зробити нерозривною характеристику перетворення незважаючи на використання цього ЦАП в АЦП з прискореною швидкодією. АЦП на базі такого ЦАП не буде мати пропусків кодів в характеристиці перетворення, а це дозволить зареєструвати значення аналогових сигналів у всьому діапазоні перетворення.

Висновки

1. Проаналізовано методи використання надлишковості при аналого-цифровому та цифро аналоговому перетворенні та її переваги.
2. Розглянуто методи побудови високолінійних швидкодіючих перетворювачів аналог-цифра-аналог з можливістю запам'ятовування та відтворення сигналів з використанням вагової надлишковості. Обґрунтована можливість значного підвищення швидкодії та зниження вартості.

Список літератури

- [1] Emmanuel C. Ifeachor (Author), Barrie W. Jervis, Digital Signal Processing: A Practical Approach 2nd Edition – Wokingham, England: Addison-Wesley Publishing Company, 2001.
- [2] W. Kesler, *The Data Conversion Handbook*. Burlington, USA: Newnes, 2005.

- [3] Ю. Р. Гнатек, *Справочник по цифроаналоговым и аналого-цифровым преобразователям: Пер. с англ.* Москва, СССР: Радио и связь, 1982.
- [4] А. П. Стахов, *Введение в алгоритмическую теорию измерения.* Москва, СССР: "Сов. Радио", 1977.
- [5] О. Д. Азаров. *Аналого-цифрове порозрядне перетворення на основі надлишкових систем числення з ваговою надлишковістю: монографія.* Вінниця, Україна: ВНТУ, 2010.
- [6] Л. В. Крупельницький, О. Д. Азаров, *Аналого-цифрові пристрої систем, що самокалібруються, для вимірювань і оброблення низькочастотних сигналів: монографія.* Вінниця, Україна: УНІВЕРСУМ-Вінниця, 2005.
- [7] O. D. Azarov, L. V. Krupelnitskyi, P. Komada, T. Ławicki, N. Askarova, A. Sagymbekova, "AD systems for processing of low frequency signals based on self calibrate ADC and DAC with weight redundancy", *Przegląd Elektrotechniczny*, volume R. 93, № 5, pp. 125-128. 2017.
- [8] О. Азаров, М. Обертюх, "Генератори однакових струмів із високими вихідними опорами для багатозрядних ЦАП", *Інформаційні технології та комп'ютерна інженерія*, т. 3, № 46, с. 33-39, 2019. doi: 10.31649/1999-9941-2019-46-3-28-38.

Стаття надійшла: 20.05.2022.

References

- [1] Emmanuel C. Ifeachor (Author), Barrie W. Jervis, *Digital Signal Processing: A Practical Approach* 2nd Edition – Wokingham, England: Addison-Wesley Publishing Company, 2001.
- [2] W. Kesler, *The Data Conversion Handbook.* Burlington, USA: Newnes, 2005.
- [3] Yu. R. Gnatek, *Spravochnik po cifroanalogovym i analogo-cifrovym preobrazovatelyam: Per. s angl.* Moskva, SSSR: Radio i svyaz', 1982 [in Russian].
- [4] A. P. Stahov, *Vvedenie v algoritmicheskuyu teoriyu izmereniya.* Moskva, SSSR: "Sov. Radio", 1977 [in Russian].
- [5] O. D. Azarov. *Analooho-tsyfrove porozriadne peretvorennia na osnovi nadlyshkovykh system chyslennia z vahovoiu nadlyshkovistiu: monohrafiia.* Vinnytsia, Ukraina: VNTU, 2010 [in Ukrainian].
- [6] L. V. Krupelnitskyi, O. D. Azarov, *Analooho-tsyfrovi prystroi system, shcho samokalibriuetsia, dlia vymiriuvan i obrobliannia nyzkochastotnykh syhnaliv: monohrafiia.* Vinnytsia, Ukraina: UNIVERSUM-Vinnytsia, 2005 [in Ukrainian].
- [7] O. D. Azarov, L. V. Krupelnitskyi, P. Komada, T. Ławicki, N. Askarova, A. Sagymbekova, "AD systems for processing of low frequency signals based on self calibrate ADC and DAC with weight redundancy", *Przegląd Elektrotechniczny*, volume R. 93, № 5, pp. 125-128. 2017.
- [8] O. D. Azarov and M. R. Obertiukh, "Generators of identical currents with high output resistance for multi-digit DACs", *ITKI*, vol. 46, no. 3, pp. 28–38, Dec. 2019, doi: 10.31649/1999-9941-2019-46-3-28-38 [in Ukrainian].

Відомості про авторів

Азаров Олексій Дмитрович – доктор технічних наук, професор, завідувач кафедри обчислювальної техніки.

Фігас Ганна Сергіївна – аспірант кафедри обчислювальної техніки.

O. D. Azarov, A. S. Figas

HIGH-LINEAR ANALOGUE-CODE-ANALOGUE SYSTEM WITH WEIGHT REDUNDANCY BASED ON CURRENT CONVERTERS

Vinnytsia National Technical University, Vinnytsia

УДК 004.21

Д. О. Каліновський, С. В. Осієвський

АНАЛІЗ МЕТОДІВ ТА МОДЕЛЕЙ ПРИЙНЯТТЯ РІШЕННЯ З ВИКОРИСТАННЯМ КАТЕГОРІЙ ТА СПОСОБІВ ВРАХУВАННЯ ВХІДНОЇ ІНФОРМАЦІЇ

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

Анотація. У статті запропоновано аналіз методів та моделей прийняття рішення в залежності від етапів процесу прийняття рішення, використання категорій та способів врахування вхідної інформації, яка описує умови в яких виконується завдання та складові самого завдання. Найбільш складніше в цьому процесі - це прийняти таке рішення в умовах дефіциту часу, інформаційної невизначеності та наявності протиріч у відповідній сфері. Тому формуючи управлінські рішення необхідно користуватись певною класифікацією, яка б відповідала сфері прийняття рішення і враховувала специфіку управління. Наведено класифікацію управлінських рішень, враховуючи основи теорії прийняття рішень, менеджменту та характеру задач, які вирішуються за допомогою взаємодії особи, яка приймає рішення та системою підтримки прийняття рішень. До кожного етапу сформованого процесу наведено методи та моделі які використовуються в залежності від вхідної інформації. Відмінність від традиційної послідовності полягає в паралельному аналізі інформації, виборі і створенні альтернатив особою яка приймає рішення та системою підтримки прийняття рішення, перед тим як буде прийняте рішення. Ефективність реалізації, полягає в скороченні часу на прийняття рішення особою яка приймає рішення так як він може прийняти рішення використовуючи часткову інформацію на проміжних етапах, ще до вироблення альтернатив. Крім того особа яка приймає рішення може використовувати методи, які не реалізовані в системі підтримки прийняття рішення та основані на особистому досвіді та інтуїції. Наукова новизна отриманих результатів полягає в виявленні закономірностей використання методів та моделей в процесі прийняття рішення. Актуальність даного дослідження зумовлена визначенням перспективного напрямку досліджень з використанням методів та моделей які будуть враховувати зміни умов обстановки або ситуацію, яка склалась.

Ключові слова: метод, модель, моделювання, процес прийняття рішення.

Abstract. The article offers an analysis of decision-making methods and models depending on the stages of the decision-making process, the use of categories and methods of taking into account input information that describes the conditions in which the task is performed and the components of the task itself. The most difficult thing in this process is to make such a decision in the conditions of lack of time, information uncertainty and the presence of contradictions in the relevant field. Therefore, when forming management decisions, it is necessary to use a certain classification that corresponds to the area of decision-making and takes into account the specifics of management. The classification of management decisions is presented, taking into account the basics of decision-making theory, management and the nature of tasks that are solved through the interaction of a decision-maker and a decision-making support system. Methods and models are given for each stage of the formed process, which are used depending on the input information. The difference from the traditional sequence consists in the parallel analysis of information, the choice and created alternatives by the decision-maker and the decision-making support system, before a decision is made. The effectiveness of the implementation consists in reduced decision-making time by the person who makes the decision, as he can make a decision using partial information at intermediate stages, even before developing alternatives. In addition, the decision maker can use methods that are not implemented in the decision support system and are based on personal experience and intuition. The scientific novelty of the obtained results lies in the revealed regularities of the use of methods and models in the decision-making process. The relevance of this study is due to the determination of the prospective direction of research using methods and models that will take into account changes in the conditions of the situation or the situation that has developed.

Key words: method, model, modeling, decision-making process.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-74-78>.

Вступ

Кожна людина щодня приймає велику кількість рішень в різних сферах життєдіяльності. Кожне рішення передбачає реалізацію знань, вмінь та навичок особи яка приймає рішення (ОПР), які направлені на досягнення мети шляхом виконання завдання. Творчий пошук шляхів, напрямів та засобів виходу з ситуації яка викликала необхідність в прийнятті рішення формує певний досвід, який може використовуватись не тільки ОПР, яка досягла його за рахунок власних міркувань але й в інформаційних системах. Використання інформаційних систем (ІС) значно скорочує час, який необхідний для прийняття управлінських рішень, проте сучасні тенденції розвитку методів, моделей прийняття рішення та сучасних технологій розширюють можливості не тільки інформаційних систем а й ОПР. Вихідним фактором являється інформація і можливість її своєчасного збору та обробки в залежності від способів її подання і категорій. Великі обсяги інформації створюють зростання інформаційного навантаження, що сповільнює або унеможливує своєчасність її обробки.

Актуальність

Одним із основних завдань науковців є пошук шляхів автоматизованого забезпечення творчих процесів у діяльності органів управління. У напрямі досліджень питань управління та прийняття рішень ведуться інтенсивні дослідження. В роботах науковців в області інформаційних технологій сфери безпеки та оборони С. О. Кірсанов, С. М. Островський, М. Д. Рудніченко, І. В. Рубан, роботах зарубіжних вчених Л. Заде, Т. Сааті, Р. Р. Ягер, Д. Дубоїс, А. Кауфман, Е. Н. Мамдані, М. Мізумото, М. Сугено, С. Дж. Расселл проведено дослідження і отримані фундаментальні результати проте вони невичерпні та потребують узагальнення накопиченого досвіду тому подальші дослідження в цьому напрямку безсумнівно актуальні як в практичному так і в теоретичному аспектах.

Мета

Дослідження методів та моделей прийняття рішення використовуючи мультиваріативність даних для прийняття управлінського рішення на основі класичного процесу прийняття рішення.

Задачі

1. Класифікувати управлінські рішення
2. Сформулювати процес прийняття рішення.
3. Здійснити аналіз використання методів та моделей відносно етапів прийняття рішення.

Розв'язання задач

Управлінські рішення, як правило, приймаються в умовах високої невизначеності, при дефіциті інформації, тому суб'єкт управління не завжди може об'єктивно встановити критерії оцінки та пріоритети їхньої важливості. Через це, на практиці часто використовуються методи та моделі, які дають змогу приймати не оптимальні, а задовільні рішення. Вони вважаються прийнятними, оскільки вкладаються в рамки наявних обмежень і забезпечують поліпшення проблемної ситуації. Перевага зазвичай надається тому рішення, з яким суб'єкти управління вже знайомі й воно призвело до прийнятних результатів. Вибираючи остаточне рішення з ряду допустимих необхідно обов'язково враховувати як позитивні, так і негативні наслідки його реалізації, які відображаються на своїх можливостях.

Отримання та вибір необхідного результату вимагає від ОПР усвідомлення завдання, його декомпозицію на часткові завдання. Кожне з таких завдань передбачає врахування факторів за відома відомих або невизначених, які будуть впливати на нього на кожному з етапів його виконання [1] так як вони корелюють один з одним і неврахування одного з факторів приведе до похибки в дослідженнях або значного відхилення від реального результату. Такий рід діяльності потребує використання знань, вмінь та аналітичних навичок спеціалістів, які мають найвищу кваліфікацію в даній області або навіть є експертами.

Використовуючи знання експертів, консультантів в поєднанні з технологіями збору та обробки інформації, системами зв'язку, технологіями створення інтелектуального програмного забезпечення та взаємозв'язку людини з комп'ютером реалізовано: експертні системи; інформаційні системи підтримки прийняття рішення; перспективні автоматизовані системи підтримки та прийняття рішення (АСППР); інтелектуальні системи підтримки та прийняття рішення (ІСППР). Правильно використовуючи зібрані знання в наведених системах можливо отримати управлінське рішення ОПР яке і буде відповіддю на існуючий виклик. Найбільш складніше в цьому процесі – це прийняти таке рішення в умовах дефіциту часу, інформаційної невизначеності та наявності протиріч у відповідній сфері. Тому формуючи управлінські рішення необхідно користуватись певною класифікацією, яка б відповідала сфері прийняття рішення і враховувала специфіку управління. Приведемо варіант класифікації управлінських рішень враховуючи основи теорії прийняття рішень, менеджменту, управління [2-4] та характер задач, які виконуються в сфері управління (рис.1).

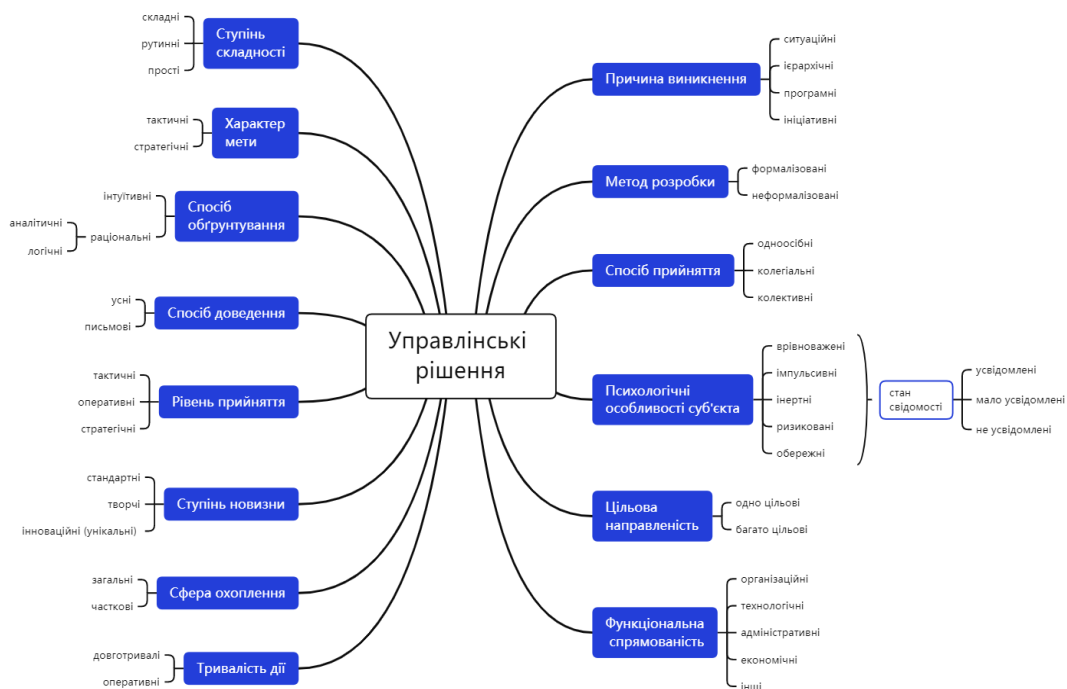


Рисунок 1 – Варіант класифікації управлінських рішень

Розробка та реалізація управлінського рішення являє собою сукупність дій, які складаються з окремих етапів, процедур і операцій [5]. Вибір методу та моделі розв'язання проблеми впливає на перелік етапів, які наведені у так званій традиційній (класичній) схемі (рис. 2), яка включає такі етапи: формулювання задачі; вибір критеріїв оцінки ефективності рішення; збір, обробка інформації та виявлення обмежень; розробка альтернативних (можливих) варіантів рішення; складання математичних та імітаційних моделей; зіставлення варіантів за критеріями ефективності та вибір альтернатив; прийняття рішення.

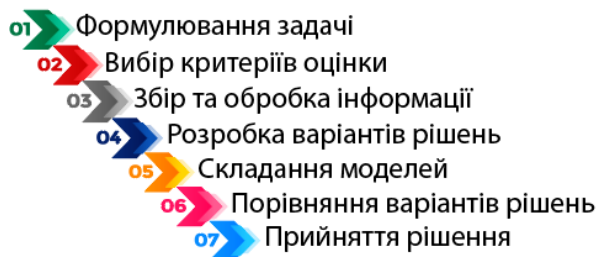


Рисунок 2 – Варіант етапів процесу прийняття рішення

Враховуючи те, що розв'язання задачі здійснюється спільно ОПР та СППР для опису процесу будемо використовувати варіант процесу прийняття рішення який наведений в [6]. Його відмінність від традиційної схеми полягає в паралельному аналізі інформації, виборі і створенні альтернатив ОПР та СППР, перед тим як ОПР прийме рішення. Ефективність реалізації, полягає в скороченні часу на прийняття рішення ОПР так як він може прийняти рішення використовуючи часткову інформацію на проміжних етапах, ще до вироблення альтернатив. Крім того ОПР може використовувати методи, які не реалізовані в СППР та основані на особистому досвіді та інтуїції.

При формулюванні задачі необхідно визначити: причини виникнення задачі; керовані та некеровані фактори, на які з них можливо впливати; цілі які необхідно досягнути; обмеження; терміновість вирішення.

Категорії інформації, які описують умови в яких виконується завдання та складові самого завдання під час прийняття рішення визначені наступним чином [3]: невідома, відома, змінна, незмінна, стохастична, суб'єктивна та об'єктивна. Способи подання інформації обмежимо використанням графічного, чисельного та лінгвістичного представлення, так як вони є необхідними та достатніми для відображення математичних моделей.

На першому етапі використовуються методи аналізу, синтезу, порівняння, аналогії, індукції, дедукції, узагальнення та абстрагування. Можуть використовуватись інструменти системного аналізу:

- метод сценаріїв (який являється засобом отримання та збору інформації про взаємозв'язки задачі з іншими задачами);
- діагностичний метод;
- графічний метод дерев цілей.

Другий етап. Критерії оцінки ефективності рішення повинні мати кількісне відображення для зіставлення варіантів рішення і вибору найкращого. Вони можуть бути як максимальними або мінімальними значеннями показників так і визначеними границями. Можливо використовувати один критерій і кілька показників або кілька критеріїв, в залежності від чого збільшиться кількість показників і буде чіткіше видно переваги і недоліки прийнятого рішення. В разі великої кількості показників їх потрібно групувати або обмежуватись вибором найбільш суттєвих. Використання різних критеріїв залежить від характеру визначеності ситуації (середовище, ОПР, цілі) [7]. У випадку коли інформація (щодо умов, характеристик) відома можливо використати методи оцінки ймовірності, в умовах невизначеності використовуються критерії Лапласа, Гурвіца, Севіджа, Вальда. Коли існує протистояння інтересів використовуються методи теорії ігор.

Третій етап. Збір та обробка інформації, яка враховується для розгляду поставленої задачі залежить від складності самої задачі, досвіду ОПР та способу подання в СППР. Крім того вона повинна бути своєчасною, достовірною та повною. Тому потрібно враховувати всі доступні категорії інформації та види. Види розділимо на первинну, тобто вся інформація, яка поступає та вторинну, а саме: систематизовані відомості та аналітичні матеріали. Проте, для їх врахування, необхідна повна об'єктивна характеристика ситуації, яка склалася та тенденції її зміни. В залежності від рівня прийняття її об'єми можуть збільшуватись, тим самим, потребувати більше часу на її обробку. Виділимо кілька методів збору та обробки інформації, відповідно до воєнної сфери. Частіше всього використовуються методи аналізу документів, факторний аналіз, порівняльний аналіз, класифікація, спостереження, прогнозування, опитування, експерименту та експертні оцінки. В свою чергу експертні оцінки включають такі методи: метод "Дельфі"; метод колективної генерації ідей, метод співвіднесеної оцінки.

Четвертий етап. Формулювання варіантів рішень буде залежати від попередніх етапів, в яких проведено усвідомлення сформованої задачі, вибрано критерії оцінки ефективності та отримано вторинну інформацію. Може враховуватись досвід рішення аналогічних завдань, однак не слід цим обмежуватись і звужувати кількість альтернатив варіантів по аналогії. При формулюванні варіантів рішень використовуються методи: прогнозування; методи експертних оцінок; діагностичні методи; графічні методи (метод дерев цілей, матричний метод та метод мережі); кількісні методи (метод економічного аналізу, морфологічні методи, статистичні методи); методи моделювання (аналітичний, графічний, чисельний).

П'ятий етап полягає в складанні математичних та імітаційних моделей [8, 9] що максимально відображають ситуацію яка склалася, умови виконання завдання, процес його протікання функції учасників процесу та саме завдання по якому потрібно прийняти рішення. При незмінності параметрів (об'єкта, умов) використовується технологія імітаційного моделювання, якщо ж ситуація змінна то використовується ситуаційне моделювання. Залежно від характеру досліджуваного процесу види моделювання можуть бути розділені на детерміновані, стохастичні, статичні, динамічні, дискретні та безперервні. На них побудовані методи: моделювання дискретних подій, системної динаміки; агентне моделювання; моделювання динамічних систем; комбіноване моделювання з використанням вище всіх перелічених методів. З використанням даних методів моделювання створюються інформаційна, кібернетична, функціональна, оптимізаційна, імітаційна, ігрова, ситуаційна та процесна моделі.

Шостий етап. Вибір альтернатив здійснюється із застосуванням методів, які дозволяють порівняти або зіставити варіанти рішень з визначеними групами факторів які впливають на процес, що моделюється, а також можуть поєднувати в собі визначені способи та категорії вхідної інформації. Тобто може відбуватися вплив випадкових факторів, які не відомі або невраховані.

Сьомий етап. На час прийняття рішення ОПР вже повинен врахувати всі рекомендації помічників (спеціалістів, експертів), вплив якісних факторів які не охоплені математичною та імітаційною моделями, що дасть змогу прийняти правильне рішення.

Висновки

За результатами проведених досліджень запропоновано варіант класифікації управлінських рішень. В основу якого покладені класичні методи та моделі, що дозволяє на підготовчому етапі обрати найбільш ефективний апарат рішення задачі по якій приймається рішення. Доведено що запропонований варіант класифікації управлінських рішень може використовуватися при паралельному формуванні варіантів рішень ОПР та СППР, що дає змогу скоротити сукупність методів та моделей, які використовуються в СППР та при прийнятті рішень ОПР.

Список літератури

- [1] І. С. Творошенко, *Технології прийняття рішень в інформаційних системах: навч. посіб.* Харків, Україна: ХНУРЕ, 2021.
 - [2] В. Т. Шатун, *Основи менеджменту: навч. посіб.* Миколаїв, Україна: МДГУ ім. Петра Могили, 2006.
 - [3] В. І. Ткаченко, Є. Б. Смірнов, *Теорія прийняття рішень органами військового управління: монографія.* Харків, Україна: ХУПС, 2008.
 - [4] І. Б. Гевко, *Методи прийняття управлінських рішень: підручник.* Київ, Україна: Кондор, 2009.
 - [5] Ю. С. Петруня, Б. В. Літовченко, Т. О. Пасічник, *Прийняття управлінських рішень: навчальний посібник.* Дніпро, Україна: Університет митної справи та фінансів, 2020.
 - [6] Д. О. Каліновський, "Аналіз факторів процесу прийняття рішення в ході управління змішаною групою сил та засобів Повітряних Сил": "Повітряна міць держави", №1, с. 85-86. 2021. [Електронний ресурс]. Режим доступу: <http://sap.nuou.org.ua/issue/view/14556>. Дата звернення: Трав. 25, 2022
 - [7] Л. С. Файнзільберг, О. А. Жуковська, В. С. Якимчу, *Теорія прийняття рішення: підручник для студентів спеціальності "Комп'ютерні науки та інформаційні технології", спеціалізації "Інформаційні технології в біології та медицині".* Київ, Україна: Освіта України, 2018.
 - [8] П. М. Павленко, *Математичне моделювання систем і процесів: навч. посіб.* Київ, Україна: НАУ, 2017.
 - [9] В. Б. Неруш, В. В. Курдеча, *Імітаційне моделювання систем та процесів: Електронне навчальне видання.* Київ, Україна: НН ІТС НТУУ "КПІ", 2012.
- Стаття надійшла: 20.05.2022

References

- [1] I. S. Tvoroshenko, *Technologies of decision making in information systems.* Kharkov, Ukraine: KhNURE, 2021 [in Ukrainian].
- [2] V. T. Shatun, *Fundamentals of Management: Textbook.* Mykolaiv, Ukraine: Publishing House of Mykolaiv State Humanitarian University named after Peter Mogila, 2006 [in Ukrainian].

- [3] V. I. Tkachenko, *Theory of decision-making by military authorities: monograph*. – Kharkov, Ukraine: KhNUAF, 2008 [in Ukrainian].
- [4] I. B. Gevko, *Methods of management decisions: Textbook*. Kyiv, Ukraine: Condor, 2009 [in Ukrainian].
- [5] Y. E. Petrunya, B. V. Litovchenko, T. O. Pasichnyk, *Adoption of management decisions: textbook*. 4th ed., Reworked. and ext. Dnipro, Ukraine: University of Customs and Finance, 2020 [in Ukrainian].
- [6] D. O. Kalinovskiy, "Analysis of factors of the decision-making process during the management of a mixed group of forces and assets of the Air Force": "Air Power of the State", № 1, p. 85-86. 2021. [Electronic resource]. Access mode: <http://sap.nuou.org.ua/issue/view/14556>. Application date: May. 25, 2022 [in Ukrainian].
- [7] L. S. Feinziilberg, O. A. Zhukovskaya, V. S. Yakymchku, *Theory of decision making: a textbook for students majoring in "Computer Science and Information Technology", specialization "Information Technology in Biology and Medicine"*. Kyiv, Ukraine: Education of Ukraine, 2018 [in Ukrainian].
- [8] P. M. Pavlenko, *Mathematical modeling of systems and processes: textbook*. Kyiv, Ukraine: NAU, 2017 [in Ukrainian].
- [9] V. B. Nerush, V. V. Kurdecha, *Simulation of systems and processes: Electronic educational publication*. Kyiv, Ukraine: NN ITS NTUU "KPI", 2012 [in Ukrainian].

Відомості про авторів

Каліновський Дмитро Олександрович – ад'юнкт Харківського національного університету Повітряних Сил імені Івана Кожедуба.

Осієвський Сергій Валерійович – кандидат технічних наук, доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба.

D. Kalinovskiy, V. Osievskiy

ANALYSIS OF DECISION-MAKING METHODS AND MODELS USING CATEGORIES AND METHODS OF TAKING INPUT INTO INFORMATION

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv

УДК 004.272.25

Т. Б. Мартинюк, Б. І. Круківський, С. В. Богомолів, А. О. Кузіна

СИНТЕЗ ПРИСТРОЮ КЕРУВАННЯ НА БАЗІ R-AВТОМАТА ДЛЯ АСОЦІАТИВНОГО ПРОЦЕСОРА

Вінницький національний технічний університет, Вінниця

Анотація. В даній статті розглядається один з відомих варіантів синтезу пристроїв керування з "жорсткою" логікою. Такі пристрої керування забезпечують значну швидкість спрацювання у порівнянні з пристроями керування з програмованою логікою, але мають трудомісткий процес на етапах абстрактного та структурного синтезу мікропрограмованого автомата (МПА) як базової моделі структури пристрою такого типу керування. Синтез МПА на базі зсувного регістра як R-автомата забезпечує компромісне рішення серед реалізацій МПА на базі паралельного регістра як T-автомата або лічильника як СТ-автомата. Це пов'язано з навантаженням пам'ятовувальної частини МПА за рахунок зниження складності логічної частини МПА, а саме його комбінаційної схеми. Використання специфічного одиничного позиційного кодування станів МПА дозволяє значно спростити складний процес формування булевих функцій, що відповідають функціям збудження при структурному синтезі МПА. А це, у свою чергу, приводить до спрощення комбінаційної частини МПА. Разом з тим, ускладнення пам'ятовувальної частини МПА на базі зсувного регістра приводить до збільшення його розрядності, не зменшуючи регулярності його структури. У статті запропоновано не стандартний підхід до синтезу пристрою керування та розроблено його функціональну схему. В результаті синтез на базі R-автомата структури пристрою керування для асоціативного процесора підтвердив перспективність такого варіанта синтезу МПА через спрощення процесу відповідного абстрактного та структурного синтезу. Це обумовлено нескладністю формування прямої та спрощеної структурних таблиць з використанням одиничного позиційного кодування станів МПА. Планується розміщення розробленої структури пристрою керування у програмованій логічній ІС (ПЛІС), що дозволить розмістити у ПЛІС весь асоціативний процесор. Такий підхід забезпечить компактність організації та швидкодію спрацювання асоціативного процесора.

Ключові слова: пристрій керування, мікропрограмований автомат, R-автомат, асоціативний процесор, сортування.

Abstract. This article discusses one of the well-known options for the synthesis of control devices with rigid logic. Such control devices provide a significant response speed compared to control devices with programmable logic, but they have a laborious process at the stages of abstract and structural synthesis of a microprogram automaton (MPA) as the basic structural model of this type of control device. Synthesis of an MPA based on a shift register as an R-automaton provides a compromise solution among the implementations of an MPA based on a parallel register as a T-automaton or a counter as a CT-automaton. This is due to the load on the memory of the MPA by reducing the complexity of the logical part of the MPA, namely its combinational scheme. The use of a specific single positional coding of the MPA states makes it possible to significantly simplify the complex process of the formation of Boolean functions corresponding to the excitation functions in the abstract synthesis of the MPA. And this, in turn, leads to a simplification of the combinational part of the MPA. At the same time, the complication of the memory part of the MPA based on the shift register leads to an increase in its bit rate without reducing the regularity of its structure. The article proposes a non-standard approach to the synthesis of a control device and develops its functional scheme. As a result, synthesis on the basis of the R-automaton of the control device structure for the associative processor confirmed the perspective of this version of MPA synthesis by simplifying the process of the corresponding abstract and structural synthesis. This is due to the simplicity of forming direct and simplified structural tables using single positional coding of MPA states. It is planned to place the developed structure of the control device in a programmable logic IC (FPGA), which will allow the placement of the entire associative processor in the FPGA. This approach will ensure the compactness of the organization and the speed of the associative processor.

Key words: control device, microprogram automaton, R-automaton, associative processor, sorting.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-79-85>.

Вступ

Якщо розглядати пристрої керування з "жорсткою" логікою, то базовими варіантами їх синтезу можна назвати три з них, які відрізняються побудовою пам'ятовувальної частини мікропрограмованого автомата (МПА). Це пов'язано з реалізацією цієї частини МПА або на тригерах (паралельному регістрі) як T-автомат (ТА), або на лічильниках як СТ-автомат (СТА), або на зсувному регістрі як R-автомат (РА) [1].

Разом з тим, вдосконалення методів синтезу пристроїв керування продовжується [2], що знаходить своє втілення, наприклад при побудові МПА з операційним автоматом переходів або операційною адресацією [3-5].

Актуальність

Серед наведених трьох базових варіантів синтезу МПА тільки використання R-автомата забезпечує вираш в апаратних витратах при побудові комбінаційної частини МПА [6]. Це пов'язано з тим, що в цьому випадку апаратне навантаження припадає на пам'ятовувальну частину МПА, якою є зсувний регістр, що має регулярну структуру і можливість нарощування його розрядності без зайвих ускладнень [7,8].

Таким чином реалізується принцип, за яким зростання апаратної складності пам'ятовувальної частини МПА зменшує апаратну складність його комбінаційної частини, зокрема за рахунок функціонального навантаження елементів пам'яті МПА [1,8]. Крім того, необхідно врахувати, що збільшення регулярної організації будь-якої структури дозволяє ефективно її розмістити у перспективних програмованих логічних ІС (ПЛІС) [9-11].

Мета

Метою роботи є аналіз можливостей побудови пристрою керування з використанням синтезу МПА на базі R-автомата для конкретного пристрою, а саме для асоціативного процесора, що реалізує алгоритм сортування з ранжуванням елементів числового масиву.

Етапи абстрактного та структурного синтезу МПА

Для побудови пристрою керування обрано як приклад спосіб функціонування асоціативного процесора на реверсивних лічильниках з достатньо високою регулярністю структури [12]. Абстрактний синтез МПА починається з розмітки граф-схеми алгоритму (ГСА) сортування з ранжуванням (рис. 1) для обраного асоціативного процесора [12].

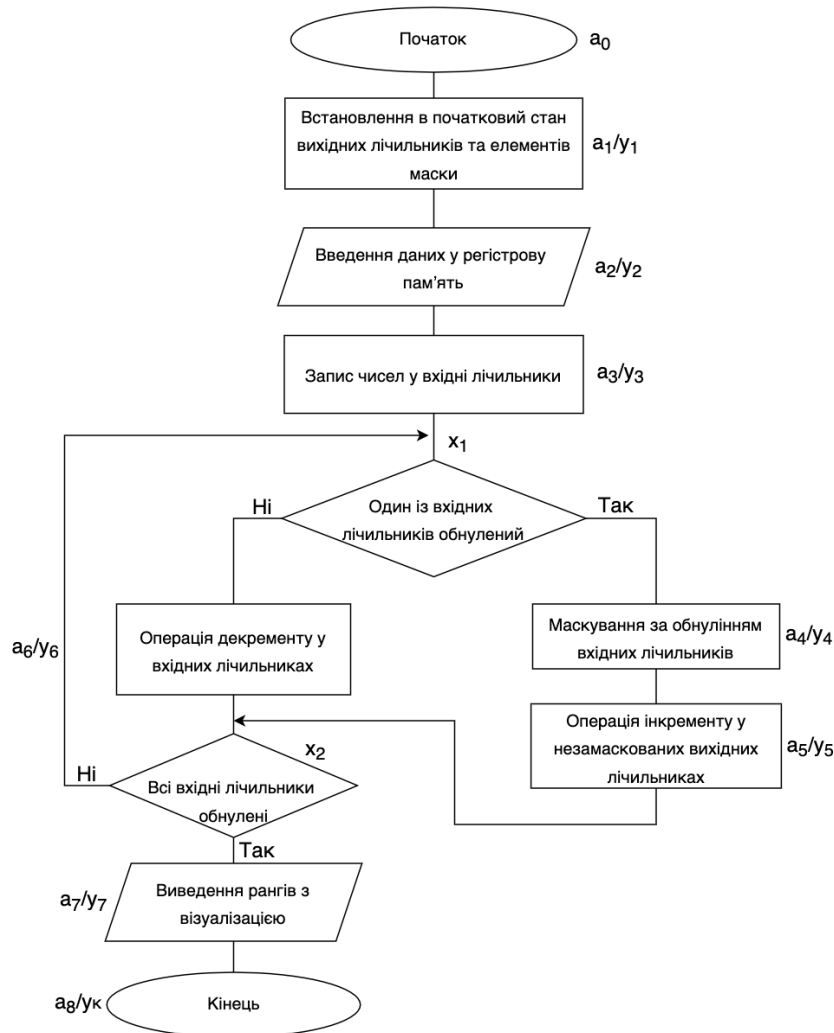


Рисунок 1 – Блок-схема алгоритму сортування з ранжуванням

Для МПА на базі RA доцільно застосувати автомат Мура (рис. 2), оскільки в цьому випадку сигнали керування співвідносяться з операторними вершинами ГСА (рис. 1). Аналіз наведеного ГСА сортування з ранжуванням на рис. 1 показав наявність лінійного ланцюга λ з вершинами, поміченими станами $a_0 - a_3$, та достатньо розгалуженої за умовними вершинами x_1, x_2 частини, що не входить до лінійного ланцюга λ , а саме вершини зі станами $a_3 - a_7$ (рис. 2).

Кількість розмічених операторних вершин ГСА визначає розрядність N зсувного регістра RG у запам'ятовувальній частині МПА [8], тобто $N=8$. Це пов'язано з тим, що для кодування станів МПА використовується специфічний одиничний позиційний код [13,14]. В результаті кожний зі станів $a_3 - a_8$ кодується одиницею у відповідному розряді $Q_1 - Q_8$ зсувного регістра RG, тобто стани подаються таким чином:

$$\begin{array}{l}
 100\dots 00 \\
 010\dots 00 \\
 \dots \\
 000\dots 10 \\
 000\dots 01.
 \end{array} \quad (1)$$

Отже, перехід між сусідніми станами в межах лінійного ланцюга λ реалізується в процесі послідовного зсуву одиниці від молодшого розряду до сусіднього старшого розряду.

Пряму структурну таблицю (ПСТ) подано у вигляді табл. 1, де показано всі можливі тринадцять переходів між станами МПА згідно з автоматом Мура (рис. 2).

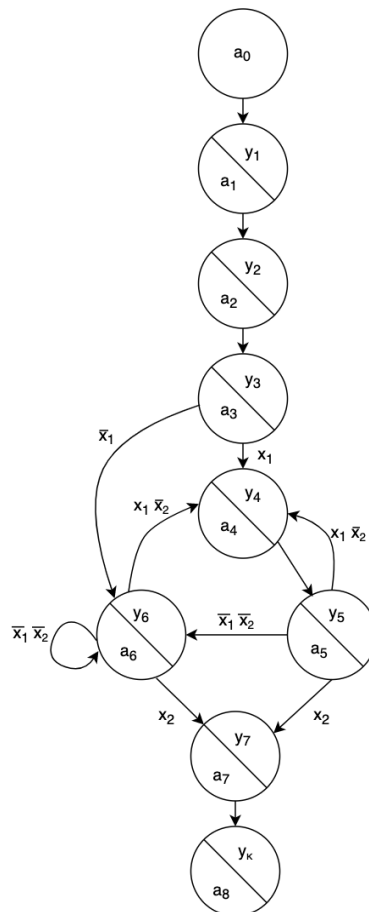


Рисунок 2 – Автомат Мура

В окрему спрощену таблицю (табл. 2) винесено всі нелінійні переходи (розгалуження), які не входять до лінійного ланцюга λ (табл. 1). Тільки ці нелінійні переходи в подальшому подаються у вигляді булевих рівнянь. У даному випадку вони складають вісім переходів з тринадцяти.

На рис. 3 наведено функціональну схему МПА, яка фактично представляє структуру пристрою керування для асоціативного процесора [12]. Оскільки зсувний регістр RG (рис. 3) є функціонально значущим вузлом МПА, то доцільно визначити особливості його спрацювання. Він має керовані входи: R – скиду, C – синхронізації та S0, S1 – вибору режиму і спрацьовує за такими сигналами: Reset – сигнал скиду, Set – настановний одиничний сигнал, Clock – тактові імпульси.

Особливістю зсувного регістра RG як запам'ятовувальної частини МПА (рис.3) є те, що він спрацьовує у двох режимах:

- послідовного зсуву у бік старших розрядів для виконання послідовних переходів між станами лінійного ланцюга λ ;
- паралельного завантаження по його входах $D_1 - D_8$ для виконання нелінійних переходів у точках розгалуження ГСА (рис. 1), що відповідає примусовому встановленню нового стану та обнуленню поточного стану зсувного регістра RG.

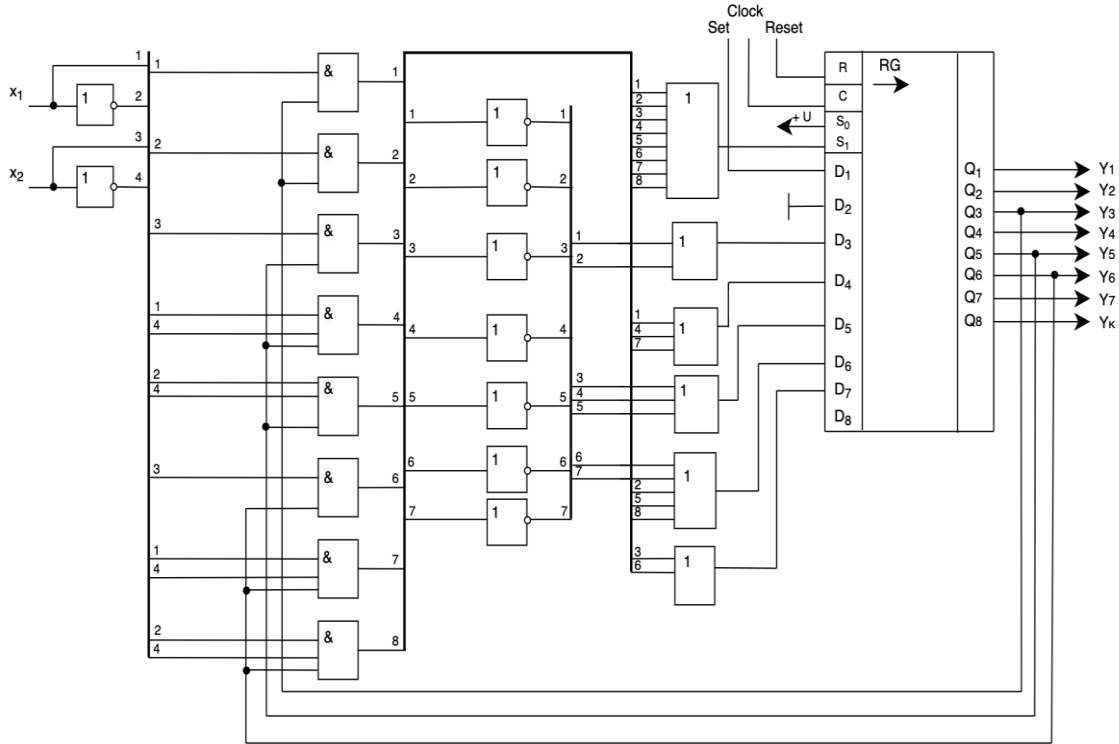


Рисунок 3 – Функціональна схема МПА

Таблиця 1 – Структурна таблиця переходів між станами МПА

Початковий стан a_m	Код початкового стану $K(a_m)$	Стан переходу a_s	Код стану переходу $K(a_s)$	Вхідний сигнал $X(a_m, a_s)$	Вихідний сигнал $Y(a_m, a_s)$	Функція збудження $\Phi(a_m, a_s)$	Ознака належності $(a_m, a_s) \in \lambda$	Номер переходу h
a_0	00000000	a_1	10000000	1	y_1	D_1	+	1
a_1	10000000	a_2	01000000	1	y_2	D_2	+	2
a_2	01000000	a_3	00100000	1	y_3	D_3	+	3
a_3	00100000	a_4	00010000	x_1	y_4	$\bar{D}_3 D_4$	-	4
		a_6	00000100	\bar{x}_1	y_6	$\bar{D}_3 D_6$	-	5
a_4	00010000	a_5	00001000	1	y_5	D_5	+	6
a_5	00001000	a_4	00010000	$x_1 \bar{x}_2$	y_4	$\bar{D}_5 D_4$	-	7
		a_6	00000100	$\bar{x}_1 \bar{x}_2$	y_6	$\bar{D}_5 D_6$	-	8
		a_7	00000010	x_2	y_7	$\bar{D}_5 D_7$	-	9
a_6	00000100	a_4	00010000	$x_1 \bar{x}_2$	y_4	$\bar{D}_6 D_4$	-	10
		a_6	00000100	$\bar{x}_1 \bar{x}_2$	y_6	D_6	-	11
		a_7	00000010	x_2	y_7	$\bar{D}_6 D_7$	-	12
a_7	00000010	a_8	00000001	1	y_k	D_8	+	13

Таблиця 2 – Спрощена структурна таблиця переходів між станами МПА

Початковий стан a_m	Код початкового стану $K(a_m)$	Стан переходу a_s	Код стану переходу $K(a_s)$	Вхідний сигнал $X(a_m, a_s)$	Вихідний сигнал $Y(a_m, a_s)$	Функція збудження $\Phi(a_m, a_s)$	Номер переходу
a_3	00100000	a_4	00010000	x_1	y_4	$\bar{D}_3 D_4$	4
		a_6	00000100	\bar{x}_1	y_6	$\bar{D}_3 D_6$	5
a_5	00001000	a_4	00010000	$x_1 \bar{x}_2$	y_4	$\bar{D}_5 D_4$	7
		a_6	00000100	$\bar{x}_1 \bar{x}_2$	y_6	$\bar{D}_5 D_6$	8
		a_7	00000010	x_2	y_7	$\bar{D}_5 D_7$	9
a_6	00000100	a_4	00010000	$x_1 \bar{x}_2$	y_4	$\bar{D}_6 D_4$	10
		a_6	00000100	$\bar{x}_1 \bar{x}_2$	y_6	D_6	11
		a_7	00000010	x_2	y_7	$\bar{D}_6 D_7$	12

Для встановлення режиму зсуву на входи S_0, S_1 вибору режиму необхідно подати рівні сигналів високий, низький відповідно, а для режиму завантаження – обидва високі сигнали [15]. За даними табл. 2 видно, що булеві рівняння для формування відповідних функцій обнулення входів $\bar{D}_3, \bar{D}_5, \bar{D}_6$ та збудження входів D_4, D_6, D_7 зсувного регістра RG з урахуванням вхідних сигналів x_1, x_2 не представляють складності.

Отже, комбінаційна схема МПА (рис. 3) містить 9 інверторів, 8 елементів І та 6 елементів АБО, які утворюють 4 рівні логічних елементів, включаючи рівень з двох вхідних інверторів. В результаті максимальна затримка проходження сигналів функцій збудження складає 3τ , де τ – максимальний час затримки на логічних елементах відповідних рівнів. При розміщенні схеми МПА (рис. 3) в одній мікросхемі ПЛІС архітектури FPGA можна отримати швидкість її спрацювання в мілісекундному діапазоні [9,10,16,17].

Таким чином, використаний варіант синтезу МПА на базі RA, а також застосування одиничного позиційного кодування станів МПА на зсувному регістрі дозволяє реалізувати відомий принцип оптимального синтезу МПА, а саме забезпечення зменшення частки складного логічного перетворювача (комбінаційної схеми) за рахунок збільшення частки, а також функціонального навантаження регулярної за структурою запам'ятовувальної частини МПА [18].

Висновки

Результат синтезу на базі R – автомата структури пристрою керування для асоціативного процесора підтвердив перспективність такого варіанта синтезу МПА через спрощення процесу відповідного абстрактного та структурного синтезу. Це обумовлено нескладністю формування прямої та спрощеної структурних таблиць з використанням одиничного позиційного кодування станів МПА, що, в свою чергу, зумовлює зниження апаратної складності комбінаційної схеми МПА.

Разом з тим, зростання апаратної складності запам'ятовувальної частини МПА, що реалізована на зсувному регістрі, компенсується регулярністю її структури з можливістю нарощування необхідної розрядності. А це, у свою чергу, дає можливість реалізувати таку структуру пристрою керування разом з операційною частиною асоціативного процесора на одній мікросхемі ПЛІС з прийнятною швидкістю спрацювання.

Список літератури

- [1] Ю. А. Бузунов, И. Г. Буренков и Н. Н. Шипилов, "Микропрограммные автоматы на параллельно-последовательных машинах", *Управляющие системы и машины*, № 2, с. 26-29. 1982.
- [2] В. І. Жабін, І. А. Жуков, І. А. Кліменко та В. В. Ткаченко, *Прикладна теорія цифрових автоматів*. К.: Книжкове видання НАУ, 2007.
- [3] А. А. Баркалов и Р. М. Бабаков, "Операционное формирование кодов состояний в микропрограммных автоматах", *Кибернетика и системный анализ*, № 2, с. 21-26. 2011.
- [4] Р. М. Бабаков, "Алгебраический синтез микропрограммного автомата с операционным автоматом переходов", *Інформаційні технології та комп'ютерна інженерія*, № 2, с. 35-41. 2017.

- [5] А. А. Баркалов и Р. М. Бабаков, "Организация устройств управления с операционной адресацией", *Управляющие системы и машины*, № 6, с. 34-39. 2008.
- [6] В. П. Кожем'яко, Т. Б. Мартинюк, Н. В. Фофанова та В. В. Дмитрук, "Порівняльний аналіз варіантів синтезу мікропрограмних автоматів", *Оптико-електронні інформаційно-енергетичні технології*, № 1(9), с. 225-233. 2005.
- [7] В. П. Кожем'яко, Т. Б. Мартинюк и К. В. Кожем'яко, "Синтез устройства управления на R-автомате", *Управляющие системы и машины*, № 1/2, с. 22-25. 1995.
- [8] Т. Б. Мартинюк, "Особенности синтеза микропрограммных R-автоматов", *Управляющие системы и машины*, № 3, с. 22-26. 1998.
- [9] А. В. Палагин и В. Н. Опанасенко, *Реконфигурируемые вычислительные системы*. К. Україна: Просвіта, 2006.
- [10] В. Соловьев и А. Климович, "Использование входных буферов ПЛИС в качестве элементов памяти конечных автоматов", *Chip News*, № 2(22), с. 24-28. 2003.
- [11] А. А. Баркалов и А. А. Баркалов, "Оптимизация логической схемы автомата Мура на программируемых БИС", *Управляющие системы и машины*, № 6, с. 38-41. 2001.
- [12] Т. Б. Мартинюк, Л. В. Крупельницький та Б. І. Круківський, "Регулярна обчислювальна структура для ранжування даних", *Інформаційні технології та комп'ютерна інженерія*, № 3(52), с. 70-76. 2021.
- [13] В. П. Кожем'яко, Т. Б. Мартинюк, В. В. Дмитрук та В. В. Власійчук, "Класифікація одиничних кодів", *Оптико-електронні інформаційно-енергетичні технології*, № 1(11), с. 36-42. 2006.
- [14] Т. Б. Мартинюк та О. В. Войцеховська, "Ефективність одиничного кодування даних", *Інформаційні технології та комп'ютерна інженерія*, № 2, с. 30-36. 2021.
- [15] В. И. Зубчук, В. П. Сигорский и А. Н. Шкуро, *Справочник по цифровой схемотехнике*. К.: Техника, 1990.
- [16] А. М. Сергиенко, *VHDL для проектирования вычислительных устройств*. К.: ТИД «ДС», 2003.
- [17] В. Стещенко, "Школа разработки аппаратуры цифровой обработки сигналов на ПЛИС", *Chip News*, № 8. с. 2-6. 1999.
- [18] С. М. Ачасова, *Алгоритмы синтеза автоматов на программируемых матрицах*. М.: Радио и связь, 136 с, 1987.

Стаття надійшла: 10.05.2022.

References

- [1] Ju. A. Buzunov, I. G. Burenkov i N. N. Shipilov, "Mikroprogrammnye avtomaty na parallel'no-posledovatel'nykh mashinakh", *Upravljajushhie sistemy i mashiny*, № 2, s. 26-29. 1982 [in Russian].
- [2] V. I. Zhabin, I. A. Zhukov, I. A. Klimenko та V. V. Tkachenko, *Prykladna teoriia tsysfrovyykh avtomativ*. K.: Knyzhkove vydannia NAU, 2007 [in Ukrainian].
- [3] A. A. Barkalov i R. M. Babakov, "Operacionnoe formirovanie kodov sostojanij v mikroprogrammnykh avtomatah", *Kibernetika i sistemnyj analiz*, № 2, s. 21-26. 2011 [in Russian].
- [4] R. M. Babakov, "Alhebraycheskyi syntez mykroprohrammnoho avtomata s operatsyonnym avtomatom perekhodov", *Informatsiini tekhnolohii ta komp'uterna inzheneriia*, № 2, s. 35-41. 2017 [in Russian].
- [5] A. A. Barkalov i R. M. Babakov, "Organizacija ustrojstv upravlenija s operacionnoj adresaciej", *Upravljajushhie sistemy i mashiny*, № 6, s. 34-39. 2008 [in Russian].
- [6] V. P. Kozhemiako, T. B. Martyniuk, N. V. Fofanova та V. V. Dmytruk, "Porivnialnyi analiz variantiv syntezu mikroprohramnykh avtomativ", *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, № 1(9), s. 225-233. 2005 [in Ukrainian].
- [7] V. P. Kozhemiako, T. B. Martyniuk i K. V. Kozhemiako, "Sintez ustrojstva upravlenija na R-avtomate", *Upravljajushhie sistemy i mashiny*, № 1/2, s. 22-25. 1995 [in Russian].
- [8] T. B. Martyniuk, "Osobennosti sinteza mikroprogrammnykh R-avtomatov", *Upravljajushhie sistemy i mashiny*, № 3, s. 22-26. 1998 [in Russian].
- [9] A. V. Palagin i V. N. Opanasenko, *Rekonfiguriruemye vychislitel'nye sistemy*. K.: Prosvita, 2006. [in Russian].
- [10] V. Solov'ev i A. Klimovich, "Ispol'zovanie vhodnykh buferov PLIS v kachestve jelementov pamjati konechnykh avtomatov", *Chip News*, № 2(22), s. 24-28. 2003 [in Russian].
- [11] A. A. Barkalov i A. A. Barkalov, "Optimizacija logicheskoy shemy avtomata Mura na programmiruemym BИS", *Upravljajushhie sistemy i mashiny*, № 6, s. 38-41. 2001 [in Russian].
- [12] T. B. Martyniuk, L. V. Krupelnytskyi та B. I. Kruktivskiy, "Rehuliarna obchysliuvalna struktura dlja ranzhuvannia danykh", *Informatsiini tekhnolohii ta kompiuterna inzheneriia*, № 3(52), s. 70-76. 2021 [in Ukrainian].

- [13] V. P. Kozhemiako, T. B. Martyniuk, V. V. Dmytruk ta V. V. Vlasiichuk, "Klasyfikatsiia odynychnykh kodiv", *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, № 1(11), s. 36-42. 2006 [in Ukrainian].
- [14] T. B. Martyniuk ta O. V. Voitsekhovska, "Efektyvnist odynychnoho koduvannia danykh", *Informatsini tekhnolohii ta komp'iuterna inzheneriia*, № 2, s. 30-36. 2021 [in Ukrainian].
- [15] V. I. Zubchuk, V. P. Sigorskij i A. N. Shkuro, *Spravochnik po cifrovoj shemotehnikе*. K.: Tehnika, 1990 [in Russian].
- [16] A. M. Sergienko, *VHDL dlja proektirovaniia vychislitel'nyh ustrojstv*. K.: TID «DS», 2003 [in Russian].
- [17] V. Steshenko, "Shkola razrobotki apparatury cifrovoj obrabotki signalov na PLIS", *Chip News*, № 8, s. 2-6. 1999 [in Russian].
- [18] S. M. Achasova, *Algoritmy sinteza avtomatov na programmiruemykh matricah*. M.: Radio i svjaz', 1987 [in Russian].

Відомості про авторів

Мартинюк Тетяна Борисівна – доктор технічних наук, професор, професор кафедри обчислювальної техніки.

Круківський Богдан Ігорович – аспірант факультету інформаційних технологій та комп'ютерної інженерії.

Богомолів Сергій Віталійович – кандидат технічних наук, доцент, доцент кафедри обчислювальної техніки.

Кузіна Аріна Олегівна – студентка факультету інформаційних електронних систем.

T. B. Martyniuk, B. I. Krukivskyi, S. V. Bohomolov, A. O. Kuzina
**SYNTHESIS OF A CONTROL DEVICE BASED ON
R-AUTOMATON FOR ASSOCIATIVE PROCESSOR**

Vinnitsia National Technical University, Vinnitsia

УДК 681.3:621.74:004.8

О. В. Tokova¹, V. S. Doroshenko², О. В. Yanchenko³

COMPUTER SYSTEMS OF THERMAL ANALYSIS FOR MONITORING OF FOUNDRY AND METALLURGICAL PROCESSES

¹International Research and Training Center for Information Technologies and Systems of the NAS and MES of Ukraine, Kyiv

²Physical-technological Institute of Metals and Alloys of the National Academy of Science of Ukraine, Kyiv

³Vinnitsia National Technical University, Vinnitsia

Анотація. Описано комп'ютерну систему моніторингу теплових процесів, що відбуваються на ливарних та металургійних заводах. Теплові процеси детально розглядаються як основні процеси, що відбуваються в процесі лиття. Розглянуто два способи контролю якості металу методом термічного аналізу лиття за втраченою піномоделлю. У статті описані характеристики термоаналіза та теплових процесів. Зображено методи контролю якості чавуну шляхом заливання проби рідким металом і виконання комп'ютерного термоаналізу. Перераховано методи термічного аналізу металу, а також методи оптимізації литих конструкцій на основі результатів комп'ютерного порівняння даних від термоаналізу різних частин чи стінок виливка, в яких визначено механічні чи експлуатаційні характеристики металу в цих частинах чи стінках виливка як даних для оптимізації литої конструкції за цими даними. Дано короткий огляд програмного забезпечення для моніторингу теплових процесів. Подано структурну схему обчислювальної техніки, призначеної для моделювання теплових процесів, опис проблем, які вона вирішує, а також її короткий опис. Розроблено програмне забезпечення для підтримки рішень ливарного цеху, яке дозволить автоматизувати окремі етапи процесу лиття, підвищити якість металевих виробів. Це можна розглядати як перші кроки до створення систем штучного інтелекту для управління ливарними та металургійними процесами з точки зору якості металу, оптимізації шихтування і технології його виплавки, оптимізації конструкції виливків на основі даних термічного аналізу, отриманих з багатьох точок виливків. Одночасно цифрові записи, нарощування бази даних від термоаналізу і комп'ютерний аналіз цієї бази, як елемент цифровізації ливарно-металургійної технології, дає можливість коригувати технологію по ходу виплавки он-лайн, що підвищує продуктивність виробництва і якість металопродукції.

Ключові слова: теплові процеси, комп'ютерна техніка, контроль якості, комп'ютерний моніторинг, чавунне лиття, оптимізація, економія металу.

Abstract. A computer system for monitoring thermal processes occurring in foundries and metallurgical plants is described. Thermal processes are considered in detail as the main processes occurring in the casting process. Two methods of metal quality control by the method of thermal analysis of casting on the lost foam model are considered. The article describes the characteristics of thermal analysis and thermal processes. Methods of quality control of cast iron by filling the sample with liquid metal and performing computer thermal analysis are presented. Methods of thermal analysis of metal, as well as methods of optimization of cast structures based on the results of computer comparison of data from thermal analysis of different parts or walls of the casting, which determines the mechanical or operational characteristics of metal in these parts or walls of the casting as data for optimizing cast structures data. A brief overview of software for monitoring thermal processes is given. The block diagram of the computer equipment intended for modeling of thermal processes, the description of problems which it solves, and also its short description is given. Software has been developed to support the decisions of the foundry, which will automate certain stages of the casting process, improve the quality of metal products. This can be seen as the first steps towards creating artificial intelligence systems to control foundry and metallurgical processes in terms of metal quality, optimization of charge and smelting technology, optimization of casting design based on thermal analysis data obtained from many casting points. Simultaneously, digital records, building a database of thermal analysis and computer analysis of this database, as an element of digitization of foundry and metallurgical technology, allows you to adjust the technology in the course of online smelting, which increases productivity and quality of metal products.

Key words: thermal processes, computer technology, quality control, computer monitoring, cast iron casting, optimization, metal saving.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-86-93>.

Introduction

Introduction of a computer system for remote monitoring of parameters of technological processes, means of processing and transfer of informative data characterizing quality of performance of technological processes of casting will allow to manage foundry and metallurgical production efficiently taking into account minimization of expenses and increase of quality of metal castings. One way to increase the efficiency of the processes that take place in the production of metal castings is to model these processes in order to delegate the solution of a number of necessary tasks for a founder to the computer. The development of a user-friendly computer technology would provide a founder with a convenient tool to support his decisions in the casting process.

The main methods of assessing the quality of the casting in the foundry are thermal and chemical analysis, testing to determine the speed and modes of cooling of the casting. Thermal analysis (TA) is the most well-known one among these methods. It has been used for a long time. At the same time it is the most developed method both theoretically and experimentally.

The pace and level of development of domestic foundry and metallurgical technologies with the use of computer technologies on the basis of a database of materials, metals and alloys in accordance with the State Standards DSTU, methods for improving TA using methods of adaptive filtering, an inductive approach and other latest developments in applied mathematics, would allow foundry workers to model and regulate thermal

and other processes in order to optimize the physical and mechanical properties of casting and increase of production productivity. These technologies remain without adequate competitiveness, given the presence of numerous considered foreign software products that are difficult to use in Ukraine, but contribute to the irrevocable trend of digitalization of foreign production.

Actuality

The leading role of thermal processes in the production of foundry and metallurgical products is highlighted. The development of high-tech foundry processes, taking into account the current trend of saving metals should be combined with solving the problem of quality control of castings at the current level of digitalization of the industry. One such control method is thermal analysis (TA), which is supported by software. Thermal analysis is used, in particular, Fassmet (www.fassmet.com, Italy) [1], Institute of Physics and Technology of Metals and Alloys (PTIMA). NAS of Ukraine [2-6] and other enterprises for quality control of metals in the foundry and metallurgical industry at the stages from smelting metal, bottling it into molds to crystallization of the casting. There is a growing need for digitization and improvement of powerful domestic thermal analysis software.

The purpose of research

The aim of the article is to study the methods of thermal analysis in the field of foundry and metallurgical production and to develop software to support solutions for modeling thermal processes. Ensure that TA technologies provide a reliable opportunity not only to determine the composition of chemical elements in the melt, but also to predict the properties of the metal in the casting at a stage when the metal is still in the furnace or in the ladle. Optimization and simplification of TA as a set of methods for determining temperatures during the time when the processes are accompanied by either the release of heat (eg, crystallization), or its absorption (melting, thermal dissociation, etc.).

Research objectives

1. TA systems of metals and alloys require a mathematical description of control and measurement processes, the creation of computer databases and software to analyze a significant number of temperature dependences on the composition or properties of controlled metal samples.
2. Make TA systems components of digitization of existing or new control methods using applied mathematics for existing foundry processes.
3. TA systems also require the development of certain programs for measuring and monitoring data over time.

Quality Control of Cast Iron by thermal analysis

These moulds are produced by a vacuum forming process referred to as Lost Foam Casting (LFC), but they are also applicable to traditional sand moulds, which account for over 75% of the world's castings.

Computer-recorded temperature measurement curves over time during crystallization of a measuring amount of metal are used in the TA method to determine alloying and impurity elements and gases in metals, including sampling. The samples are made with thermocouples placed in them. When the samples are cooled, the "temperature-time" curves are recorded for further analysis [2]. The practical implementation of the method includes pouring a molten metal into samplers, keeping them heated when the metal solidifies in them when the curves are recording, as well as utilizing samples and associated waste. These operations are connected with some labour intensity in the category of hot and unsafe working conditions, time and material costs, as well as compliance with the safety of working with a molten metal.

One of the latest developments is the TA method for liquid iron [4]. One of the distinctive features of the method is that the samples are taken using an immersion sample cup in order to carry out the analysis. The peculiarities of such specially made samplers, without which analysis is impossible, is that they are made of high-quality refractory materials that are resistant to immersion into the metal melt or its pouring with the metal melt without destroying the samplers and inert to interact with the sample.

Samplers are used by analogy with calorimeters and must be manufactured with high accuracy to ensure the same cooling conditions for a metal sample during TA and many reference samples, which affects the accuracy of TA. Manufacturing and preparation of samplers for filling with metal, filling them with molten metal, carrying out measurements require labour costs when working with molten metal. The safety measures to avoid unforeseen cases of leakage or splash of molten metal from the samplers as well as burns and injuries of a qualified caster when manually filling samplers should be provided. Even the illustration of the TA presented on the Fassmet website shows spilled metal around the samples (Fig. 1).

The used container-sampler for immersion in the cast iron melt during sampling is made of special alloys of high heat resistance [4]. In this case, the material of the casting mould, where the metal is poured after analysis, differs significantly from the material of such a sampler, as well as the conditions for cooling the samples from the conditions for the metal of the casting.



Figure 1 – Filling and cooling of samples at TA [1]

The vast majority of castings from metals and alloys are obtained in sand moulds, therefore, according to the State Standard GOST 24648-90, it is recommended to cast samples for mechanical tests of cast iron into moulds made of quartz sand, and only for castings obtained in metal moulds, it is allowed to cast samples into metal moulds. The task was to make a sand sampler as a mould for casting iron.

A New Way for a Thermal Analysis of Metal

Metal TA methods [2, 4] reveal the properties of the metal in the sample, the crystallization conditions of which are often not similar to the crystallization conditions of the casting metal in the sand mold. The validity of the State Standard GOST 24648-90 regulation is obvious, that samples, in particular for cast iron, should be cast in the same mould in which the casting is obtained.

In addition, the development of a new TA method was aimed at using improved software, reducing labor intensity, increasing the accuracy and speed of issuing results (express level) and safety, as well as creating conditions for conducting TA in the same form that is used to manufacture a casting as a product.

The novelty of the solution was that the sand mould played the role of the sampler [5]. The model of the sample was moulded into this sand mould using the LFC technology, in particular, of the gasified material Cellular Polystyrene (CP). This sand mould can be made separately (in a separate flask), or (the most advisable option) together (in one flask) with a sand mould for producing a casting, for which the metal was smelted and TA was carried out.

A sand mould-sampler made in a separate flask served the same task, which is achieved by the known methods of TA of metal for various purposes [2, 4]. And when forming a one-time sample model in the same flask with a sand mould for obtaining a casting, the sampler is not a separate object from this mould, because only a small part of the mould around the sample model performs its function. In this case, the thermocouple is placed not in the cavity of the sampler (as in [2, 4]), but in the body of a one-time model made of CP (with a density of up to 25 kg/m³). The use of a sand mixture without a binder, traditional for LFC, as one of the most resource-saving foundry process for the manufacture of samplers, excludes special labour costs and expensive materials (usually imported), which are typical for the manufacture of sand samplers by the well-known methods of TA of metals.

During the development of the technology, the model was made with a small feeder, which was glued to the model of the casting made of CP or to the model of its gating-feeding system in the case of making the casting using the LFC process. The casting model with the sample model was moulded in a container mould in dry recycled quartz sand according to known operations for LFC. The free ends of the thermocouple were connected to recording devices and they received TA data according to a calculation technique similar to known methods.

Computer Monitoring Systems for Foundry Processes

In modern conditions, a tendency towards mounting a device for TA as a part of modern computer systems for monitoring casting processes is developing. For example, the software at Fassmet [1] allows foundry workers to view TA results online on tablets, smartphones or PCs at the foundry's premises. The web interface can be configured to control the quality of a specific type of cast iron produced. It is linked to a large, constantly updated database. The TA method gives an advantage in the case of fulfilling diverse orders, or the need to obtain a completely new type of cast iron [1]. The developed method of sampling by metal casting with help of the LFC technology gives a possibility to reduce labour intensity [5]. Usually, it was practiced to pour the sample into the gating system with disposal for re-melting together with it.

Filling with metal with spontaneous sampling in one mould with casting according to one model of the CP, or through a model cluster, took place without labour and time waste (increasing the express level). The TA pro-

cesses took place spontaneously in the same mould with the casting without the need to comply with the safety rules inherent in a separate pouring from the sampler ladle or filling it by immersion in the melt. And the conditions for solidification of the sample were similar to those for a casting in the same sand mould. The constancy of filling the volume of the sampler (obtaining an accurate sample) [5] is facilitated by the vacuum of the mould, increasing the filling of the mould with the metal due to the effect of vacuum suction of the metal. It is not difficult to form a sample model with a simple design when joining to gating systems or walls of a commodity casting model for all types of sand moulds. A model made of polystyrene with a specified density is about 300 times lighter than, for example, liquid iron, which easily replaces it when pouring into a sand mould.

Molding the sample model in various fixtures with the shape of a commodity casting is recommended for preliminary analysis of the metal with the possibility of correcting its composition before pouring the mould to obtain a casting. The TA variants developed by us provide its flexibility, expanding the possibilities of its use in comparison with the known methods for the operational forecasting of technological and performance attributes of metal (chemical composition, structure, casting, physical-mechanical and other properties) in the production of castings for various purposes.

Optimization of Cast Structures and Shaping Technologies

An important cycle of our research is devoted to the optimization of cast structures and shaping technologies in order to reduce their weight and casting from high-strength metals. The use of the developed TA method [5] makes it possible to study the crystallization, mechanical and other operational characteristics of the casting at any point of the installation of the sample model and liquid metal. Analysis and comparison of TA indicators on different walls of the casting is proposed as a mechanism of practical optimization according to the criterion of dependence of steel intensity and strength of castings in order to select the optimal options for their design, to optimize their wall thicknesses according to TA data. This gives a possibility to adapt computer methods for determining and forecasting the performance attributes of cast parts, to create on this basis digital twins of castings, as well as databases for automated systems for designing castings, taking into account the technical and economic indicators of a new class of cast structures of low steel intensity.

We also improved the method of sampling with a portable sampler [6] in the form of an evacuated casting mold in a metal cup (container) with a capacity of 0.5–0.7 l. The sampler was moulded, making the solidification conditions for the sample in it as close as possible to those for a commodity casting (composition of the sand mixture, the degree of its compaction, etc.). The sampler was installed on a stand and pumping was turned off, providing cooling of the sample in a sand mixture with control and recording of the temperature of the sample metal during the TA process.

In the process of developing the described TA methods [5, 6], the most common foreign programs were also considered, which can be suitable as software for the adequate identification of temperature curves of TA, measured over time, with the corresponding properties, chemical composition, or structure of a cast controlled metal sample. Foreign programs are created for foreign standards of raw materials and grades of casting alloys, types and characteristics of casting equipment and technical specifications for products. Their use implies not only the need for language translation, but also the search for domestic analogues of material and technical conditions with certain errors and tolerances.

All foreign software is not cheap, it is updated and monitored via the Internet, it constantly requires servicing in rapidly changing software environment. Domestic enterprises have difficulties finding sufficient funds for that purpose. In addition, technical and commercial data protection must be applied. The absence of mathematical models of the dependence of the cooling rate of a cast sample on the modes of its cooling in a casting mould causes the low ability of computer processing of TA data. These circumstances complicate the control of the cooling process and the determination of its optimal modes. They do not allow online forecasting of structure formation and performance attributes of castings.

In particular domestic software products with almost instantaneous presentation of the results of TA on the monitor screen, and even more are necessary for automation, digitalization and manufacturing application of control systems of TA, which are being actively improved by domestic engineering science. The results of the inspection of quality control systems for metal products using the TA method showed that the solution of key problems of improving the quality of foundry production is impossible without the creation of automated software tools for control and support of this production by information technology specialists. At the same time, the software of such effective control systems as TA must be equipped with a software and information data set specific for it, with means for absorbing noise and reducing the influence of the human factor on the accuracy of measurements of thermo-chemical processes. The method of recognition of cooling curves of a casting used in TA by comparing the coefficients of models approximating these curves (differential TA method) has low recognition accuracy for determining the chemical composition of a metal melt in a furnace or an alloy of an unknown casting.

The development of domestic foundry computer technologies based on a database of materials, metals and alloys, as well as methods for improving TA methods using adaptive filtering methods, inductive approach and

other developments in applied mathematics will allow foundry workers to achieve increased productivity. Modern foreign software products are difficult to use in Ukraine.

Review of TA Monitoring Software

Scientific progress in the field of foundry production takes place due to the widespread use of computers and special software.

To date, many different software products have been developed in order to solve the problems of different stages of the casting process. Let's briefly consider some of them. MAGMA5 software, developed by the specialists in the field of metal casting by MAGMA GmbH (Aachen, Germany) [7]. To date, this software is considered one of the best in the industry. This product is used by more than eight hundred companies in the world.

NovaCast has developed a unique, highly efficient technology for the production of cast iron with vermicular graphite based on careful metallurgical preparation of base cast iron. In the process of adjusting the composition to control the thermodynamic properties of the metal an advanced system of thermal analysis is used.

ATAS® software system is designed to control metallurgical processes in the production of castings from gray cast iron and high-strength cast iron. ATAS is a comprehensive system that includes equipment, software, and user training and support provided by a team of skilled metallurgists.

The technology, called PrimeQuality CGI (PQ-CGI® is a technology for producing castings from high-quality compacted graphite cast iron [8]. It allows suppressing the formation of platelet graphite and provides the balance of oxides in the metal necessary to create optimal conditions for the formation of vermicular graphite inclusions.

A more detailed overview of the existing software for processing thermal processes with a comparative table of existing tools is given in [9].

This review shows that foreign software tools such as Magmasoft, CastCAE, JSCast, AnyCasting do not have a database of metals and alloys used in domestic production, they require modern computer equipment, appropriate operating system, constant updating of functional modules and most importantly, they are designed to work on large-scale production and can not be used on small plants.

Therefore, a new technology was developed [10]. It includes a domestic database of metals and alloys and solves the problems the founder faces during the manufacture of castings. These problems include determining the chemical composition of the unknown casting, obtaining recommendations for choosing the optimal cooling mode for the given structure of a future product.

A Computer Technology for Modeling Thermal Processes

Founders, especially in industries with frequent readjustment of the product range, in their activities meet the need to perform complex scientific and technical calculations related to solving problems of modelling and optimization of metallurgical processes in order to make effective decisions to achieve the desired result. It is important for the company to develop a software product that will contain a database of metals and alloys, their chemical and mechanical properties in accordance with the State Standard DSTU, as well as to process express test results, analyze and select the necessary components to obtain a quality end product, to adjust an operational mode of the foundry.

The developed technology is designed to solve practical problems of modelling thermal processes in the field of foundry production. The toolkit should have an architecture that provides for the expansion of its functionality by introducing new modules and updating existing ones with new information. The technology includes a domestic database of metals and alloys and 3 functional modules that interact with each other during operation. The software is easy to use, has a fairly clear interface, focused on domestic small-scale production and meets its requirements. Fig. 2 shows a diagram and a detailed description of the modules of this technology [11].

Fig. 2 shows a scheme of the software equipped with the following functional modules:

Module 1 is designed to compare the functions that describe the cooling process of the casting; a model is built and used; it allows selecting quickly and accurately from the database of reference functions exactly the one that is closest to the experimental.

Module 2 is designed to determine the physical and mechanical properties of the casting by chemical composition; the developed models help to determine the physical and mechanical properties of the casting by chemical composition.

Module 3 is designed to determine the cooling modes; the developed models allow selecting the required cooling modes to obtain the desired structure of the future product.

The software is supplemented with functional modules: filtering of the recorded temperature curves of cooling of casting (Module 4 - Polynomial Filtering) and the ThermoEX module (Module 5) is intended for visualization of the recorded cooling curve and definition of characteristic points on it; the module Polynomial Filtering is meant to filter it from noise present in experimental data.

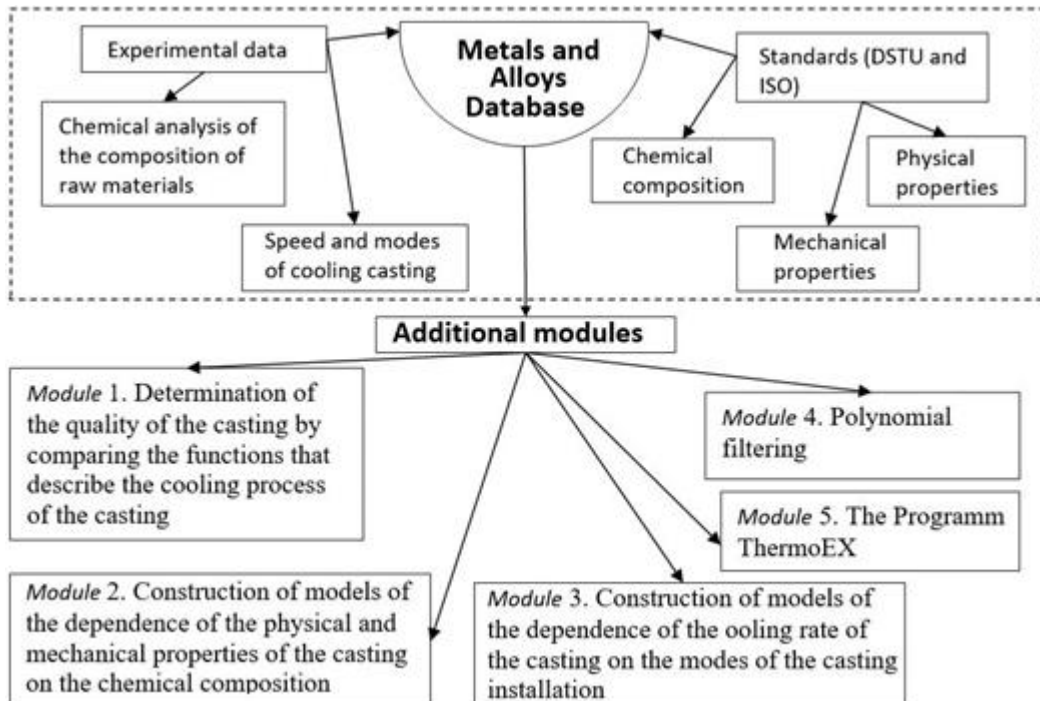


Figure 2 – Block diagram of computer technology for modelling thermal processes of foundry and metallurgical production

Fig. 3 shows a window with the interface of the implemented technology, which includes the ThermoEX submodule [12], which allows to visualize the obtained cooling curve.

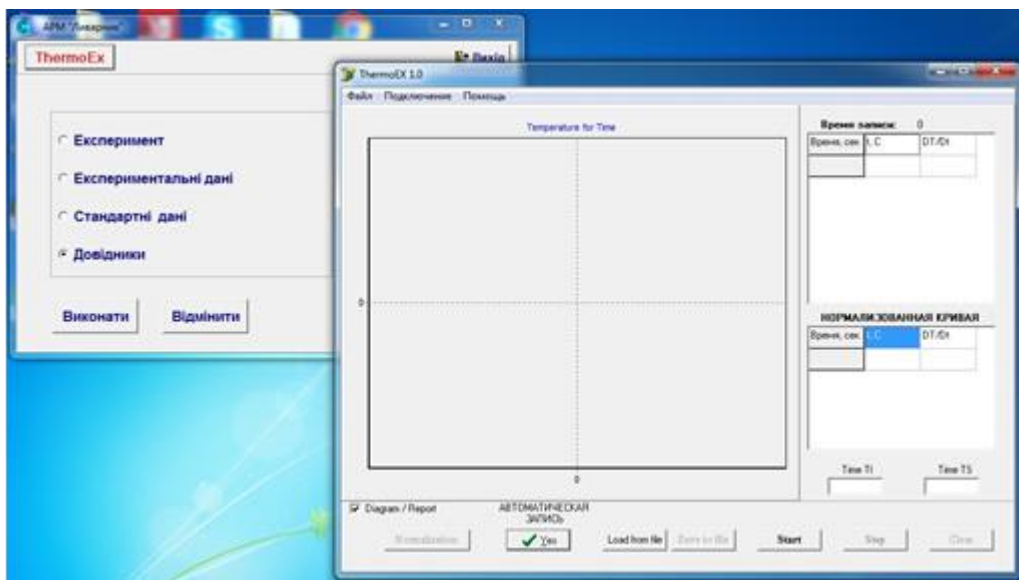


Figure 3 – ThermoEX Module Startup Window

After being processed, the curves are compared with the reference curves, which are stored in the database of experimental data and their chemical composition and physical and mechanical properties are determined. All data can be saved to the database of experimental data.

When the Load from file function is selected, the module addresses the database of experimental data that have just been recorded and written to the appropriate .txt file for further processing.

Fig. 4 shows how the ThermoEX program operates.

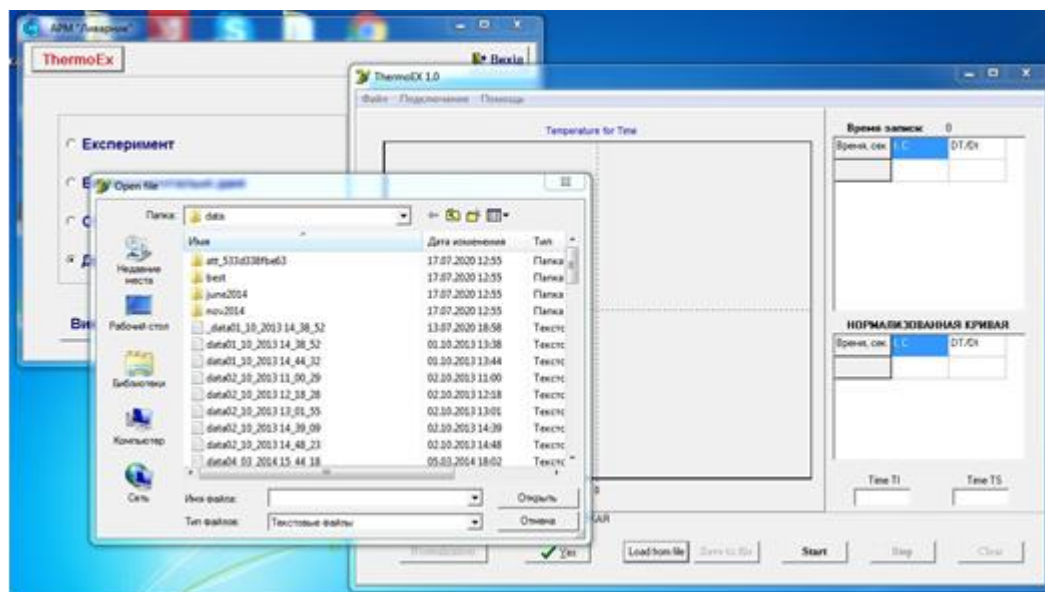


Figure 4 – Example of ThermoEX access to the experimental database

The technology allows controlling the cooling process of the casting, which can simplify the work of founders and avoid defective products

The developed computer technology for solving the problems of modelling the cooling processes of metal foundry products allows increasing the efficiency of support of founder's solutions in the process of making castings due to the developed models.

The developed technology consists of a domestic database of metals and alloys and solves the problems which founders face during the manufacture of castings: determining the chemical composition of the unknown casting, obtaining recommendations for choosing the optimal cooling mode of the casting to obtain a given structure of the future product.

The developed computer technology meets the needs of domestic production and solves a number of problems that arise during the manufacture of castings.

Conclusions

The article describes the characteristics of TA and thermal processes. Methods of quality control of cast iron are depicted. Methods of thermal analysis of metal, as well as methods of optimization of cast structures are listed. A brief overview of software for monitoring thermal processes is given. The block diagram of computer technology intended for modeling of thermal processes, the description of problems which it solves, and also its short description is given. Software to support the foundry's solutions, which will automate certain stages of the casting process, improve the quality of metal products, has been developed. It can be considered as the first steps towards the creation of artificial intelligence systems for the management of foundry and metallurgical processes.

References

- [1] Chemical analysis versus thermal analysis of Cast Iron. Global Casting Magazine, 2016. Vol. 6 (3), pp. 54. [Online] Available at: <http://content.yudu.com/web/y5b2/0A1snzj/GlobCastingVol6No3/flash/resources/index.htm>. Accessed 06 Dec. 2020.
- [2] A. s. USSR №1636766, IPC G01N 33/20. Method of determination of alloying impurity elements and gases in alloys / N.A. Abramov, B.A. Greshishchev, V.A. Dinershtein, S.A. Kozlov, M.D. Molchanov, A.A. Smulsky, Publ. 1991. Bull. 11 [in Ukrainian].
- [3] E. V. Zakharchenko, L. D. Zhukov, E. A. Sirenko, et al., «Improvement of the universal method of thermal express analysis of liquid cast irons, based on the recognition of the shape of the cooling curves», *Casting processes*, 2, pp. 3–9. 2015 [In Russian].
- [4] Patent Of Ukraine № 99968, IPC G01N 33/20, G01N 25/04. Method of thermal analysis of liquid cast iron / E. V. Zakharchenko, K. A. Sirenko, A. L. Goncharov, A. V. Bogdan., Publ. 2015, bul. 12 [in Ukrainian].
- [5] Patent 112646 Ukraine, IPC G01N 33/20. Method of thermal analysis of metal and alloy / V. S. Doroshenko, O. V. Tokova, Publ. 2016, Bull. 24 [in Ukrainian].
- [6] Patent 131912 Ukraine, IPC G01N 33/20, G01N 25/04. Express method of thermal analysis or (and) sampling of metal or alloy / V. S. Doroshenko, V. O. Shinsky, O. V. Tokova. Publ. 2019, Bull. 3 [in Ukrainian].

- [7] MAGMASOFT autonomous engineering. [Online]. Available: <http://www.magmasoft.com>. Accessed 18 Jan. 2016.
- [8] NovaCast Technologies AB. [Online]. Available: <http://www.ruscastings.ru/work/168/2130/2984/2988>. Accessed 27 Feb. 2019.
- [9] O. V. Tokova, «An overview of methods and tools for computer modeling of foundry production processes», *Inductive modeling of complex systems. Collected research papers, Issue 9*, Kyiv: IRTC ITS NASU, pp. 204–213. 2017 [in Ukrainian].
- [10] O. V. Tokova, «The Task of the Computer Technology Construction for Thermal Processes Modeling of Foundry Production», *Upravlausie sistemy i masiny*, 4, pp. 84–95. 2018 [in Ukrainian].
- [11] O. Tokova, Ye. Savchenko, V. Stepashko, «Construction of a computer technology for information support of decisions in the foundry production process», *Cybernetics and Computer Engineering*, 4, pp. 41–55. 2019.
- [12] I. V. Varava, «Information technologies of control of a complex scientific experiment in a multiphase environment». Abstract of Ph.D. dissertation: 05.13.06, Kyiv, 2016 [in Ukrainian].

Стаття надійшла: 09.12.2021.

Відомості про авторів

Токова Олена Володимирівна – кандидат технічних наук, молодший науковий співробітник відділу інформаційних технологій індуктивного моделювання.

Дорошенко Володимир Степанович – доктор технічних наук, старший науковий співробітник, провідний науковий співробітник відділу фізико-хімії ливарних процесів.

Янченко Олександр Борисович – кандидат технічних наук, доцент кафедри галузевого машинобудування.

О. В. Токова¹, В. С. Дорошенко², О. Б. Янченко³

КОМП'ЮТЕРНІ СИСТЕМИ ТЕРМІЧНОГО АНАЛІЗУ ДЛЯ МОНІТОРИНГУ ЛИВАРНИХ ТА МЕТАЛУРГІЙНИХ ПРОЦЕСІВ

¹Міжнародний науково-навчальний центр інформаційних технологій і систем НАН та МОН України, Київ

²Фізико-технологічний інститут металів та сплавів НАН України, Київ

³Вінницький національний технічний університет, Вінниця

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 519.65

О. В. Бісікало¹, Р. Н. Кветний¹, О. В. Кудрик¹, Ю. А. Олексій²

ЗАСТОСУВАННЯ ІНТЕРПОЛЯЦІЇ КУБІЧНИМИ СПЛАЙНАМИ В ІНТЕЛЕКТУАЛЬНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ ПРОГНОЗУВАННЯ ФАЗОВОЇ СТАБІЛЬНОСТІ ТВЕРДИХ РОЗЧИНІВ

¹ Вінницький національний технічний університет, Вінниця² Донецький національний університет імені Василя Стуса, Вінниця

Анотація. Дана дослідницька робота присвячена застосуванню інтерполяції кубічними сплайнами для розв'язання актуальної задачі прогнозування фазової стабільності твердих розчинів. Для розрахунку енергій змішування (параметрів взаємодії) та критичних температур розкладання (температур стабільності) твердих розчинів було використано теорію ізоморфних заміщень у кристалах Урусова. Запропонована інтелектуальна інформаційна система (ІІС) автоматизує побудову діаграм, що дає змогу прогнозувати термодинамічну стійкість твердих розчинів. ІІС також надає інтерактивні функції для зручності користувачів. Отримані результати можуть бути корисними при виборі співвідношення компонентів у «змішаних» матрицях, кількості активатора в люмінесцентних, лазерних та інших практично важливих матеріалах, а також у матрицях для іммобілізації токсичних і радіоактивних відходів. При цьому результати застосування інтерполяції на великих відрізках, тобто з відносно великою кількістю вузлових точок, часто виходять незадовільними. З одного боку, при великих відстанях між вузловими точками знижується точність інтерполяції, а, з іншого боку, зі збільшенням кількості вузлових точок через вплив багаточленів високих порядків виникають осциляції інтерполяційної кривої, оскільки тільки таким чином криву можна змусити пройти через задані точки. Такий стан не відповідає реальній залежності, що випливає з табличних значень вузлових точок. Тому запропоновано застосувати сплайн інтерполяцію, яка має низку важливих переваг. По-перше, це висока збіжність. На відміну від інтерполяційних поліномів Лагранжа послідовність кубічних сплайнів на рівномірній сітці вузлів завжди сходиться до безперервної функції, що інтерполюється. По-друге, має мінімальну чутливість до похибки вихідних даних. Невеликі зміни значень функції в одній або кількох сусідніх точках інтерполяції не позначається дуже істотно на поведінці сплайну на деякому віддаленні від цих точок. Як наслідок вище сказаного – більш висока точність інтерполяції. В результаті дослідження формалізовано розрахунок невідомих коефіцієнтів для запропонованих сплайнів та визначено переваги практичного застосування запропонованого методу інтерполяції. Проведено вдосконалення ІІС фазової стабільності твердих розчинів з використанням інтерполяції кубічними сплайнами, як наслідок – було підвищено точність результатів на 4,96%.

Ключові слова: інтелектуальна інформаційна система, тверді розчини, математичне моделювання, інтерполяція, сплайни.

Abstract. This research work is devoted to the use of cubic spline interpolation to solve the current problem of predicting the phase stability of solid solutions. The theory of isomorphic substitutions in Urusov crystals was used to calculate the mixing energies (interaction parameters) and critical decomposition temperatures (stability temperatures) of solid solutions. The proposed intelligent information system (IIS) automates the construction of diagrams, which allows to predict the thermodynamic stability of solid solutions. IIS also provides interactive features for user convenience. The obtained results can be useful in choosing the ratio of components in "mixed" matrices, the amount of activator in luminescent, laser and other practically important materials, as well as in matrices for immobilization of toxic and radioactive waste. The results of the application of interpolation on large segments, ie with a relatively large number of nodes, are often unsatisfactory. On the one hand, at large distances between nodes the interpolation accuracy decreases, and on the other hand, with increasing number of nodes due to the influence of high-order polynomials there are oscillations of the interpolation curve, because only in this way the curve can be forced to pass through given points. This state does not correspond to the real dependence resulting from the tabular values of the nodes. Therefore, it is proposed to use spline interpolation, which has a number of important advantages. First, it is high convergence. In contrast to Lagrange interpolation polynomials, the sequence of cubic splines on a uniform grid of nodes always converges to a continuous interpolated function. Secondly, we have minimal sensitivity to the error of the original data. Small changes in the values of the function at one or more adjacent interpolation points do not significantly affect the behavior of the spline at some distance from these points. As a consequence of the above - higher interpolation accuracy. As a result of the research the calculation of unknown coefficients for the proposed splines is formalized and the advantages of practical application of the proposed interpolation method are determined. The IIS of phase stability of solid solutions was improved using interpolation by cubic splines, as a result, the accuracy of the results was increased by 4.96%.

Key words: intelligent information system, solid solutions, mathematical modeling, interpolation, splines.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-94-102>.

Вступ

При поданні табличних даних функціональними або графічними залежностями використовують два основних підходи [1]. При одному з них потрібно, щоб апроксимуюча крива (кусково-гладка) проходила через усі точки, задані таблицею. Це вдається зробити за допомогою методів інтерполяції, причому найчастіше використовують інтерполяційні багаточлени, що подаються у формах Лагранжа або Ньютона [2]. За іншого підходу дані апроксимують простою функцією, яка застосовується у всьому діапазоні табличних даних, але необов'язково проходить через усі точки. Такий підхід називають підгонкою кривої, яку прагнуть провести так, щоб її відхилення від табличних даних були мінімальними. Зазвичай прагнуть звести до мінімуму суму квадратів різниць між значеннями функції, визначеними обраною кривою та відповідними даними таблиці. Такий метод підгонки називають методом найменших квадратів. Той та інший підхід мають свої переваги та недоліки.

Щодо методу найменших квадратів, то тут найбільша складність виникає при виборі відповідних апроксимуючих функцій. Цей вибір має здійснюватися з урахуванням специфіки табличних даних, під якою розуміється їх періодичність, ступеневий, експоненційний або логарифмічний характер, властивості симетрії, наявність асимптотики. Якщо табличні дані відповідають якійсь закономірності і добре описуються, наприклад, лінійною або параболічною залежністю, то даний метод дає хороші результати, в іншому випадку можуть виникнути серйозні розбіжності між табличними даними та даними, отриманими на основі апроксимуючої кривою.

При використанні інтерполяції на великих відрізках, тобто з відносно великою кількістю вузлових точок, її результати часто виходять незадовільними. З одного боку, при великих відстані між вузловими точками знижується точність інтерполяції, а, з іншого боку, зі збільшенням кількості вузлових точок через вплив багаточленів високих порядків виникають осциляції інтерполяційної кривої, оскільки тільки таким чином криву можна змусити пройти через задані точки. Зрозуміло, це ніяк не відповідає реальній залежності, що впливає з табличних значень вузлових точок. Виходом із становища може бути кускова інтерполяція нижчого порядку, тобто у цьому випадку інтерполяція здійснюється за невеликою кількістю вузлових точок відрізка, а потім багаточлени об'єднують у загальну інтерполяційну функцію. Проте при цьому в точках стикування зазвичай терпить розрив перша похідна, що також призводить до помилок інтерполяції.

Значною мірою вільним від перерахованих вище недоліків є сплайн-інтерполяція, яка відносно недавно стала використовуватись у обчислювальній математиці [1]. Свою назву (у перекладі з англійської «spline» – пружна лінійка) даний метод отримав тому, що форма розрахункової інтерполяційної кривої збігається з профілем пружної лінійки, яку необхідно певним чином зігнути, щоб вона проходила через вузлові точки. Під сплайном розуміють сукупність пов'язаних інтерполяційних поліномів, що описують кусково-гладку криву, що проходить через вузлові точки, причому в місцях сполучення перша та друга похідна безперервні. Зазвичай обмежуються поліномом третього ступеня, тобто кубічним сплайном.

Мета

Метою статті є підвищення точності результатів інтелектуальної інформаційної системи прогнозування фазової стабільності твердих розчинів за рахунок застосування в ній можливостей інтерполяції кубічними сплайнами.

Порівняння та розв'язання задачі

Порівняно з іншими інтерполяційними методами сплайн інтерполяція має низку важливих переваг [3]. По-перше, це гарна збіжність. На відміну від інтерполяційних поліномів Лагранжа послідовність кубічних сплайнів на рівномірній сітці вузлів завжди сходиться до безперервної функції, що інтерполюється [4]. По-друге, мінімальна чутливість до похибки вихідних даних. Невеликі зміни значень функції в одній або кількох сусідніх точках інтерполяції не позначається дуже істотно на поведінці сплайну на деякому віддаленні від цих точок. Як наслідок вище сказаного – більш висока точність інтерполяції.

Суть методу кубічної сплайн-інтерполяції полягає в наступному (1). Нехай є $(i + 1)$ вузлових точок (x, y) , що розбивають деякий відрізок $[a, b]$ на осі абсцис на t інтервалів. Для кожного інтервалу потрібно розрахувати функції:

$$S_i(x) = k_i + k_2 x + k_3 x^2 + k_4 x^3 \quad (1)$$

причому ні самі функції, ні їх перша та друга похідні не повинні зазнавати розриву в місцях сполучення, що призводить до додаткових умов, що мають вигляд:

$$S_i(x_i) = S_{i+1}(x_i) = y_i \quad (i = 1, 2, \dots, m) \quad (2)$$

$$S'_i(x_i) = S'_{i+1}(x_i) \quad (i = 1, 2, \dots, m - 1) \quad (3)$$

$$S''_i(x_i) = S''_{i+1}(x_i) \quad (i = 1, 2, \dots, m - 1) \quad (4)$$

Виходить $4m$ невідомих та $(4m-2)$ рівняння. Для того, щоб система мала розв'язок, потрібні ще два рівняння, в якості яких використовують додаткові умови, що накладаються на функцію та її похідні межі відрізка $[a, b]$. Найчастіше використовують так званий нормальний випадок, згідно з яким другі похідні кубічного сплайну на межах інтерполяційного відрізка $[a, b]$ дорівнюють нулю.

Рішення системи з 4m рівнянь спрощується, якщо уявити сплайни у вигляді:

$$S_i(x) = ty_i + \bar{t}y_{i+1} + x_i \left[(k_{i-1} - d_i)t\bar{t}^2 - (k_i - d_i)t^2\bar{t} \right], \quad (5)$$

$$\text{де } t = \frac{x - x_{i-1}}{x_i - x_{i-1}}, \quad \bar{t} = 1 - t, \quad d_i = \frac{y_i - y_{i-1}}{x_i - x_{i-1}}, \quad (i = 1, 2, \dots, m).$$

Нескладно показати, що при такому виборі сплайнів їх «зшивання» в точках сполучення забезпечується автоматично. Кожне з рівнянь (5), починаючи з другого, містить лише один невідомий коефіцієнт. Це дає змогу звести завдання знаходження інтерполяційних функцій (1) до вирішення системи лінійних рівнянь з невідомими коефіцієнтами k . У матричній формі система рівнянь має вигляд:

$$\begin{bmatrix} 2 & 1 & 0 & \dots & 0 \\ \Delta x_2 & 2(\Delta x_1 + \Delta x_2) & \Delta x_1 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & \Delta x_m & 2(\Delta x_{m-1} + \Delta x_m) & \Delta x_{m-1} \\ 0 & 0 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} k_0 \\ k_1 \\ \dots \\ k_{m-1} \\ k_m \end{bmatrix} = \begin{bmatrix} d_1 \\ d_1 \Delta x_2 + d_2 \Delta x_1 \\ \dots \\ d_{m-1} \Delta x_m + d_m \Delta x_{m-1} \\ d_m \end{bmatrix}, \quad (6)$$

де $\Delta x_i = x_i - x_{i-1}$.

Знайдені в результаті розв'язання цієї системи (6) коефіцієнти k , підставляються в систему рівнянь (5), що дозволяє розрахувати масив точок, які визначають криву, що проходить через вузлові точки.

Для прикладу візьмемо графік системи $\text{La}_{1-x}\text{Ln}_x\text{PO}_4$ [5, 6], з кроком обчислень 0.25, x в межах від 0 до 0.5.

Після розрахунку, без використання інтерполяції кубічними сплайнами маємо такі результати (таблиця 1)

Таблиця 1 – Результати без використання інтерполяції кубічними сплайнами

№	x	y
0	0	86
1	0.25	446
2	0.5	488

Використаємо рівняння кубічного сплайна на окремій ділянці.

$$S(x) = a + b(x - x_0) + c(x - x_0)^2 + d(x - x_0)^3 \quad (7)$$

Для двох ділянок зробимо 2 рівняння:

$$\begin{cases} S_0 = a_0 + b_0(x - x_0) + c_0(x - x_0)^2 + d_0(x - x_0)^3 \\ S_1 = a_1 + b_1(x - x_1) + c_1(x - x_1)^2 + d_1(x - x_1)^3 \end{cases} \quad (8)$$

Підставимо вхідні дані в рівняння:

$$\begin{cases} S_0 = a_0 + b_0(x - 0) + c_0(x - 0)^2 + d_0(x - 0)^3 \\ S_1 = a_1 + b_1(x - 0.25) + c_1(x - 0.25)^2 + d_1(x - 0.25)^3 \end{cases} \quad (9)$$

Отже, маємо 8 невідомих коефіцієнтів.

Для розрахунку коефіцієнтів використаємо наступні умови:

1) Сплайни повинні проходити через вузлові точки.

Сплайн $S_0 = a_0 + b_0(x - 0) + c_0(x - 0)^2 + d_0(x - 0)^3$, проходить через точки, які позначені у таблиці 2, жовтим кольором.

Таблиця 2 – Вузлові точки сплайна S_0

№	x	y
0	0	86
1	0.25	446
2	0.5	488

Сплайн $S_1 = a_1 + b_1(x - 0.25) + c_1(x - 0.25)^2 + d_1(x - 0.25)^3$, проходить через точки, які позначені у таблиці 3, жовтим кольором.

Таблиця 3 – Вузлові точки сплайна S_1

№	x	y
0	0	86
1	0.25	446
2	0.5	488

Після підстановки та спрощення, отримаємо систему з 4 рівнянь:

$$\begin{cases} a_0 = 86 \\ a_0 + 0.25b_0 + 0.625c_0 + 0.015625d_0 = 446 \\ a_1 = 446 \\ a_1 + 0.25b_1 + 0.625c_1 + 0.015625d_1 = 488 \end{cases} \quad (10)$$

2) В стиках сплайнів повинна забезпечуватися гладкість - не повинно бути зламів та зміни кривизни.

Знайдемо першу та другу похідну кожного сплайна:

$$\begin{cases} S'_0 = b_0 + 2c_0(x-0) + 3d_0(x-0)^2 \\ S'_1 = b_1 + 2c_1(x-0.25) + 3d_1(x-0.25)^2 \\ S''_0 = 2c_0 + 6d_0(x-0) \\ S''_1 = 2c_1 + 6d_1(x-0.25) \end{cases} \quad (11)$$

Виконаємо умову (3) та (4), підставивши точку, позначену у таблиці 4, жовтим кольором.

Таблиця 4 – Вузлова точка умови 2

№	x	y
0	0	86
1	0.25	446
2	0.5	488

Після підстановки та спрощення, отримаємо систему з 2 рівнянь:

$$\begin{cases} b_0 + 0.5c_0 + 1.875d_0 - b_1 = 0 \\ 2c_0 + 1.5d_0 - 2c_1 = 0 \end{cases} \quad (12)$$

3) Задамо поведінку сплайнів в початковій та кінцевій точках.

Наприклад, задамо нульову кривизну сплайнів

$$\begin{cases} S''_0 = 0 \\ S''_2 = 0 \end{cases} \quad (13)$$

Підставимо в сплайни S''_0 та S''_2 точки, які позначені жовтим кольором, з таблиць 5 та 6, відповідно.

Таблиця 5 –Точка для сплайна S_0''

№	x	y
0	0	86
1	0.25	446
2	0.5	488

Таблиця 6 – Точка для сплайна S_1''

№	x	y
0	0	86
1	0.25	446
2	0.5	488

Після підстановки та спрощення, отримаємо систему з 2 рівнянь:

$$\begin{cases} 2c_0 = 0 \\ 2c_1 + 1.5d_1 = 0 \end{cases} \quad (14)$$

Отже, отримаємо систему з 8 лінійних рівнянь:

$$\begin{cases} a_0 = 86 \\ a_0 + 0.25b_0 + 0.625c_0 + 0.015625d_0 = 446 \\ a_1 = 446 \\ a_1 + 0.25b_1 + 0.625c_1 + 0.015625d_1 = 488 \\ b_0 + 0.5c_0 + 1.875d_0 - b_1 = 0 \\ 2c_0 + 1.5d_0 - 2c_1 = 0 \\ 2c_0 = 0 \\ 2c_1 + 1.5d_1 = 0 \end{cases} \quad (15)$$

Спростивши її, отримаємо:

$$\begin{cases} a_0 = 86 \\ a_1 = 446 \\ c_0 = 0 \\ 0.25b_0 + 0.015625d_0 = 360 \\ 0.25b_1 + 0.625c_1 + 0.015625d_1 = 42 \\ b_0 + 1.875d_0 - b_1 = 0 \\ 1.5d_0 - 2c_1 = 0 \\ 2c_1 + 1.5d_1 = 0 \end{cases} \quad (16)$$

Складемо систему рівнянь, у матричній формі (6).

$$\begin{bmatrix} 0.25 & 0.015625 & 0 & 0 & 0 \\ 0 & 0 & 0.25 & 0.625 & 0.015625 \\ 1 & 1.875 & -1 & 0 & 0 \\ 0 & 1.5 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2 & 1.5 \end{bmatrix}^{-1} \begin{bmatrix} 360 \\ 42 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1762 \\ -5110 \\ 804 \\ -3832 \\ 5110 \end{bmatrix} \quad (17)$$

В результаті отримаємо значення вільних коефіцієнтів (таблиця 7).

Таблиця 7 – Вільні коефіцієнти

a_0	86
b_0	1762
c_0	0
d_0	-5110
a_1	446
b_1	804
c_1	-3832
d_1	5110

Підставимо вільні коефіцієнти в рівняння (8), та отримаємо такі результати (таблиця 8).

Таблиця 8 – Результати з використанням інтерполяції кубічними сплайнами

№	x	y
0	0	85,65621
1	0,025	129.6339
2	0,05	173.1325
3	0,075	215.6729
4	0,1	256.7761
5	0,125	295.9629
6	0,15	332.7543
7	0,175	366.6711
8	0,2	397.2343
9	0,225	423.9648
10	0,25	446,38357
11	0,275	464.1711
12	0,3	477.6468
13	0,325	487.2899
14	0,35	493.5793
15	0,375	496.9942
16	0,4	498.0136
17	0,425	497.1167
18	0,45	494.7825
19	0,475	491.4902
20	0,5	487,71876

Побудуємо графік на основі отриманих результатів в інтелектуальній інформаційній системі прогнозування фазової стабільності твердих розчинів [7] (рисунок 1):

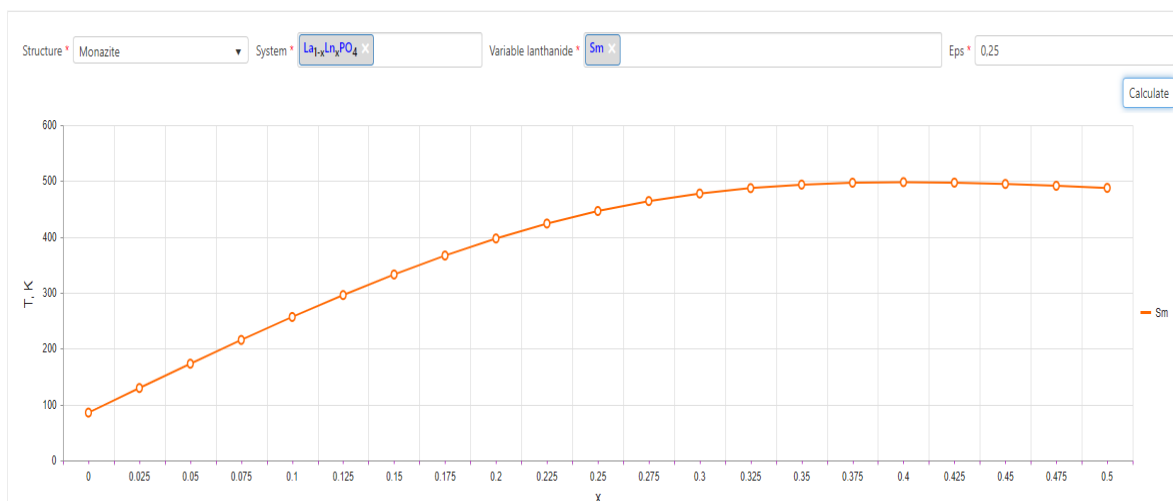


Рисунок 1 – Графік з використанням інтерполяції кубічними сплайнами

Для наочності наведено графік тієї ж самої системи, але без застосування інтерполяції (рисунок 2):

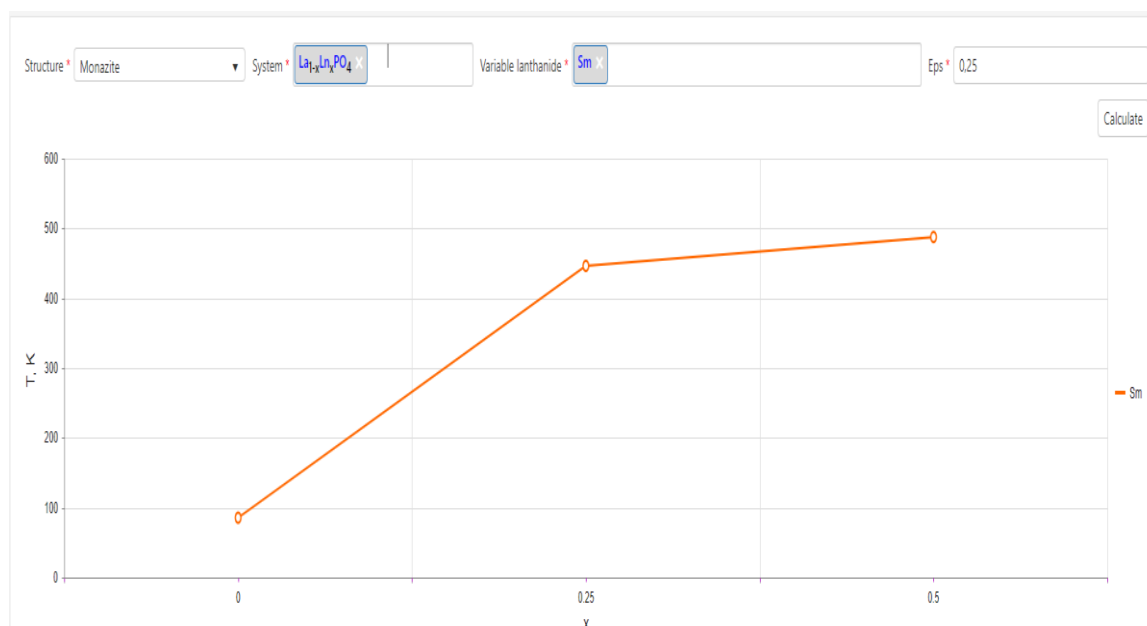


Рисунок 2 – Графік без використання інтерполяції кубічними сплайнами

Візьмемо літературні дані даної системи [8] та проведемо порівняння літературних результатів з результатами інтерполяції кубічними сплайнами та результатами без інтерполяції кубічними сплайнами (таблиця 9).

Таблиця 9 – Порівняння літературних результатів з інтерполяцією кубічними сплайнами та результатів без інтерполяції кубічними сплайнами

x	y з інтерполяцією	y без інтерполяції	y [7]	Δy з інтерполяцією	Δy без інтерполяції	Підвищено точність %
0	85,65621	85,65621	86	0,34379	0,34379	0
0,03	129,63	120,58572	235	105,3661	114,41428	7,908261102
0,05	173,13	155,10631	277	103,8675	121,89369	14,78845213
0,1	256,78	250,27946	330	73,2239	79,72054	8,149267428
0,15	332,75	316,67127	366	33,2457	49,32873	32,60377877
0,2	397,23	424,96536	393	4,2343	31,96536	86,75347313
0,25	446,38357	446,38357	413	33,38357	33,38357	0
0,3	477,65	478,52042	428	49,6468	50,52042	1,729241364
0,35	493,58	482,27911	440	53,5793	42,27911	-26,72759668
0,4	498,01	483,20394	448	50,0136	35,20394	-42,06818896
0,45	494,78	486,62353	452	42,7825	34,62353	-23,56481272
0,5	487,71876	487,71876	452	35,71876	35,71876	0

Дані таблиці 9, графічно представлено на рисунку 3.

Отже, поравувавши середнє значення, підвищення точності кожної точки, які наведені у таблиці 8, отримуємо 4,96%.

Висновки

В даній роботі проведено вдосконалення інтелектуальної інформаційної системи фазової стабільності твердих розчинів з використанням інтерполяції кубічними сплайнами. Було підвищено точність результатів на 4,96%. За результатами аналізу видно, що для системи $\text{La}_{1-x}\text{Ln}_x\text{PO}_4$ найкращі результати інтерполяції кубічними сплайнами досягаються на відрізку $0 - 0,25$, а для того, щоб зменшити погіршення на відрізку $0,25 - 0,5$, потрібно провести додаткову інтерполяцію, автори вважають, що потрібне проведення додаткових досліджень.

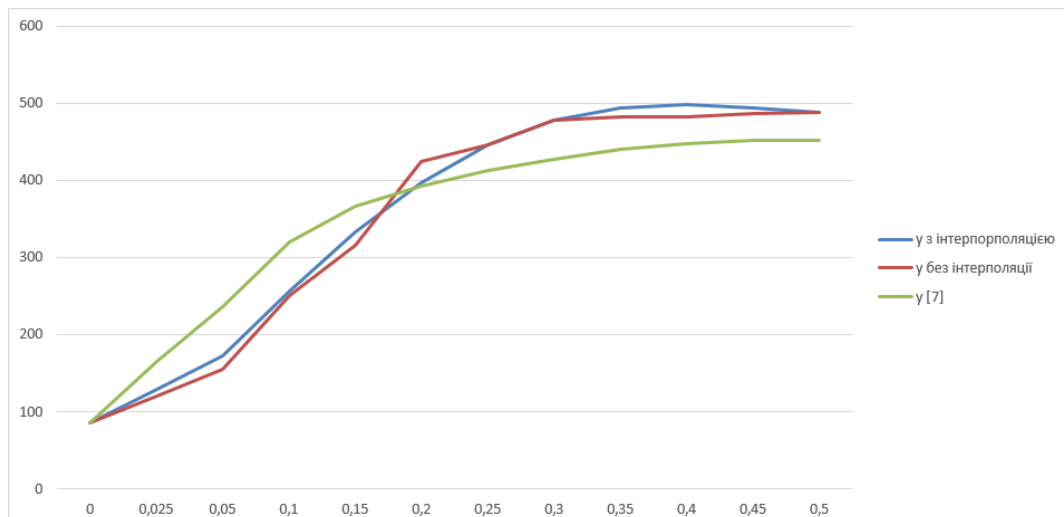


Рисунок 3 – Порівняння літературних результатів з інтерполяцією кубічними сплайнами та результатів без інтерполяції кубічними сплайнами

Список літератури

- [1] Р. Н. Кветний, В. Ю. Дементьев, М. О. Машницький, О. О. Юдін, *Різницеві методи та сплайни в задачах багатовимірної інтерполяції*, Вінниця: УНІВЕРСУМ, с. 193, 2011.
- [2] И. Н. Бронштейн, К. А. Семендяев, *Справочник по математике*. М.: Наука, 1981.
- [3] Д. М. Королев, В. Б. Никулин, С. А. Колесников, "Застосування сплайн-функцій для обробки результатів вимірювань", *Прилади та системи управління*, № 6, 1998.
- [4] Р. Н. Кветний, І. В. Богач, О. Р. Бойко, О. Ю. Софіна, О. М. Шушура, *Комп'ютерне моделювання систем та процесів. Методи обчислень. Частина 1, Навчальний посібник*, 2012, с. 193.
- [5] A. Meldrum, L. A. Boatner, L. M. Wang, "Ion-beam-induced amorphization of LaPO_4 and ScPO_4 ", *Nucl. Instr. and Meth. in Phys. Res. B*, vol. 127–128, pp. 160–165, 1997. doi: 10.1016 / S0168-583X (96) 00873-7.
- [6] E. Grechanovsky, N. N. Eremin, V. S. Urusov, "Radiation resistance of LaPO_4 (monazite structure) and YbPO_4 (zircon structure) from computer simulation data", *Physics of the Solid State*, vol. 55(9), pp. 1929–1935, 2013. doi: 10.1134 / S1063783413090138.
- [7] О. В. Кудрик, О. В. Бисикало, Ю. А. Олексій, С. В. Радио, "Intelligent information system for predicting chemicals with interactive possibilities", *CoLInS, Computational Linguistics and Intelligent Systems. CoLInS 2021*. [Електронний ресурс]. Режим доступу: <http://ceur-ws.org/Vol-2870/paper68.pdf>.
- [8] Е. И. Гетьман, Л. Б. Игнатова, С. В. Радио, "К вопросу расчета пределов замещений в твердых растворах монацитов редкоземельных элементов состава $\text{La}_{1-x}\text{Ln}_x\text{PO}_4$, где $\text{Ln} = \text{Pr} - \text{Dy}$ ", *Вісник Донецького національного університету імені Василя Стуса, Серія хімічні науки*, №2, с. 33-40, 2017.

Стаття надійшла: 28.04.2022.

References

- [1] R. N. Kvyetnyy, V. Yu. Dementiev, M. O. Mashnytsky, O. O. Yudin, *Difference methods and splines in multidimensional interpolation problems*, Vinnitsya: UNIVERSUM, p. 193, 2011 [in Ukrainian].
- [2] I. N. Bronshtein and K. A. Semendyaev, *Spravochnik po matematike*. M.: Nauka. 1981 [in Russian].
- [3] D. M. Korolev, V. B. Nikulin, S. A. Kolesnikov, "Device of spline functions for processing the results of simulation", *Application of the control system*, № 6. 1998 [in Ukrainian].
- [4] R. N. Kvyetnyy, I. V. Bogach, O. R. Boiko, O. Yu., Sofina, O. M. Shushura, *Computer modeling of systems and processes. Calculate methods. Part 1, Navchalny posibnik*, 2012, p. 193 [in Ukrainian].
- [5] A. Meldrum, L. A. Boatner, L. M. Wang, "Ion-beam-induced amorphization of LaPO_4 and ScPO_4 ", *Nucl. Instr. and Meth. in Phys. Res. B*, vol. 127–128, pp. 160–165, 1997. doi: 10.1016 / S0168-583X (96) 00873-7.
- [6] A. E. Grechanovsky, N. N. Eremin, V. S. Urusov, "Radiation resistance of LaPO_4 (monazite structure) and YbPO_4 (zircon structure) from computer simulation data", *Physics of the Solid State*, vol. 55(9), pp. 1929–1935, 2013. doi: 10.1134/S1063783413090138.
- [7] O. V. Kudryk, O. V. Bisikalo, Yu. A. Oleksii, S. V. Radio, "Intelligent information system for predicting chemicals with interactive possibilities", *CoLInS, Computational Linguistics and Intelligent Systems. CoLInS 2021*. [Online]. Available: <http://ceur-ws.org/Vol-2870/paper68.pdf>.

- [8] E. I. Hetman, L. B. Ignatova, S. V. Radio, "On the calculation of the limits of substitutions in solid solutions of monazites of rare earth elements of the composition $La_{1-x}Ln_xPO_4$, where $Ln = Pr - Dy$ ", *Visnyk Donetsky Vasyly Stus National University, Chemical Sciences Series*, №2, pp. 33-40, 2017 [in Russian].

Відомості про авторів

Бісікало Олег Володимирович – доктор технічних наук, професор, завідувач кафедри автоматизації та інтелектуальних інформаційних технологій.

Квєтний Роман Наумович – доктор технічних наук, професор, професор кафедри автоматизації та інтелектуальних інформаційних технологій.

Кудрик Олексій Володимирович – аспірант групи 126-21а, кафедра автоматизації та інтелектуальних інформаційних технологій.

Олексій Юлія Анатоліївна – студентка групи M20_д/102_ХМ, кафедра неорганічної, органічної та аналітичної хімії.

O. V. Bisikalo¹, R. N. Kvyetnyy¹, O. V. Kudryk¹, Y. A. Oleksii²

INTRODUCTION OF INTERPOLATION BY CUBIC SPLINES INTO INTELLIGENT INFORMATION SYSTEM FOR PREDICTING OF PHASE STABILITY OF SOLID SOLIDS

¹ Vinnytsia National Technical University, Vinnytsia

² Vasyly Stus Donetsk National University, Vinnytsia

УДК 519.876.5

М. П. Дивак, В. І. Манжула, А. М. Мельник, А. В. Пукас

МЕТОД СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ НЕЛІНІЙНИХ ІНТЕРВАЛЬНИХ МОДЕЛЕЙ СТАТИЧНИХ ОБ'ЄКТІВ

Західноукраїнський національний університет, Тернопіль

Анотація. Розглянуто процес побудови математичних моделей статичних об'єктів та систем, що включає розв'язок двох задач: структурну та параметричну ідентифікації. При цьому складнішою та первинною є задача ідентифікації структури моделі. Задача структурної ідентифікації інтервальних моделей характеристики статичного об'єкта є задачею багаторазового розв'язування задач параметричної ідентифікації цієї моделі, а отже з обчислювальної точки зору вона є NP складною. Процедура пошуку оптимальної структури моделі розглядається як напрямлений перебір окресленої множини структур у такий спосіб, щоб мінімізувати кількість ітерацій формування інтервальних систем нелінійних алгебричних рівнянь (ІНАР). У статті сформульовано задачу структурної ідентифікації інтервальних моделей статичних об'єктів, як задачі багаторазового пошуку розв'язків інтервальних систем нелінійних алгебричних рівнянь, у вигляді оптимізаційних задач з нелінійною функцією мети та нелійними обмеженнями. Вперше запропоновано та обґрунтовано метод структурної ідентифікації інтервальних моделей характеристик статичних об'єктів на основі аналізу інтервальних даних, який на відміну від існуючих ґрунтується на процедурах самоорганізації та самоадаптації обчислювальних процедур за аналогією з поведінковими моделями бджолоїної колонії (ПМБК), що дає можливість реалізувати процедури ідентифікації структури моделей з нижчою обчислювальною складністю та отримати інтервальні моделі з простішими структурами у порівнянні із відомими методами. Запропонований метод апробовано на прикладі побудови інтервальної моделі характеристик малої гідроелектростанції з метою дослідження та забезпечення максимальної ефективності використання гідроенергетичних ресурсів, що продемонструвало ефективність використання обчислювальних процедур на основі поведінкових моделей бджолоїної колонії. Відповідно, запропонований метод дає можливість отримувати прості, з точки зору складності, інтервальні моделі складних статичних об'єктів із заданою гарантованою точністю та з нижчою обчислювальною складністю ідентифікації цих моделей. Такі особливості методу, забезпечують ефективний розвиток математичного апарату, який використовуються як в процесах прийняття рішень так і в процесах підготовки рішень у інтелектуалізованих системах, орієнтованих на дані.

Ключові слова: математична модель, інтервальний аналіз, структурна ідентифікація моделей, статичний об'єкт, поведінкова модель бджолоїної колонії (ПМБК).

Abstract. The process of building mathematical models of static objects and systems, which includes the solution of two problems: structural and parametric identification, is considered. At the same time, the task of identifying the structure of the model is more difficult and primary. The problem of structural identification of interval models of the characteristic of a static object is the problem of multiple solving of problems of parametric identification of this model, and therefore, from a computational point of view, it is NP complex. The procedure for finding the optimal structure of the model is considered as a directed selection of a defined set of structures in such a way as to minimize the number of iterations of the formation of interval systems of nonlinear algebraic equations. The article formulates the problem of structural identification of interval models of static objects, as a problem of repeatedly searching for solutions of interval systems of nonlinear algebraic equations, in the form of optimization problems with a nonlinear objective function and nonlinear constraints. For the first time, a method of structural identification of interval models of the characteristics of static objects based on the analysis of interval data is proposed and substantiated, which, unlike the existing ones, is based on self-organization and self-adaptation procedures of computing procedures by analogy with artificial bee colony (ABC), which gives the ability to implement model structure identification procedures with lower computational complexity and obtain interval models with simpler structures compared to known methods. The proposed method was tested on the example of building an interval model of the characteristics of a small hydroelectric plant for the purpose of research and ensuring the maximum efficiency of the use of hydropower resources, which demonstrated the effectiveness of using computational procedures based on the artificial bee colony. Accordingly, the proposed method makes it possible to obtain simple, from the point of view of complexity, interval models of complex static objects with a given guaranteed accuracy and with a lower computational complexity of identifying these models. Such features of the method ensure the effective development of the mathematical apparatus, which is used both in decision-making processes and in the processes of preparing decisions in intellectualized data-oriented systems.

Key words: mathematical model, interval analysis, structural identification of models, static object, artificial bee colony (ABC).

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-103-114>.

Вступ

Сучасні тенденції розвитку інформаційних технологій передбачають використання інтелектуалізованих систем, орієнтованих на дані. Одним із засобів, що забезпечує розвиток таких систем є математичне моделювання, що дає можливість створити ряд математичних моделей, які використовуються як в процесах прийняття рішень так і в процесах підготовки рішень. Існуючі методи побудови таких моделей мають недоліки, оскільки результати спостережень за тим чи іншим об'єктом або процесом є з похибками, які призводять до неточності побудованої моделі. Одним із підходів, який враховує межові значення похибок є теоретико-множинний інтервальний підхід [1], який дає можливість побудувати інтервальні моделі статичних об'єктів з гарантованими прогностичними властивостями. Проте, застосування цього підходу призводить до суттєвого ускладнення методів ідентифікації параметрів моделей у порівнянні із детермінованим чи стохастичним підходами [2-4]. Таким чином, виникає протиріччя, яке полягає – з одного боку у необхідності побудови інтервальних моделей статичних об'єктів з гарантованими прогностичними властивостями, а з іншого боку, це призводить до ускладнення методів ідентифікації цих моделей та у більшості випадків до ускладнення самих моделей.

Актуальність

Процес побудови математичних моделей статичних об'єктів та систем включає розв'язок двох задач: структурну та параметричну ідентифікації [5, 6]. При цьому складнішою та первинною є задача ідентифікації структури моделі, оскільки необхідно спочатку визначити базисні функції, згенерувати структуру моделі, а потім обчислити оцінки параметрів для вибору оптимальної або «кращої». Так, для побудови моделей статичних об'єктів, використовують методи редукції елементів, або нарощування структури. Розроблені алгоритми реалізації, вимагають налаштувань багатьох параметрів алгоритмів, залежно від конкретної задачі. Найбільш ефективні методи структурної ідентифікації інтервальних моделей, побудовані на процедурах самоадаптації та самоорганізації за аналогією з поведінковими моделями бджолиної колонії. Для цього розв'язують складні оптимізаційні задачі. З досвіду використання відомих алгоритмів реалізації методів структурної ідентифікації, можна зробити висновок, що вони достатньо складні з обчислювальної точки зору [3,4]. Також в основі цих методів є обчислювальні процедури параметричної ідентифікації, які побудовані на оцінюванні розв'язків ІСНАР, що також суттєво знижує їх ефективність. Таким чином, актуальною є задача розробки нових методів структурної ідентифікації інтервальних моделей статичних об'єктів, реалізація яких дозволить зменшити кількість складних обчислювальних процедур оцінювання розв'язків ІСНАР.

Мета

Метою статті є розвиток методів структурної ідентифікації інтервальних моделей статичних об'єктів, реалізація яких відрізняється меншою обчислювальних складністю.

Задачі

1. Формалізація задачі структурної ідентифікації інтервальних моделей статичних об'єктів, як задачі багаторазового пошуку розв'язків інтервальних систем нелінійних алгебричних рівнянь (ІСНАР), у вигляді оптимізаційних задач з нелінійною функцією мети та нелінійними обмеженнями;

2. Розробка методу структурної ідентифікації інтервальних моделей характеристик статичних об'єктів на основі аналізу інтервальних даних, який на відміну від існуючих ґрунтується на процедурах самоорганізації та самоадаптації обчислювальних процедур за аналогією з поведінковими моделями бджолиної колонії (ПМБК), реалізація яких дозволить зменшити кількість складних обчислювальних процедур оцінювання розв'язків ІСНАР.

Постановка задачі

Як відомо, задача структурної ідентифікації, полягає у редукції, чи нарощуванні структури інтервальної моделі [7]. Складні об'єкти будемо описувати математичними моделями у вигляді нелінійного алгебричного виразу. Тоді вихідну характеристику y_0 статичного об'єкта будемо знаходити у вигляді нелінійного алгебричного виразу

$$y_0 = \varphi_{m+1}(\vec{g})\varphi_1(\vec{x}) + \dots + \varphi_{2m}(\vec{g})\varphi_m(\vec{x}), \quad (1)$$

де $\varphi_1(\vec{x}), \dots, \varphi_m(\vec{x}), \varphi_{m+1}(g_1), \dots, \varphi_{2m}(g_m)$ – невідомі базисні функції, причому базисні функції $\varphi_{m+1}(g_1), \dots, \varphi_{2m}(g_m)$, стосуються невідомих параметрів моделі $g_i, i = 1, \dots, m$, а результати експерименту отримано в інтервальному вигляді:

$$x_{i1} \cdots x_{in} \longrightarrow [y_i^-, y_i^+], i = 1, \dots, N \quad (2)$$

Спираючись на означений вище вираз для представлення математичної моделі характеристики статичного об'єкта, уведемо поняття множини структурних елементів:

$$\lambda_s = \{\varphi_1^s(\vec{x}), \dots, \varphi_m^s(\vec{x}), \varphi_{m+1}^s(\vec{g}), \dots, \varphi_{2m}^s(\vec{g})\}, \quad (3)$$

де s – означає певний набір структурних елементів, на основі якого будемо s -ту модель у вигляді (1), тобто як згортку цього набору елементів.

В подальшому розгляді, позначення λ_s означатиме s -ту структуру, оскільки усі моделі на основі зазначеного набору, будемо на основі згортки цих елементів.

Для визначення структури λ_s (набору елементів), які забезпечать розробку адекватної моделі характеристики статичного об'єкта, необхідно розв'язувати задачу структурної ідентифікації із застосування результатів експерименту у вигляді інтервальних даних (2)

Математичні моделі, які розглядатимемо в процесі структурної ідентифікації, назвемо моделі-претенденти, а представлення їх структури із урахуванням зазначених вище позначень, матиме такий вигляд:

$$y_0(\lambda_s) = \varphi_{m+1}^s(\vec{g})\varphi_1^s(\vec{x}) + \dots + \varphi_{2m}^s(\vec{g})\varphi_m^s(\vec{x}). \quad (4)$$

Задаємо умови узгодженості моделі-претендента із експериментальними інтервальними даними, як це прийнято в інтервальному аналізі:

$$y_0(\lambda_s, \vec{x}_i) \in [y_i^-; y_i^+], \forall i = 1, \dots, N, \quad (5)$$

де $y_0(\lambda_s, \vec{x}_i)$ – означає істинне значення вихідної характеристики для фіксованого набору структурних елементів λ_s і для фіксованих значень вхідних змінних \vec{x}_i .

Невідомими в цьому випадку залишаються тільки значення параметрів g_1, \dots, g_m моделі. Приймаючи до уваги умови (5) із заміною в них замість $y_0(\lambda_s, \vec{x}_i)$ на вираз (4) для фіксованих значень вхідних змінних \vec{x}_i , отримуємо таку систему:

$$\begin{cases} y_1^- \leq \varphi_{m+1}^s(\vec{g})\varphi_1^s(\vec{x}_1) + \dots + \varphi_{2m}^s(\vec{g})\varphi_m^s(\vec{x}_1) \leq y_1^+; \\ \vdots \\ y_N^- \leq \varphi_{m+1}^s(\vec{g})\varphi_1^s(\vec{x}_N) + \dots + \varphi_{2m}^s(\vec{g})\varphi_m^s(\vec{x}_N) \leq y_N^+. \end{cases} \quad (6)$$

Таким чином, отримали загальну форму задачі параметричної ідентифікації інтервальних моделей статичних об'єктів у вигляді інтервальної системи нелінійних алгебраїчних рівнянь (ІСНАР) для окремої s -тої моделі-претендента. Як відомо, розв'язки цієї системи отримуємо внаслідок реалізації ітераційної процедури, на кожній l -тій ітерації якої, обчислюємо функцію $\delta([\hat{g}_l^-; \hat{g}_l^+])$ «якості» оцінки параметрів математичної моделі. Проте, у випадку структурної ідентифікації, ІСНАР (6) може виявитися несумісною для поточної структури λ_s математичної моделі. Тому в цих випадках, доводиться формувати нову структуру, а на її основі – нову ІСНАР (6) і знову перевіряти сумісність останньої. Отже, задача структурної ідентифікації інтервальних моделей характеристики статичного об'єкта є задачею багаторазового розв'язування задач параметричної ідентифікації цієї моделі. При цьому необхідно забезпечити напрямлений перебір окресленої множини структур у такий спосіб, щоб цей перебір був оптимальним з обчислювальної точки зору.

Припустимо, що на якійсь ітерації напрямленого перебору структур λ_s , ІСНАР (6) виявилась сумісною. Тобто отримано її розв'язок у вигляді деяких інтервалів значень оцінок параметрів $[\hat{g}_1^-; \hat{g}_1^+], \dots, [\hat{g}_m^-; \hat{g}_m^+]$ моделі. Підставимо отримані інтервальні оцінки $[\hat{g}_1^-; \hat{g}_1^+], \dots, [\hat{g}_m^-; \hat{g}_m^+]$ у вираз (4) одночасно із зафіксованими значеннями вхідної змінної \vec{x}_i (у точках експерименту). В результаті цих підстановок, отримуємо оцінки вихідної характеристики у вигляді інтервалів:

$$\begin{aligned} [\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)] &= \varphi_{m+1}^s([\hat{g}_1^-; \hat{g}_1^+])\varphi_1^s(\vec{x}_i) + \dots \\ &+ \varphi_{2m}^s([\hat{g}_l^-; \hat{g}_l^+])\varphi_m^s(\vec{x}_i), \quad i = 1, \dots, N. \end{aligned} \quad (7)$$

Таким чином, сумісність ІСНАР (6) означає належність інтервалів значень $[\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)]$ прогнозованої характеристики у точках експерименту \vec{x}_i , до інтервалів $[y_i^-; y_i^+], i = 1, \dots, N$, отриманих експериментально, тобто за виконання таких умов:

$$[\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)] \subset [y_i^-; y_i^+], \quad i = 1, \dots, N. \quad (8)$$

По аналогії із методом параметричної ідентифікації інтервальних моделей статичних об'єктів, який багаторазово використовується в методі структурної ідентифікації для кожної з фіксованих структур λ_s , можемо стверджувати, що ітераційна процедура для методу формування та оцінювання розв'язків поточної ІСНАР (6) повинна ґрунтуватися на оцінюванні на кожній ітерації «якості» оцінки структури та параметрів математичної моделі, представленій алгебричним виразом (4). Наскільки якісною виявиться оцінка параметрів на кожній l -тій ітерації можемо задати величиною $\delta(\lambda_s)$, по аналогії із задачею параметричної ідентифікації, у вигляді різниці центрів найбільш віддалених між собою прогнозного $[\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)]$ та експериментального інтервалів $[y_i^-; y_i^+]$ – у випадку, коли вони не перетинаються та найменшою шириною перетину серед прогнозних та експериментальних інтервалів – для випадку їх перетину. Вираз для функції $\delta(\lambda_s)$, для вище зазначених обох випадків, представимо у такому вигляді:

$$\delta(\lambda_s) = \max_{i=1, \dots, N} \{ |mid([\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)]) - mid([y_i^-; y_i^+])| \},$$

якщо

$$[\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)] \cap [y_i^-; y_i^+] = \emptyset, \quad \exists i = 1, \dots, N \quad (9)$$

$$\delta(\lambda_s) = \max_{i=1, \dots, N} \{ \text{wid}([\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)]) - \text{wid}([\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)] \cap [y_i^-; y_i^+]) \},$$

якщо

$$[\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)] \cap [y_i^-; y_i^+] \neq \emptyset, \forall i = 1, \dots, N. \quad (10)$$

Очевидною є набагато вища складність розв'язування цієї задачі у порівнянні із задачами параметричної ідентифікації. В цих умовах необхідно розробити новий метод напрямленого перебору, попередньо окресленої множини структур у такий спосіб, щоб цей перебір був оптимальним з обчислювальної точки зору. З іншого боку метод повинен бути орієнтований на розв'язування задач структурної ідентифікації лінійної за параметрами моделі, взамін методів редукції та нарощування структури, так і для загального випадку нелінійної моделі. Такий спільний підхід до розв'язування цих обох задач дасть можливість створити також єдиний інструментарій та спростити процес побудови цих моделей для користувачів-практиків.

Констатуючи той факт, що задача структурної ідентифікації інтервальних моделей характеристики статичного об'єкта є задачею багаторазового розв'язування задач параметричної ідентифікації цієї моделі, а отже з обчислювальної точки зору вона є NP складною, то необхідно розробити процедуру напрямленого перебору окресленої множини структур у такий спосіб, щоб мінімізувати кількість ітерацій формування ІСНАР (6). З цієї метою необхідно математично сформулювати оптимізаційну задачу.

Перепишемо формули (9) та (10) для обчислення значень функції $\delta(\lambda_s)$, яка задає якість поточної структури у розгорнутому вигляді. Для цього підставимо замість інтервалу прогнозованих значень характеристики $[\hat{y}^-(\lambda_s, \vec{x}_i); \hat{y}^+(\lambda_s, \vec{x}_i)]$ у цих формулах, вираз (7), яким обчислюємо зазначений інтервал. Отримаємо:

$$\delta(\lambda_s) = \max_{i=1, \dots, N} \{ \text{mid}(\varphi_{m+1}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_1^s(\vec{x}_i) + \dots + \varphi_{2m}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_m^s(\vec{x}_i)) - \text{mid}([y_i^-; y_i^+]) \}$$

якщо

$$(\varphi_{m+1}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_1^s(\vec{x}_i) + \dots + \varphi_{2m}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_m^s(\vec{x}_i)) \cap [y_i^-; y_i^+] = \emptyset, \exists i = 1, \dots, N \quad (11)$$

$$\delta(\lambda_s) = \max_{i=1, \dots, N} \{ \text{wid}(\varphi_{m+1}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_1^s(\vec{x}_i) + \dots + \varphi_{2m}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_m^s(\vec{x}_i)) - \text{wid}(\varphi_{m+1}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_1^s(\vec{x}_i) + \varphi_{2m}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_m^s(\vec{x}_i)) \cap [y_i^-; y_i^+] \},$$

якщо

$$(\varphi_{m+1}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_1^s(\vec{x}_i) + \dots + \varphi_{2m}^s([\hat{g}_i^-; \hat{g}_i^+])\varphi_m^s(\vec{x}_i)) \cap [y_i^-; y_i^+] \neq \emptyset, \forall i = 1, \dots, N \quad (12)$$

Тепер важливим питанням залишається, як оптимальним чином організувати ітераційну процедуру обчислення послідовності структур $\lambda_{s=1}, \lambda_{s=2}, \dots, \lambda_s, \dots$ у такий спосіб, щоб забезпечити таку послідовність оцінювання значень функції, яка визначає їх якість $\delta(\lambda_{s=1}), \delta(\lambda_{s=2}), \dots, \delta(\lambda_s), \dots$, обчислених за виразами (11), або (12), яка призводить до виконання таких умов:

$$\delta(\lambda_{s=1}) > \delta(\lambda_{s=2}) > \dots > \delta(\lambda_s), \dots, \delta(\lambda_{s=s_{opt}}) = \delta([\hat{g}_{l=L}^-; \hat{g}_{l=L}^+] \subset \Omega), \quad (13)$$

де s_{opt} – номер структури, для якої сформовано сумісну ІСНАР (6), Ω – область розв'язків цієї ІСНАР.

Відповідно, постає задача організації даної ітераційної процедури для обчислення послідовності структур $\lambda_{s=1}, \lambda_{s=2}, \dots, \lambda_s, \dots$.

Спираючись на викладене вище, задачу структурної ідентифікації інтервальних моделей статичного об'єкта сформулюємо у вигляді оптимізаційної задачі:

$$\delta(\lambda_s) \xrightarrow{\lambda_s = \{\varphi_1^s(\vec{x}), \dots, \varphi_m^s(\vec{x}), \varphi_{m+1}^s(\hat{g}), \dots, \varphi_{2m}^s(\hat{g})\}, [\hat{g}_i^-; \hat{g}_i^+]} \min, \quad (14)$$

$$m_s \in [I_{min}; I_{max}],$$

$$\varphi_1(\vec{x}), \dots, \varphi_m(\vec{x}), \varphi_{m+1}(\hat{g}), \dots, \varphi_{2m}(\hat{g}) \in F, \quad (15)$$

$$[\hat{g}_{jl}^-; \hat{g}_{jl}^+] \subset [g_{jl}^{low}; g_{jl}^{up}],$$

$$j = 1, \dots, m, l = 1, \dots, S,$$

де $m_s \in [I_{min}; I_{max}]$ – кількість структурних елементів s -ї структури інтервальної моделі, $F = \{\varphi_1(\vec{x}), \dots, \varphi_m(\vec{x}), \varphi_{m+1}(\hat{g}), \dots, \varphi_{2m}(\hat{g})\}$ – множина потенційних структурних елементів моделі, $[\hat{g}_i^-; \hat{g}_i^+]$, $[\hat{g}_{jl}^-; \hat{g}_{jl}^+]$ – інтервальный вектор параметрів s -ї структури моделі-претендента та його компоненти, відповідно, g_{jl}^{low} , g_{jl}^{up} – найменше та найбільше значення для кожного параметра моделі.

Тоді, чим менше значення $\delta(\lambda_s)$, тим «краща» поточна структура інтервальної моделі. Якщо ж виконується рівність $\delta(\lambda_s) = 0$, то поточна структура дозволяє побудувати адекватну інтервальну модель статичного об'єкта, для якої умови (8) виконуються на множині усіх спостережень $i = 1, \dots, N$.

Метод структурної ідентифікації інтервальних моделей статичних об'єктів на основі поведінкових моделей бджолоїної колонії (ПМБК)

ПМБК є одним із найефективніших інструментів організації розв'язування складних оптимізаційних задач за рахунок елементів самоорганізації та адаптації. Тому цей підхід використано для побудови методу структурної ідентифікації інтервальних моделей статичних та динамічних об'єктів. Алгоритм штучної бджолоїної колонії (АБК), який є формальним представленням поведінкової моделі однойменної колонії, є евристичним алгоритмом, який ґрунтується на принципах ройового інтелекту. Його схема реалізації полягає у відображенні поведінки колонії медоносних бджіл у процесі пошуку нектару [8-13].

При розгляді методу розв'язування оптимізаційної задачі (14), (15), встановимо аналогії між компонентами поведінкової моделі і поняттями, які використаємо при розробці методу структурної ідентифікації математичних моделей статичних об'єктів.

Зокрема:

- поведінка бджоли при виборі місцезнаходження джерела нектару – реалізує спосіб синтезу поточної структури моделі;
 - область пошуку нектару – означає множину усіх можливих структур моделей;
 - окіл джерела нектару – означає набір структур, що можуть бути згенеровані на основі поточної, шляхом заміни її окремих структурних елементів;
 - місцезнаходження джерела нектару – означає поточну структуру моделі λ_s ;
 - якість джерела нектару представлено значенням функції мети $\delta(\lambda_s)$ задачі (14).
- Тепер розглянемо основні фази методу структурної ідентифікації на основі ПМБК.

Фаза ініціалізації.

На цій фазі задаємо основні параметри методу: $LIMIT, S, [I_{min}; I_{max}]$, $m_{сп} = 0$ – поточний номер ітерації; MCN – загальна кількість ітерацій та множину структурних елементів F , а також випадковим чином формуємо початкову множину Λ_0 (з потужністю S) структур λ_s із набору структурних елементів F .

Фаза робочих бджіл.

Для зручності оперування структурними елементами, множину всіх структурних елементів $F = \{\varphi_1(\vec{x}), \dots, \varphi_m(\vec{x}), \varphi_{m+1}(\hat{g}), \dots, \varphi_{2m}(\hat{g})\}$ – пронумеруємо за допомогою десяткових чисел. Кодування структурних елементів показано в табл. 1.

Таким чином, кожному структурному елементу із множини F можна поставити у відповідність його десятковий код, представлений порядковим номером у таблиці 1. Для обчислювальних процедур поточної структури λ_s представимо у вигляді набору $\{N_1, N_2, \dots, N_{m_s}\}$, де N – номер структурного елемента із табл. 1.

Таблиця 1 – Кодування структурних елементів

№	Структурний елемент
1	$\varphi_1(\vec{x})$
2	$\varphi_2(\vec{x})$
...	...
m	$\varphi_m(\vec{x})$
m+1	$\varphi_{m+1}(\vec{g})$
...	...
2m	$\varphi_{2m}(\vec{g})$

Далі, для формування структур розглянемо ряд операторів. Отже, на фазі робочих бджіл використовуємо оператор $P(A_{mcn}, F)$, який здійснює перетворення структури інтервальної моделі у вигляді (4), відповідно до процедури дослідження робочими бджолами околу відомого джерела нектару. Відповідно, на поточній ітерації реалізації методу структурної ідентифікації, оператор P на основі кожної з поточних структур λ_s математичної моделі формує по одній «новій» структурі λ'_s , яка є «околом». Це означає, що сформована структура λ'_s дуже близька до поточної λ_s .

Таким чином, оператор $P(A_{mcn}, F)$ здійснює перетворення множини A_{mcn} поточних структур λ_s , згенерованих на m -тій ітерації у множину A'_{mcn} структур λ'_s . При цьому, «нову» структуру λ'_s для кожної поточної формуємо у спосіб випадкового вибору та заміни частини елементів поточної структури λ_s . При цьому, заміну проводимо також випадково обраними елементами із множини, на вибрані із множини $F = \{\varphi_1(\vec{x}), \dots, \varphi_m(\vec{x}), \varphi_{m+1}(\vec{g}), \dots, \varphi_{2m}(\vec{g})\}$. Тут важливим питанням є: скільки елементів у поточній структурі необхідно замінити? Для цього вводимо змінну цілого типу n_s , значення якої визначає кількість елементів у поточній структурі λ_s , яку необхідно замінити. Значення цієї змінної залежить від значення функції мети $\delta(\lambda_s)$ у задачі (14), (15), яке, своєю чергою, обчислюємо за формулами (11) чи (12). Чим більше це значення $\delta(\lambda_s)$ – тим гірша поточна структура λ_s , отже тим більше елементів потрібно в ній замінити. При обчисленні значення змінної n_s необхідно також враховувати загальну кількість елементів у поточній структурі, яка, як відомо з постановки оптимізаційної задачі (14), (15), може бути різною для різних структур, але задана в межах інтервалу $m_s \in [I_{min}; I_{max}]$. Тому, при обчисленні кількості елементів n_s , які необхідно замінити в поточній структурі, слід враховувати як якість $\delta(\lambda_s)$ поточної структури λ_s , так і кількість її елементів m_s .

З урахуванням вище зазначеного, змінну n_s можемо обчислювати за такою формулою:

$$n_s = \begin{cases} \text{int} \left(\left(1 - \frac{\min\{\delta(\lambda_s) | s=1 \dots S\}}{\delta(\lambda_s)} \right) \cdot m_s \right), \\ \text{if } \delta(\lambda_s) \neq \min\{\delta(\lambda_s) | s = 1 \dots S\} \\ \text{and } n_s \neq 0; \\ 1, \text{ if } \delta(\lambda_s) = \min\{\delta(\lambda_s) | s = 1 \dots S\} \\ \text{or } n_s = 0. \end{cases} \quad (16)$$

Детальніше обґрунтування формули (16), наведено у праці [9]. Хоча, запропонований вираз вимагає також додаткових досліджень з точки зору впливу отриманих з нього значень на часову складність реалізації методу структурної ідентифікації.

На цій же фазі проводимо попарну селекцію, для вибору кращої структури з поточної та згенерованої. Для цього використовуємо оператор попарної селекції «кращої» із пари структур λ_s, λ'_s :

$$D_1(\lambda_s, \lambda'_s): \lambda_s^1 = \begin{cases} \lambda_s, \text{ if } \delta(\lambda_s) \leq \delta(\lambda'_s) \\ \lambda', \text{ if } \delta(\lambda_s) > \delta(\lambda'_s) \end{cases} \quad (17)$$

Оператор $D_1(\lambda_s, \lambda'_s)$ реалізує процес синтезу множини «кращих» структур A^1_{mcn} із поточних множин A_{mcn}, A'_{mcn} . Таким чином, отримуємо множину структур першого ряду формування $\lambda_s^1 \in A^1_{mcn}$.

Фаза бджіл дослідників.

Бджоли-дослідники обирають (за ймовірністю) нові джерела нектару в околі поточних. В контексті задачі структурної ідентифікації це означає визначення кількості структур, які будуть згенеровані на ос-

нові λ_s^1 структури λ_s^1 із множини A_{mcn}^1 , відповідно до процедури вибору відомого джерела нектару бджолами-дослідниками. Зазначений показник R_s у контексті ПМБК означає кількість бджіл-дослідників, які обрали відоме джерело-нектару з координатами λ_s^1 . Його значення обчислюватимемо на основі такого припущення: кількість бджіл-дослідників, що летить в окіл джерела нектару, про яке повідомила робоча бджола, прямо пропорційно залежить від його якості.

Багаточисленні прикладні дослідження показали, що для обчислення значення R_s доцільно використати ймовірнісний підхід. Він базується на обчисленні ймовірності вибору бджолами-дослідниками певного джерела нектару із врахуванням специфіки оптимізаційної задачі (14), (15). У цьому випадку пропонуємо використати формулу, яка ґрунтується на обчисленні для кожного поточного джерела нектару ймовірності того, що група бджіл-дослідників обере саме окіл s -того джерела нектару.

Отже, для обчислення ймовірної кількості новосформованих структур моделі на основі поточної множини відомих будемо використовувати запропоновану формулу:

$$P_s(\lambda_s^1) = \frac{1 - \delta(\lambda_s^1)}{\sum_{s=1}^S (1 - \delta(\lambda_s^1))}, s = 1 \dots S. \quad (18)$$

Тепер, на основі формули (18) отримаємо точні значення кількості новосформованих структур для кожної поточної структури із множини A_{mcn}^1 за такою формулою:

$$R_s = \text{ToInt}(P_s(\lambda_s^1) \cdot S), s = 1 \dots S. \quad (19)$$

Тепер, зупинимося детальніше на другому підході до обчислення значень змінної R_s . Він ґрунтується на основі класичних виразів для обчислення ймовірності того, що група бджіл-дослідників обере відоме джерело нектару, запропонованих у працях D. Karaboga [10, 11], але є дещо модифікованими з урахуванням особливостей саме оптимізаційної задачі структурної ідентифікації (14), (15).

Обчислювати ймовірність $P_s(\lambda_s^1)$ синтезу на основі поточної структури S новосформованих будемо таким чином:

$$P_s(\lambda_s^1) = \frac{1}{\delta(\lambda_s^1) \cdot \sum_{s=1}^S \frac{1}{\delta(\lambda_s^1)}}, s = 1 \dots S - 1. \quad (20)$$

Далі знаходимо точні значення кількості «нових» структур моделей, які потрібно сформувати на основі кожної поточної (відомої) структури за такою формулою:

$$R_s = \text{ToInt}(P_{s-1}(\lambda_{s-1}^1) \cdot S), s = 2 \dots S, R_1 = 0. \quad (21)$$

На цій фазі також використаємо оператор $P_\delta(A_{mcn}, F)$, який здійснює перетворення структури відповідно до процедури дослідження околу відомого джерела нектару бджолами-дослідниками, подібно як на фазі робочих бджіл. Тільки на відміну від зазначеної фази, де формувалася одна структура в околі поточної, в цьому випадку кількість структур навколо поточної визначається виразом (19) чи (21) (в залежності від використання для розрахунку формули (18) чи (20), відповідно).

Отже, оператор $P(A_{mcn}, F)$ означає перетворення кожної структури λ_s^1 з множини структур $\lambda_s^1 \in A_{mcn}^1$ першого ряду формування, згенерованих на ітерації алгоритму mcp , у множини структур A'_s . При цьому, по аналогії із фазою робочих бджіл, «нові» структури λ'_s (як зазначено вище, в цьому випадку кількість «нових» структур для поточної структури обчислюємо за формулами (19) чи (21)) для кожної поточної λ_s^1 формуємо у спосіб випадкового вибору та заміни частини елементів поточної структури λ_s^1 . При цьому, заміну проводимо також випадково обраними елементами із множини F . Кількість елементів для кожної структури, які потрібно замінити, визначаємо за формулою (16).

Далі на цій фазі проводимо групову селекцію $D_2(\lambda_s^1, A'_s)$ «кращої» структури із поточної λ_s^1 та сформованої в її околі множини $A'_s = \{\lambda_1, \dots, \lambda_r, \dots, \lambda_{R_s}\}$ за значеннями функції мети. Оператор групової селекції $D_2(\lambda_s^1, A'_s)$ реалізує процес синтезу множини «кращих» структур A_{mcn}^2 із поточних множин A_{mcn}^1 та A'_{mcn} у спосіб селекції структур λ_s^2 за показниками якості, де $A'_{mcn} = \{A'_1 \cup A'_2 \dots \cup \dots A'_s \dots \cup A'_S\}$. Таким чином отримуємо множини структур другого ряду формування A_{mcn}^2 .

Для виходу із локальних мінімумів функції мети задачі (14), (15) запропоновано використовувати фазу бджіл розвідників.

Фаза бджіл розвідників.

Це фаза бджіл, які обирають нові джерела нектару випадковим чином, тобто це означає, що на цій фазі необхідно випадковим чином сформувати нові структури у спосіб, описаний на фазі ініціалізації. Для цього для кожної поточної структури λ_s введемо лічильник Limits, який в контексті ПМБК моделює процес зменшення кількості нектару відповідно до процедури виявлення вичерпаних джерел нектару.

Для розв'язування задачі виходу із локальних мінімумів функції мети оптимізаційної задачі (14), (15), значення лічильника Limits збільшуємо на «1» кожного разу, якщо під час парної чи групової селекції поточна структура не «оновилася», та обнуляємо – в іншому випадку. Збільшення значення лічильника Limits імітує процес вичерпування джерела нектару. Водночас використаємо критерій, який дозволяє виявляти вичерпані джерела нектару. Для цього введено константу LIMIT, значення якої дослідник задає як один із параметрів методу структурної ідентифікації перед його застосуванням. Таким чином, кожна структура λ_s^2 моделі другого ряду формування, для якої виконується умова $Limits \geq LIMIT$, вважатиметься локальним мінімумом.

У такому випадку використовуємо оператор $P_N(F, I_{min}, I_{max})$, який випадковим чином генерує «нову» структуру λ_s^2 з множини F всіх структурних елементів, де кількість структурних елементів для цієї структури визначається випадково на інтервалі $m_s \in [I_{min}; I_{max}]$ відповідно до процедури випадкового пошуку нового джерела нектару. Оператор $P_N(F, I_{min}, I_{max})$ означає генерування випадковим чином структури λ_s^2 із множини усіх структурних елементів. Варто зазначити, що при формуванні «нової» структури ІДМ оператором $P_N(F, I_{min}, I_{max})$ йому будуть доступні всі структурні елементи із множини F.

Варто зазначити, що таких структур, згенерованих на цій фазі, є усього декілька відсотків від значення S (усіх робочих бджіл).

Варто зазначити, що використання розроблених операторів перетворень забезпечує ряд переваг, у порівнянні з алгоритмами ройового інтелекту чи генетичними алгоритмами. Зокрема, таблиця усіх структурних елементів є початково сформована і її використовуємо на кожній ітерації перетворення поточних структур моделей. Очевидно, що потужність сформованої початково множини структурних елементів не впливає на обчислювальну складність реалізації методу. З іншого боку, постійне використання (на кожній ітерації перетворення структур) таблиці структурних елементів знижує ризик втрати значущих елементів структури математичної моделі в процесі виконання операторів парної чи групової селекції, відповідно.

Якщо ж порівнювати запропонований алгоритм синтезу структури із алгоритмами на основі генетичних алгоритмів, то в запропонованому алгоритмі формування «нових» варіантів структур інтервальних моделей здійснюється на основі однієї структури із заміною або частковою заміною її компонентів, що не вимагає розробки та реалізації складних та нестандартних операторів для «схрещування» двох структур. Це у цілому спрощує реалізацію методу структурної ідентифікації.

Ймовірнісний підхід до розподілу кількості «нових» структур, на фазі активності бджіл-дослідників означає, що для структур, функції мети яких характеризуються найменшими значеннями, ймовірніше, що дослідження проводяться інтенсивніше, оскільки існує достатньо велика ймовірність, що ці ділянки містять структури близькі до оптимальних чи можливо і оптимальні. Такий механізм дає можливість швидше знайти розв'язок у вигляді оптимальної структури, або встановити факт зациклення процедури пошуку оптимальної структури на структурі, яка є локальним мінімумом функції мети.

Також застосування критерію «вичерпаності» дозволяє не тільки встановлювати факт зациклення процедури пошуку оптимальної структури на структурі, яка є локальним мінімумом функції мети, але і використовувати механізм на фазі бджіл-розвідників виходу із локального мінімуму, тобто здійснювати перехід на абсолютно іншу структуру.

Варто також відзначити, що у порівнянні із алгоритмами структурної ідентифікації на основі генетичних алгоритмів, а також у порівнянні із існуючими методами на основі ПМБК, формальні перетворення структур в запропонованому методі, націлені на більш «глибоке» перетворення структур інтервальних моделей статичних об'єктів з одночасним зменшенням кількості оцінювань значень функції мети. Це дає можливість зменшити кількість складних обчислювальних процедур оцінювання розв'язків ІСНАР. Разом з тим, поєднання запропонованого методу із ефективними методами параметричної ідентифікації інтервальних моделей дає можливість підсилити вираш щодо зниження обчислювальної складності і спрощення процедур побудови зазначених моделей.

Приклад застосування

Для апробації запропонованого методу застосуємо його для ідентифікації математичної моделі характеристик гідроелектростанції з метою дослідження та забезпечення максимальної ефективності використання гідроенергетичних ресурсів. За приклад таких досліджень обрано МГЕС «Топольки», яку побудовано на річці Стрипа в Тернопільській області. Зазначена МГЕС має дві турбіни, які з'єднано з генераторами з потужністю 70 та 90 кВт. Робота генераторів в системі вимагає постійної оцінки стану характеристик гідроресурсів та прогнозування можливої генерованої електроенергії з метою заощадливого використання обладнання станції. Зокрема, необхідним є прогнозування кожен раз при зміні погодних умов та сезонних коливань наявних гідроресурсів, з метою прийняття рішень про доцільність використання двох турбін одночасно, або використання однієї з двох турбін є доцільним. В такому випадку, одну із турбін можемо виводити на ремонт. Таким чином, виникає необхідність розробки та використання моделі, яка пов'яже кількість потенційно можливої згенерованої електроенергії в залежності від характеристик гідротехнічного обладнання та наявних гідроресурсів.

Спираючись на попередні праці [14, 15], в яких досліджувалися характеристики зазначеної МГЕС, модель генерованої електроенергії МГЕС подаємо у вигляді (1), де y_0 в даному випадку означає обсяг генерованої електроенергії за добу, вектор $\vec{x} = (x_1, x_2, x_3)$ складається з трьох компонент: x_1 – реактивна потужність, x_2 – напір води, x_3 – рівень води на гідростаті.

У результаті досліджень цієї МГЕС отримано таблицю експериментальних даних [14]. Як бачимо з таблиці, кількість виробленої за добу електроенергії представлено в інтервальному вигляді внаслідок похибок оцінювання цієї величини технічними засобами.

Таблиця 2 – Узагальнені дані кількості згенерованої електроенергії МГЕС та факторів впливу на її генерування

№	Реактивна потужність, ВАр	Напір (різниця б'єфів), м	Рівень води на гідростаті, м	Вироблена електроенергія, кВт
	x_1	x_2	x_3	$[y_i^-; y_i^+]$
1	182,5	4,6	6,5	[1087,2;1211,28]
2	182,7	4,7	5,5	[1069,08;1191,092]
3	182,7	4,7	4,97	[1069,08;1191,092]
4	182,7	4,7	5,45	[1087,2;1211,28]
5	182,9	4,7	7,5	[1069,08;1191,092]
6	183	4,7	11,9	[1087,2; 1211,28]
7	183,1	4,7	12,5	[1105,32;1231,468]
8	183,1	4,7	9,8	[1123,44;1251,656]
9	183,1	4,55	10,4	[1087,2;1211,28]
10	183,1	4,6	13,7	[1141,56;1271,844]
11	184,6	4,6	14,9	[1159,68; 1292,032]
12	184,6	4,6	14	[1159,68; 1292,032]
13	184,6	4,7	12,8	[1159,68; 1292,032]
14	184,7	4,65	12,5	[1141,56; 1271,844]
15	184,8	4,6	11,6	[1159,68; 1292,032]
16	184,8	4,7	10,4	[1159,68; 1292,032]
17	184,8	4,7	10,1	[1177,8; 1312,22]
18	184,8	4,8	7,3	[1050,96; 1170,904]
19	187,2	4,8	7,5	[1087,2; 1211,28]
20	187,2	4,7	7,1	[1105,32;1231,468]
21	187,2	4,8	7,3	[1105,32;1231,468]
22	187,2	4,75	8,3	[1087,2;1211,28]
23	187,2	4,7	8,3	[1069,08;1191,092]
24	189,1	4,6	7,24	[1050,96;1170,904]
25	189,1	4,7	5,74	[1105,32;1231,468]
26	189,2	4,7	4,64	[1014,72;1130,528]
27	189,4	4,6	4,78	[1032,84;1150,716]
28	189,4	4,8	5,74	[1105,32;1231,468]
29	189,4	4,8	4,11	[1014,72;1130,528]
30	189,5	4,75	5,01	[1105,32;1231,468]

Спираючись на умову (5), де i означатиме номер доби, під час яких робилися виміри, отримаємо ІСНАР у вигляді (6). Для оцінювання розв'язків цієї ІСНАР використаємо метод параметричної ідентифікації, який наведено в праці [9], а для визначення структури математичної моделі запропонований метод структурної ідентифікації.

Сформовані набори структурних елементів на основі базисних функцій, подано в табл. 3. При цьому взято до уваги попередні дослідження щодо цієї моделі.

Із використанням методу структурної ідентифікації отримуємо таку інтервальну модель щодобової генерованої електроенергії:

$$[\hat{y}^-(\vec{x}); \hat{y}^+(\vec{x})] = [\hat{g}_0] + [\hat{g}_1] \cdot x_1 \cdot x_3 + [\hat{g}_2^2] \cdot x_3 \quad (22)$$

де $[g_0] = [1083,431; 1086,137]$, $[g_1] = [0,048; 0,054]$, $[g_2] = [-0,217; -0,242]$.

Таблиця 3 – Множина усіх потенційних структурних елементів для моделі характеристики МГЕС

№	Структурний елемент	№	Структурний елемент
1	x_1	12	$x_3^2 x_2$
2	x_2	13	$x_3^2 x_1$
3	$x_1 x_2$	14	$x_3 x_1^2$
4	x_1^2	15	$x_3^2 x_2^2$
5	x_2^2	16	$x_3^2 x_1^2$
6	x_3^2	17	$\sin x_3$
7	$x_1 x_3$	18	$\sin x_3 x_2$
8	$x_2 x_3$	19	$\sin x_3 x_1$
9	$x_1^2 x_2$	20	$\sin x_1 x_2$
10	$x_1 x_2^2$	21	g_i
11	$x_3 x_2^2$	22	g_i^2

На рис. 1 також показано результати вимірювань. Як бачимо на цьому рисунку отримана модель прогнозує добову кількість виробленої електроенергії в межах виміряної величини, що підтверджує її адекватність.

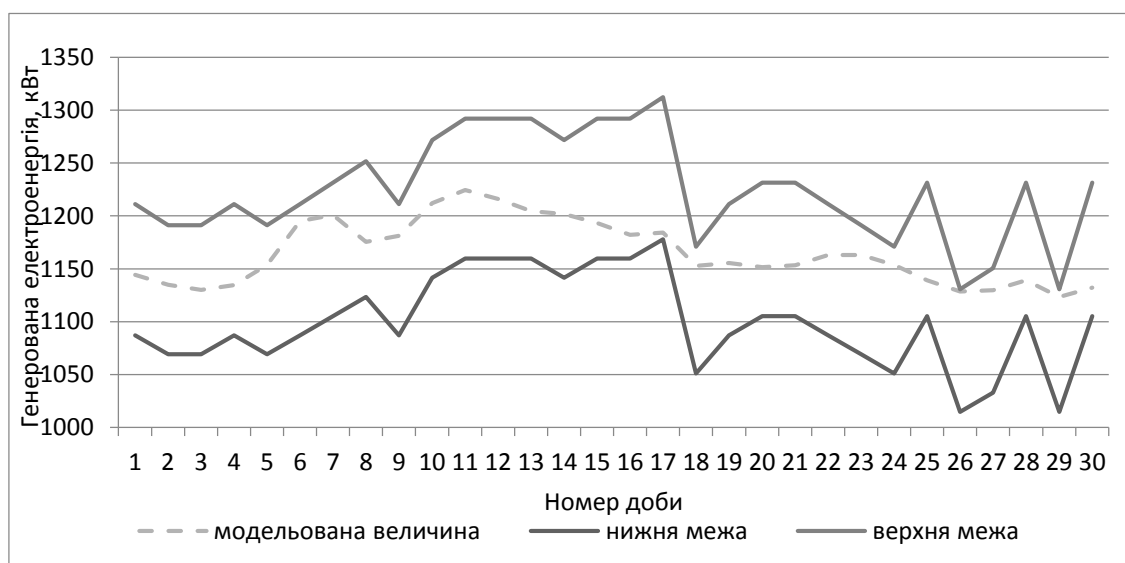


Рисунок 3 – Виміряні та прогнозовані результати добового генерування електроенергії МГЕС «Топольки»

В той час, як у праці [15] отримано таку інтервальну модель:

$$[\hat{y}(\vec{x})] = [5,5996; 5,6001] \cdot x_1 + [0,0937; 0,0941] \cdot x_1 x_3 + \\ + [-5,7855; -5,7851] \cdot \sin(x_3) + [-0,0077; -0,0073] \cdot x_1 x_2^2$$

Як бачимо, отримана модель (22) є простішою, з точки зору її використання, оскільки містить меншу кількість структурних елементів та має гарантовані прогностичні властивості. Запропонований метод дає можливість отримувати прості з точки зору складності інтервальні моделі складних статичних об'єктів із заданою гарантованою точністю. Такі особливості методу, забезпечують ефективний розвиток математичного апарату, який використовується як в процесах прийняття рішень так і в процесах підготовки рішень у інтелектуалізованих систем, орієнтованих на дані.

Висновки

1. На основі теоретичних обґрунтувань нами сформульовано задачу структурної ідентифікації інтервального моделі статичних об'єктів, як задачі багаторазового пошуку розв'язків ІСНАР, у вигляді оптимізаційної задачі з нелінійною функцією мети та нелінійними обмеженнями.

2. Вперше запропоновано та обґрунтовано метод структурної ідентифікації інтервального моделі характеристик статичних об'єктів на основі аналізу інтервального даних, який на відміну від існуючих ґрунтується на процедурах самоорганізації та самоадаптації обчислювальних процедур за аналогією з поведінковими моделями бджолоїної колонії, що дає можливість реалізувати процедури ідентифікації структури моделі з нижчою обчислювальною складністю та отримати інтервальні моделі з простішими структурами у порівнянні із відомими методами.

3. Запропонований метод апробовано на прикладі побудови інтервальної моделі характеристик малої гідроелектростанції, що продемонструвало ефективність використання обчислювальних процедур на основі поведінкового моделювання бджолоїної колонії, оскільки спрощує процес побудови моделі та забезпечує отримання інтервального моделі із мінімальною складністю за кількістю параметрів та складністю структурних елементів.

Список літератури

- [1] G. Alefeld, G. Mayer, "Interval analysis: theory and applications", *Journal of Computational and Applied Mathematics*, № 121, pp. 421-464. 2000.
- [2] А. Г. Ивахненко, *Индуктивный метод самоорганизации моделей сложных систем*, Київ: Наукова думка, 1981, 296 с.
- [3] V. Stepashko, O. Moroz, "Hybrid searching GMDH-GA algorithm for solving inductive modeling task", *Proceedings of the First Int. Conf. on Data Stream Mining & Processing (DSMP'2016)*, pp. 350-355. 2016.
- [4] В. С. Степашко, *Елементи теорії індуктивного моделювання. Стан та перспективи розвитку інформатики в Україні: монографія, Кол. Авторів*. Київ, Україна: Наукова думка, 2010, с. 481-496.
- [5] М. П. Дивак, *Задачі математичного моделювання статичних систем з інтервальними даними*. Тернопіль, Україна: Видавництво ТНЕУ «Економічна думка», 2011, 216 с.
- [6] М. П. Дивак, А. В. Пукас, "Концепція побудови міждисциплінарних математичних моделей системних характеристик складних об'єктів в умовах інтервальної невизначеності", *Вимірювальна та обчислювальна техніка в технологічних процесах: Матеріали XIV міжнародної науково-технічної конференції "ВОТТП-14-2015"*, Одеса, 2015, с. 23-25.
- [7] M. Dyvak, V. Manzhula, A. Pukas, P. Stakhiv, "Structural identification of interval models of the static systems", *International Workshop on Inductive Modelling: Proceedings of the 2nd International Workshop*. Prague, Czech Republic, 2007, pp. 172-179.
- [8] S. Camazine, J. Sneyd, "ABCA A model of collective nectar source by honey bees: Self-organization through simple rules", *Journal of Theoretical Biology*, № 149, pp. 547-571, 1991.
- [9] М. П. Дивак, Н. П. Порплиця, Т. М. Дивак, *Ідентифікація дискретних моделей динамічних систем з інтервальними даними: монографія*. Тернопіль, Україна: ВПЦ «Економічна думка ТНЕУ», 2018, 220 с.
- [10] D. Karaboga, *An idea based on honey bee swarm for numerical optimization: Techn. Rep*, TR06, Erciyes: Erciyes Univ. Press, 2005, 10 p.
- [11] D. Karaboga, B. Basturk, "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm", *Journal of Global Optimization*, 2007, vol. 39, pp. 459-471.
- [12] M. Dyvak, N. Porplytsya, Y. Maslyiak, N. Kasatkina, "Modified artificial bee colony algorithm for structure identification of models of objects with distributed parameters and control", *Proc. Of the 14th Intern. Conf. on Experience of Designing and Application of CAD Systems in Microelectronics (CADSM'2017)*, 2017, pp. 50-54.
- [13] N. Porplytsya, M. Dyvak, T. Dyvak, "Method of structure identification for interval difference operator based on the principles of honey bee colony functioning", *Computational Problems of Electrical Engineering*, vol. 4, №2, pp. 57-68, 2014.
- [14] М. П. Дивак, Ю. П. Франко, "Оцінка можливостей МГЕС «Топольки» методами аналізу інтервального даних", *Збірник наукових праць ДонНТУ серії «Інформатика, кібернетика і обчислювальна техніка»*, вип. 10(153), с. 274-278. 2011.
- [15] M. Dyvak, I. Oliynyk, A. Pukas, V. Manzhula, "Interval model for description the small hydroelectric power station and method of its construction", *Computational Problems of Electrical Engineering: Proceedings of abstracts of the 15th International Conference 'CPEE'2014'*, Terchova-Vratna Dolina, Slovak Republic, 2014, p. 38.

Стаття надійшла: 21.05.2022.

References

- [1] G. Alefeld, G. Mayer, "Interval analysis: theory and applications", *Journal of Computational and Applied Mathematics*, № 121, pp. 421-464. 2000.
- [2] А. Н. Yvakhnenko, *Induktivnyj metod samoorganizacii modelej slozhnyh sistem*, Kyiv: Naukova dumka, 1981, 296 s. [in Russian].
- [3] V. Stepashko, O. Moroz, "Hybrid searching GMDH-GA algorithm for solving inductive modeling task", *Proceedings of the First Int. Conf. on Data Stream Mining & Processing (DSMP'2016)*, pp. 350-355. 2016.
- [4] V. S. Stepashko, *Elementy teorii induktivnoho modeliuвання. Stan ta perspektyvy rozvytku informatyky v Ukraini: monohrafiia, Kol. Avtoriv*. Kyiv, Ukraina: Naukova dumka, 2010, s. 481-496 [in Ukrainian].
- [5] M. P. Dyvak, *Zadachi matematychnoho modeliuвання statychnykh system z intervalnymy danymy*. Ternopil, Ukraina: Vydavnytstvo TNEU «Ekonomichna dumka», 2011, 216 s. [in Ukrainian].
- [6] M. P. Dyvak, A. V. Pukas, "Kontseptsiiia pobudovy mizhdystyplinarnykh matematychnykh modelei sys-temnykh kharakterystyk skladnykh ob'iektiv v umovakh intervalnoi nevyznachenosti", *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh: Materialy KhIV mizhnarodnoi nauko-vo-tekhnichnoi konferentsii "VOTTP-14-2015"*, Odesa, 2015, s. 23-25 [in Ukrainian].
- [7] M. Dyvak, V. Manzhula, A. Pukas, P. Stakhiv, "Structural identification of interval models of the static systems", *International Workshop on Inductive Modelling: Proceedings of the 2nd International Workshop*. Prague, Czech Republic, 2007, pp. 172-179.
- [8] S. Camazine, J. Sneyd, "ABCA A model of collective nectar source by honey bees: Self-organization through simple rules", *Journal of Theoretical Biology*, № 149, pp. 547-571, 1991.
- [9] M. P. Dyvak, N. P. Porplytsia, T. M. Dyvak, *Identyfikatsiia dyskretnykh modelei dynamichnykh system z intervalnymy danymy: monohrafiia*. Ternopil, Ukraina: VPTs «Ekonomichna dumka TNEU», 2018, 220 s. [in Ukrainian].
- [10] D. Karaboga, *An idea based on honey bee swarm for numerical optimization: Techn. Rep*, TR06, Erciyes: Erciyes Univ. Press, 2005, 10 p.
- [11] D. Karaboga, B. Basturk, "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm", *Journal of Global Optimization*, 2007, vol. 39, pp. 459-471.
- [12] M. Dyvak, N. Porplytsya, Y. Maslyiak, N. Kasatkina, "Modified artificial bee colony algorithm for structure identification of models of objects with distributed parameters and control", *Proc. Of the 14th Intern. Conf. on Experience of Designing and Application of CAD Systems in Microelectronics (CADSM'2017)*, 2017, pp. 50-54.
- [13] N. Porplytsya, M. Dyvak, T. Dyvak, "Method of structure identification for interval difference operator based on the principles of honey bee colony functioning", *Computational Problems of Electrical Engineering*, vol. 4, №2, pp. 57-68, 2014.
- [14] M. P. Dyvak, Yu. P. Franko, "Otsinka mozhlyvostei MHES «Topolky» metodamy analizu intervalnykh danykh", *Zbirnyk naukovykh prats DonNTU serii «Informatyka, kibernetyka i obchysliuvalna tekhnika»*, vyp. 10(153), s. 274-278. 2011 [in Ukrainian].
- [15] M. Dyvak, I. Oliynyk, A. Pukas, V. Manzhula, "Interval model for description the small hydroelectric power station and method of its construction", *Computational Problems of Electrical Engineering: Proceedings of abstracts of the 15th International Conference 'CPEE'2014*, Terchova-Vratna Dolina, Slovak Republic, 2014, p. 38.

Відомості про авторів

Дивак Микола Петрович – доктор технічних наук, професор, декан факультету комп'ютерних інформаційних технологій.

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

Мельник Андрій Миколайович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук.

Пукас Андрій Васильович – доктор технічних наук, доцент, завідувач кафедри комп'ютерних наук.

M. P. Dyvak, V. I. Manzhula, A. M. Melnyk, A. V. Pukas

METHOD OF STRUCTURAL IDENTIFICATION OF NONLINEAR INTERVAL MODELS OF STATIC OBJECTS

Western Ukrainian National University, Ternopil

УДК 519.85

Ю. В. Добранюк, В. М. Михалевич, А. А. Коломієць, О. М. Козак

ЗАСТОСУВАННЯ СКМ MAPLE ДЛЯ ПОБУДОВИ 3D ГРАФІКІВ В ЗАДАЧАХ ОБЧИСЛЕННЯ ОБ'ЄМУ ФІГУР

Вінницький національний технічний університет, Вінниця

Анотація. З кожним роком збільшується число праць, що присвячені пошуку методів та прийомів впровадження систем комп'ютерної математики в навчання вищої математики. Основне місце серед них посідає система комп'ютерної математики Maple, яка є одним із лідерів універсальних систем та надає можливість користувачу використовувати інтелектуальне середовище для математичних досліджень. В даній роботі підкреслюється, що до найбільш цінних напрацювань теоретичного та прикладного характеру із застосування систем комп'ютерної математики у навчанні вищої математики слід віднести матеріали, які стосуються покращення наочності, а також формування у студентів умінь та навичок розв'язування типових задач вищої математики. Розглянуто проблеми впровадження та адаптації системи комп'ютерної математики Maple у навчальний процес закладу вищої освіти при викладанні курсу вищої математики. Використання систем комп'ютерної математики Maple надає можливість оптимізувати навчальний процес та активізувати організацію самостійної роботи студентів для закріплення навчального матеріалу. У роботі проведено адаптування використання можливостей графічного пакету системи комп'ютерної математики Maple для побудови 3D графіків з метою покращення наочності в задачах обчислення об'єму просторової фігури. Частина математичного апарату та розроблені фрагменти коду в системі комп'ютерної математики Maple надають можливість в автоматизованому режимі отримувати лінію перетину графіків функцій, будувати відповідні поверхні та фігури під час розв'язування типових задач вищої математики. В роботі обґрунтовано необхідність проектування навчальних задач нового типу з огляду на необхідність використання під час їх розв'язання сучасних інформаційно-комунікаційних технологій навчання, зокрема систем комп'ютерної математики Maple.

Ключові слова: система комп'ютерної математики, інформаційно-освітнє середовище, 3D графік, об'єм фігури, Maple.

Abstract. Every year the number of works devoted to the search for methods and techniques for introducing computer mathematics systems for teaching higher mathematics is increasing. The main place among them is occupied by the Maple computer mathematics system, which is one of the leaders in universal systems and allows the user to use an intelligent environment for mathematical research. This paper emphasizes that the most valuable developments of a theoretical and applied nature on the use of computer mathematics systems in teaching higher mathematics should include materials related to improving visibility, as well as the formation of students' skills and abilities in solving typical problems of higher mathematics. The problems of introduction and adaptation of the Maple computer mathematics system in the educational process of the institution of higher education in teaching the course of higher mathematics are considered. The use of the Maple computer mathematics system provides an opportunity to optimize the educational process and activate the organization of students' independent work to consolidate the educational material. The paper adapts the use of the Maple computer mathematics system graphics package capabilities to build 3D graphics in order to improve clarity in the tasks of calculating the volume of a spatial figure. Part of the mathematical apparatus and the developed code fragments in the Maple computer mathematics system make it possible to automatically obtain the line of intersection of graphs of functions, build the corresponding surfaces and figures when solving typical problems of higher mathematics. The paper substantiates the need to design educational problems of a new type, taking into account the need to use modern information and communication technologies for solving them, in particular Maple computer mathematics systems.

Key words: computer mathematics system, information and educational environment, 3D graph, volume of the figure, Maple.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-115-123>.

Вступ

Одним із основних напрямків удосконалення рівня викладання математичних дисциплін у ВНЗ є впровадження систем комп'ютерної математики (СКМ) у процес навчання. Незважаючи на суттєві складності впровадження СКМ у процес навчання вищої математики, з кожним роком зростає швидкість, кількість та якість наукових і навчально-методичних праць, присвячених вказаним питанням [1-14].

Актуальність

Одне із основних місць серед значної кількості систем комп'ютерної математики посідає СКМ Maple, яка є однією із універсальних систем та надає можливість користувачу використовувати інтелектуальне середовище для математичних досліджень [1-8]. Значну частку СКМ Maple займає в процесах розробки, дослідження, автоматизації та удосконалення наукових досліджень [9-14].

Незважаючи на значні переваги використання, досвід впровадження СКМ Maple у процес навчання вищої математики показує, що ускладненням отримання позитивного ефекту є додаткове інформаційне навантаження на студента, яке полягає в освоєні правил роботи потрібних команд та операторів [1-10].

Основною частиною розв'язання задач геометричного застосування кратних інтегралів є візуалізація та побудова необхідних областей і поверхонь [15]. СКМ Maple надає можливість автоматизувати процес побудови, дослідження та обчислення об'ємів просторових тіл.

Мета

Метою даної роботи є адаптування використання графічних пакетів СКМ Maple для побудови поверхонь під час розв'язання задач обчислення об'ємів складних просторових фігур.

Задачі

1. Розробка лістингу програмного коду в СКМ Maple для побудови просторових фігур під час розв'язання задач обчислення об'єму.
2. Розробка лістингу програмного коду в СКМ Maple для обчислення об'єму просторових фігур.

Розв'язання задач

Для виконання графічних побудов у СКМ Maple використовується спеціалізовані пакети графічних команд «plots» та «plottools», який надає користувачеві різноманітний спектр функцій. Спеціалізований пакет «plottools» в основному використовується для побудов спеціальних стандартизованих геометричних фігур, що надає можливість значно спростити використання СКМ Maple під час розв'язання геометричних задач [11-14].

```
restart;
with(plots):
with(plottools):
```

Розглянемо задачу обчислення об'єму фігури, яка обмежена частиною кулі та конусом. Спочатку задаємо рівняння поверхонь частини кулі та конуса у вигляді неявнозаданих функцій, які обмежують просторову фігуру (рис. 1).

```
print(`Задаємо рівняння поверхонь, які обмежують фігуру у вигляді неявнозаданих функцій:`);
F[1]:=z^2=x^2+y^2;
F[2]:=x^2+y^2+z^2=1;
```

Розв'язання задачі обчислення об'єму фігури, яка обмежена поверхнями кулі та конуса, потрібно виконувати в циліндричній системі координат, так як рівняння кулі та конуса мають значно простіший аналітичний вираз порівняно із декартовою системою. Вибір циліндричної системи координат також спрощує обчислення кратних інтегралів під час знаходження об'єму фігури, яку обмежують поверхні вказаних функцій. Для спрощення записаних виразів (F1 та F2) переходимо до циліндричної системи координат (рис. 1-2).

```
print(`Виконаємо перехід до циліндричної системи координат:`);
x:=r*cos(theta);
y:=r*sin(theta);
z:=z;
```

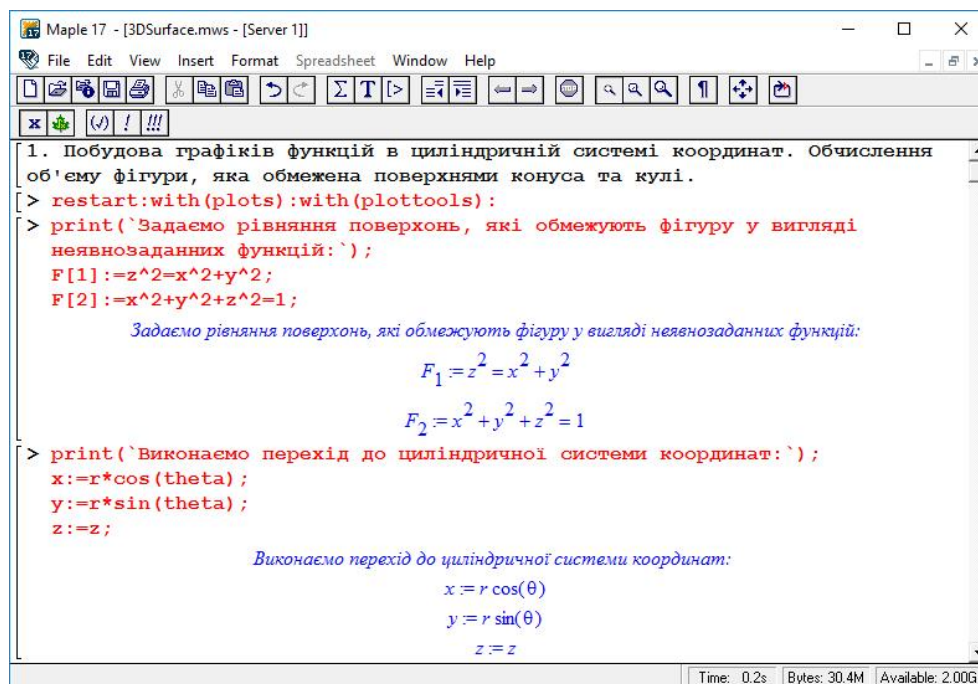


Рисунок 1 – Візуалізація задання функцій в СКМ Maple

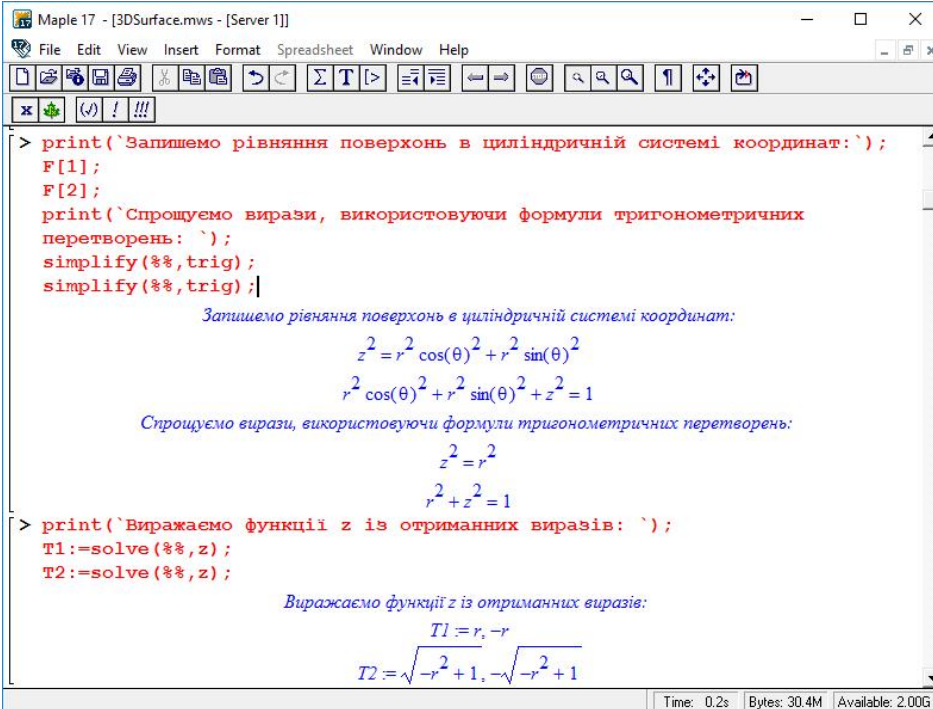
Для побудови вказаних поверхонь спрощуємо отримані вирази функцій в циліндричній системі координат та знаходимо їх розв'язок відносно координати z за допомогою функції аналітичного розв'язання систем рівнянь $solve(equations, variables)$ та спрощуємо отримані вирази за допомогою функції $simplify(expr)$ (рис. 2).

```
print(`Запишемо рівняння поверхонь в циліндричній системі координат:`);
F[1]; F[2];
print(`Спрощуємо вирази, використовуючи формули тригонометричних перетворень:`);
simplify(%, trig);
simplify(%, trig);
```

```
print(`Виражаємо функції z із отриманих виразів: `);
T1:=solve(%%,z);
T2:=solve(%%,z);
```

Для побудови просторової фігури та визначенні меж інтегрування для визначеного інтеграла потрібно визначити лінію перетину вказаних поверхонь. Лінією перетину частини кулі та конуса буде коло, яке в циліндричній системі координат визначатися радіусом r . Для знаходження вказаного радіуса в СКМ Maple використовуємо функцію аналітичного розв'язання систем рівнянь $solve(equations, variables)$ (рис. 3).

```
print(`Вирази функцій z: `);
Z1:=T1[1];
Z2:=T2[1];
print(`Знаходимо рівняння лінії перетину поверхонь F[1] та F[2] та значення
радіуса r: `);
T3:=solve({%=%%});
```



```
> print(`Запишемо рівняння поверхонь в циліндричній системі координат: `);
F[1];
F[2];
print(`Спростуємо вирази, використовуючи формули тригонометричних
перетворень: `);
simplify(%%,trig);
simplify(%%,trig);
```

Запишемо рівняння поверхонь в циліндричній системі координат:

$$z^2 = r^2 \cos^2(\theta) + r^2 \sin^2(\theta)$$

$$r^2 \cos^2(\theta) + r^2 \sin^2(\theta) + z^2 = 1$$

Спростуємо вирази, використовуючи формули тригонометричних перетворень:

$$z^2 = r^2$$

$$r^2 + z^2 = 1$$

```
> print(`Виражаємо функції z із отриманих виразів: `);
T1:=solve(%%,z);
T2:=solve(%%,z);
```

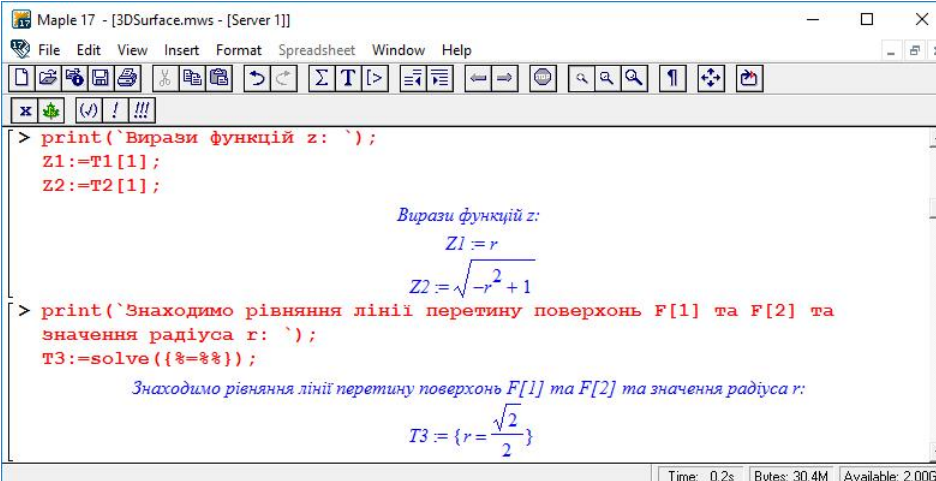
Виражаємо функції z із отриманих виразів:

$$T1 = r, -r$$

$$T2 = \sqrt{-r^2 + 1}, -\sqrt{-r^2 + 1}$$

Time: 0.2s | Bytes: 30.4M | Available: 2.00G

Рисунок 2 – Візуалізація перетворення рівнянь поверхонь кулі та конуса в СКМ Maple



```
> print(`Вирази функцій z: `);
Z1:=T1[1];
Z2:=T2[1];
```

Вирази функцій z:

$$Z1 = r$$

$$Z2 = \sqrt{-r^2 + 1}$$

```
> print(`Знаходимо рівняння лінії перетину поверхонь F[1] та F[2] та
значення радіуса r: `);
T3:=solve({%=%%});
```

Знаходимо рівняння лінії перетину поверхонь F[1] та F[2] та значення радіуса r:

$$T3 = \left\{ r = \frac{\sqrt{2}}{2} \right\}$$

Time: 0.2s | Bytes: 30.4M | Available: 2.00G

Рисунок 3 – Візуалізація знаходження лінії перетину поверхонь кулі та конуса в СКМ Maple

Наступним кроком розв'язання, в розробленому лістингу програмного коду в СКМ Maple, є побудова фігури, яку обмежують задані поверхні кулі та конуса. Для виконання графічних побудов у просторі

використовували функцію $plot3d(expr, x=a..b, y=c..d, opts)$ із різними параметрами величини елементів та їх кольору (рис. 4).

```
print(`Будуємо 3D графіки поверхонь F[1] та F[2]: `);
plot3d([Z1,Z2],theta=0..2*Pi,r=0..1, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1);
print(`Будуємо частину поверхні F[2], яка обмежує фігуру: `);
plot3d(Z2,theta=0..2*Pi,r=sqrt(2)/2..1, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1);
print(`Будуємо частину поверхні F[1], яка обмежує фігуру: `);
plot3d(Z1,theta=0..2*Pi,r=0..sqrt(2)/2, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1);
print(`Будуємо тільки фігуру, яка утворюється перетином поверхонь F[1] та F[2]: `);
F:=plot3d(Z1,theta=0..2*Pi,r=0..sqrt(2)/2, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1):
G:=plot3d(Z2,theta=0..2*Pi,r=sqrt(2)/2..1, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1):
display({F,G});
```

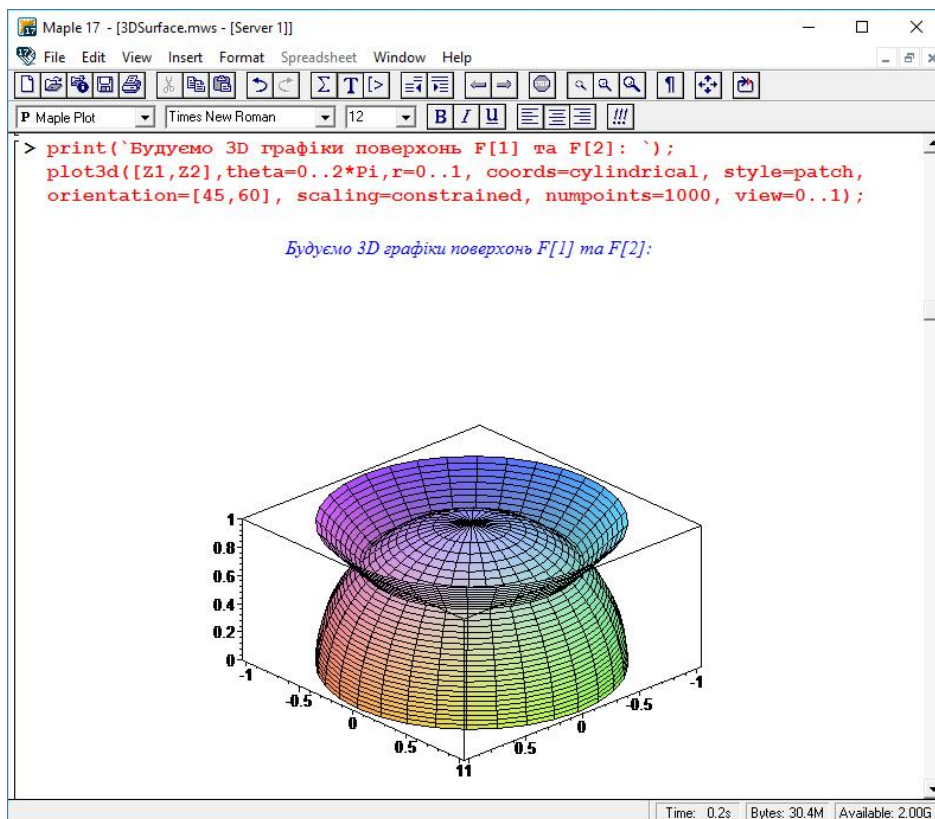


Рисунок 4 – Візуалізація побудови поверхонь кулі та конуса в СКМ Maple

Для покращення візуального представлення та сприйняття досліджуваної фігури, виконали поетапну побудову поверхонь та фігури, яка обмежена вказаними поверхнями, а також побудову кольорового виділення перерізу 1/4 частини фігури (рис. 5 - 7). Кожний графік представляли як окрему побудову, а потім реалізували їх спільне відображення на одному полотні за допомогою функції $display(L, inseq, options)$.

```
print(`Будуємо тільки 1/4 фігури, яка утворюється перетином поверхонь F[1] та F[2]: `);
F:=plot3d(Z1,theta=0..Pi/2,r=0..sqrt(2)/2, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1):
G:=plot3d(Z2,theta=0..Pi/2,r=sqrt(2)/2..1, coords=cylindrical, style=patch, orientation=[45,60], scaling=constrained, numpoints=1000, view=0..1):
```

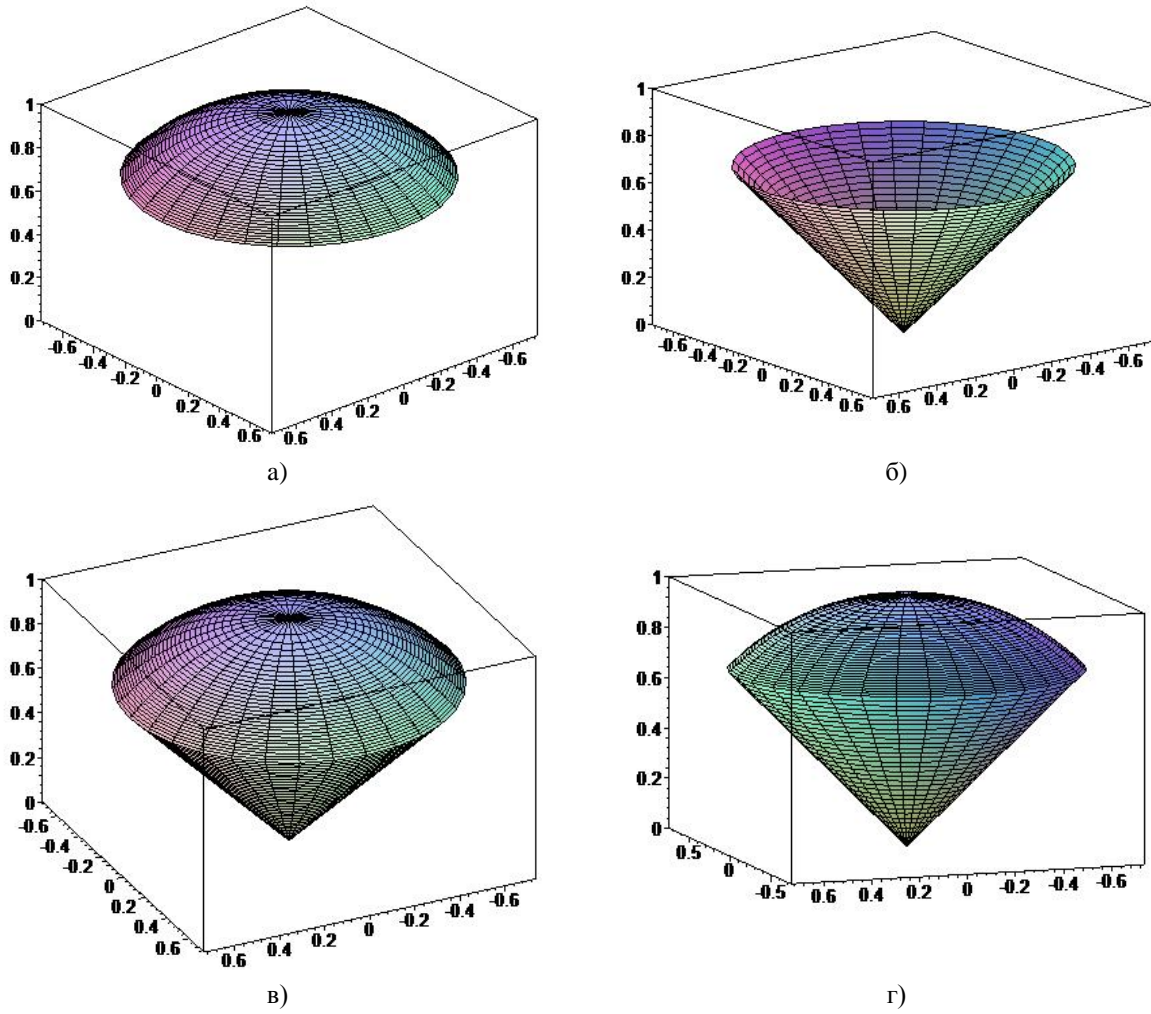


Рисунок 5 – Побудова частини поверхонь кулі а), конуса б) та фігури обмеженої вказаними поверхнями в), г) в СКМ Maple

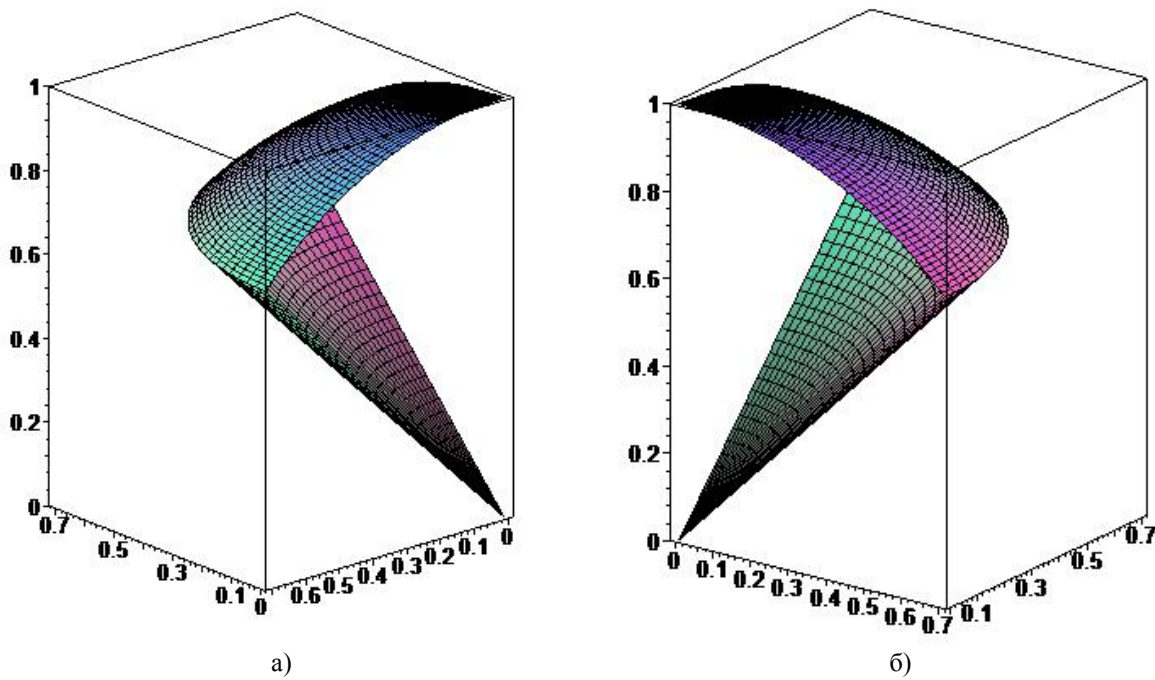


Рисунок 6 – Побудова 1/4 частини фігури а), б), яка обмежена поверхнями кулі та конуса, в СКМ Maple

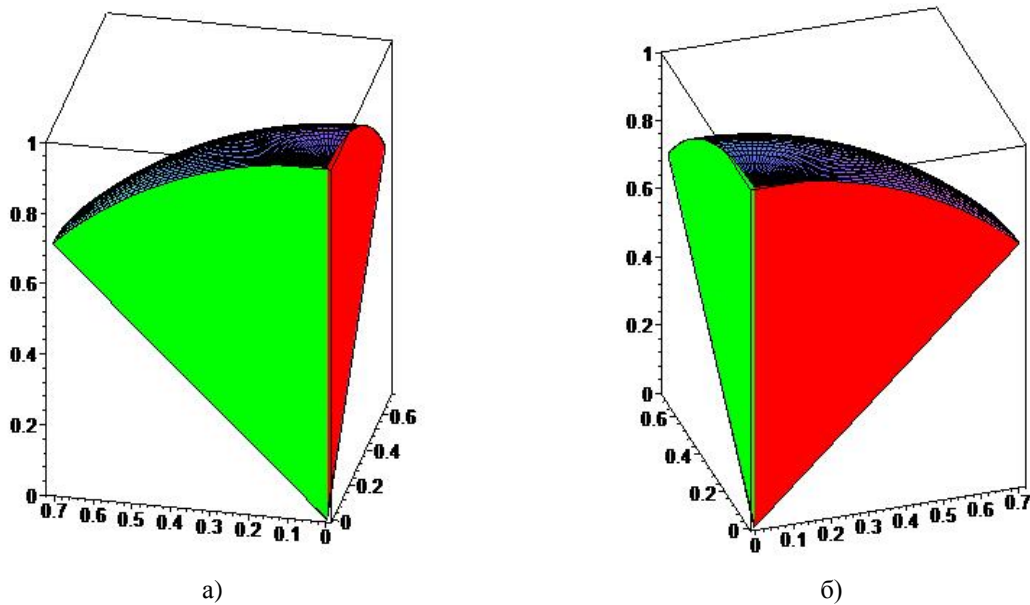


Рисунок 7 – Побудова 1/4 частини фігури із виділенням перерізу а), б), яка обмежена поверхнями кулі та конуса, в СКМ Maple

Особливої уваги потребує побудова зафарбовування перерізу фігури, яку виконували як побудову області із використанням функції графічного пакету $polygon([[x1, y1], [x2, y2], \dots, [xn, yn]], options)$.

```

11 := polygon([[0,0,0],
[0,sqrt(2)/2,sqrt(1-(sqrt(2)/2)^2)], [0,0.7,sqrt(1-0.7^2)], [0,0.6,sqrt(1-0.6^2)], [0,0.5,sqrt(1-0.5^2)], [0,0.4,sqrt(1-0.4^2)], [0,0.3,sqrt(1-0.3^2)], [0,0.2,sqrt(1-0.2^2)], [0,0.1,sqrt(1-0.1^2)], [0,0,1]], color=green, thickness=2, style=patchnograd):
12 := polygon([[0,0,0],
[sqrt(2)/2,0,sqrt(1-(sqrt(2)/2)^2)], [0.7,0,sqrt(1-0.7^2)], [0.6,0,sqrt(1-0.6^2)], [0.5,0,sqrt(1-0.5^2)], [0.4,0,sqrt(1-0.4^2)], [0.3,0,sqrt(1-0.3^2)], [0.2,0,sqrt(1-0.2^2)], [0.1,0,sqrt(1-0.1^2)], [0,0,1]], color=red, thickness=2, style=patchnograd):
display({F,G});
display({F,G,11,12});
    
```

Об'єм побудованої фігури обчислюємо за допомогою потрійного інтеграла в циліндричній системі координат з покроковим обчисленням повторного інтеграла (рис. 8).

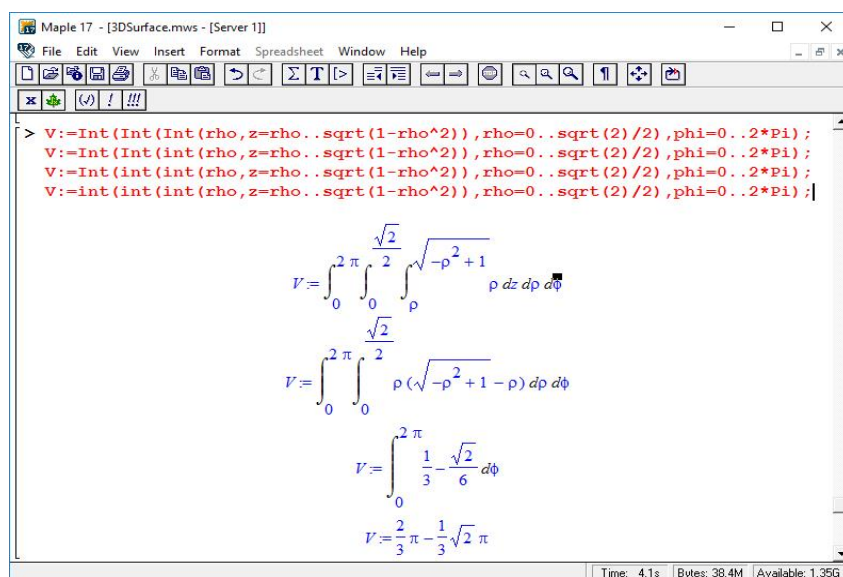


Рисунок 8 – Обчислення об'єму фігури, яка обмежена поверхнями кулі та конуса, в СКМ Maple

```

V:=Int(Int(Int(rho,z=rho..sqrt(1-rho^2)),rho=0..sqrt(2)/2),phi=0..2*Pi);
    
```

```
V:=Int(Int(int(rho,z=rho..sqrt(1-rho^2)),rho=0..sqrt(2)/2),phi=0..2*Pi);
V:=Int(int(int(rho,z=rho..sqrt(1-rho^2)),rho=0..sqrt(2)/2),phi=0..2*Pi);
V:=int(int(int(rho,z=rho..sqrt(1-rho^2)),rho=0..sqrt(2)/2),phi=0..2*Pi);
```

Висновки

1. Частина математичного апарату та розроблені фрагменти коду в СКМ Maple, які представлено в даній роботі, надають можливість студентам в автоматизованому режимі отримувати лінію перетину 3D графіків функцій, будувати відповідні поверхні та фігури, які вони обмежують та обчислювати їх об'єм, що покращує якість отриманих знань під час розв'язування типових задач вищої математики.

2. Оскільки значну частку системи комп'ютерної математики займають в процесах розробки, дослідження, автоматизації та удосконалення наукових досліджень, то постає необхідність проектування навчальних задач з вищої математики нового типу з огляду на необхідність використання під час їх розв'язання сучасних ІКТН, зокрема СКМ Maple.

Список літератури

- [1] В. М. Михалевич, та О. І. Тютюнник, *Використання систем комп'ютерної математики у процесі навчання лінійного програмування студентів ВНЗ: монографія*. Вінниця, Україна: ВНТУ, 2016, 279 с. ISBN 978-966-641-670-7.
- [2] В. М. Михалевич, та А. Ф. Дода, *Елементарна математика. Алгебра. Новітні інформаційні технології навчання (Maple). Ч. 2. : практикум*. Вінниця, Україна: ВНТУ, 2010, 160 с.
- [3] В. М. Михалевич, Н. Б. Дубова, та І. А. Клеопа, *Курс математики для слухачів-іноземців в середовищі СКМ Maple. Алгебраїчні рівняння і системи рівнянь: Електронний освітній ресурс*. Вінниця, Україна: ВНТУ, 2019, 64 с.
- [4] В. М. Михалевич, "Навчально-контролюючий Maple – комплекс з вищої математики," *Інформаційні технології та комп'ютерна інженерія*, № 1, с. 74-78. 2004.
- [5] О. І. Тютюнник, та В. М. Михалевич, "Реалізація принципу наочності за допомогою засобів СКМ у процесі навчання лінійного програмування," *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми*, Випуск 36, с. 434-440. 2013.
- [6] В. М. Михалевич, та О. І. Тютюнник, "Проектування навчальних задач з лінійного програмування з використанням систем комп'ютерної математики," *Інформаційні технології і засоби навчання*, т. 38, № 6, с. 24-33, 2013. [Електронний ресурс]. Режим доступу: <https://journal.iitta.gov.ua/index.php/itlt/article/view/896/688>. Дата звернення: Травень 20, 2022.
- [7] В. М. Михалевич, Ю. В. Добранюк, та Я. В. Крупський, "Фрагменти електронних освітніх ресурсів з функції двох змінних в середовищі СКМ Maple," на *Дистанційній всеукр. наук. конф. Математика у технічному університеті XXI сторіччя, Краматорськ : ДДМА*, 2017, с. 20-22.
- [8] В. М. Михалевич, Ю. В. Добранюк, та Я. В. Крупський, "Розробка електронних освітніх ресурсів в середовищі СКМ Maple," на *Всеукр. наук.-практ. конф. Математика та інформатика у вищій школі: виклики сучасності*, Вінниця, 2017, с. 69-72.
- [9] О. І. Тютюнник, М. С. Сичова, та М. Ю. Дунський, "Застосування системи MAPLE для знаходження дотичної до функції," на *LI науково-технічної конференції підрозділів ВНТУ*, Вінниця, 2022. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15009/12678>. Дата звернення: Травень 25, 2022.
- [10] В. М. Михалевич, Д. Б. Рогачевський, Д. Ю. Желнитський, та Б. А. Балух, "Навчальний MAPLE-тренажер з обчислення функції Ейлера," на *LI науково-технічної конференції підрозділів ВНТУ*, Вінниця, 2022. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15034/12681>. Дата звернення: Травень 25, 2022.
- [11] В. М. Михалевич, Ю. В. Добранюк, та А. А. Кашканова, "Побудова конформних відображень та дослідження їх властивостей за допомогою СКМ MAPLE," на *XLVI науково-технічної конференції підрозділів ВНТУ*, Вінниця, 2017. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2192>. Дата звернення: Травень 12, 2020.
- [12] Ю. В. Добранюк, А. В. Василич, та В. В. Грибик, "Застосування системи комп'ютерної математики Maple для побудови 2D областей в задачах обчислення площі фігур," на *LI науково-технічної конференції підрозділів ВНТУ*, Вінниця, 2022. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15848/13315>. Дата звернення: Травень 22, 2022.
- [13] Ю. В. Добранюк, Б. В. Маліцький, та Я. О. Глеба, "Застосування системи комп'ютерної математики Maple для обчислення площі фігури, яка обмежена колом та розташована поза кардіоїдою," на *III Міжнародної науково-методичної Інтернет-конф. Проблеми вищої математичної освіти: виклики сучасності*, Вінниця, 2022. [Електронний ресурс]. Режим доступу:

<https://conferences.vntu.edu.ua/index.php/pmvc/pmvc22/paper/viewFile/16248/13686>. Дата звернення: Червень 11, 2022.

- [14] Ю. В. Добранюк, та А. В. Василич, "Побудова траєкторії деформування вільної поверхні під час торцевого стиснення за допомогою системи комп'ютерної математики Maple," на *Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2022)»*, Вінниця, 2022. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/16247/13731>. Дата звернення: Червень 16, 2022.
- [15] В. О. Краєвський, Ю. В. Добранюк, та А. А. Коломієць, *Кратні, криволінійні, поверхневі інтеграли та елементи теорії поля: навчальний посібник*. Вінниця, Україна: ВНТУ, 2022, 142 с.

Стаття надійшла: 19.05.2022

References

- [1] V. M. Mykhalevych, & O. I. Tiutiunyk, *Vykorystannia system kompiuternoї matematyky u protsesi navchannia liniinoho prohramuvannia studentiv VNZ: monohrafiia*. Vinnytsia, Ukraina: VNTU, 2016, 279 s. ISBN 978-966-641-670-7. [in Ukrainian].
- [2] V. M. Mykhalevych, & A. F. Doda, *Elementarna matematyka. Alhebra. Novitni informatsiini tekhnologii navchannia (Maple). Ch. 2. : praktykum*. Vinnytsia, Ukraina: VNTU, 2010, 160 s. [in Ukrainian].
- [3] V. M. Mykhalevych, N. B. Dubova, & I. A. Kleopa, *Kurs matematyky dlia slukhachiv-inozemtsiv v seredovyschi SKM Maple. Alhebraichni rivniannia i systemy rivnian: Elektronnyi osvittii resurs*. Vinnytsia, Ukraina: VNTU, 2019, 64 s. [in Ukrainian].
- [4] V. M. Mykhalevych, "Navchalno-kontroliuiuchy Maple – kompleks z vyshchoi matematyky," *Informatsiini tekhnologii ta kompiuterna inzheneriia*, № 1, s. 74-78. 2004 [in Ukrainian].
- [5] O. I. Tiutiunyk, & V. M. Mykhalevych, "Realizatsiia pryntsyphu naochnosti za dopomohou zasobiv SKM u protsesi navchannia liniinoho prohramuvannia," *Suchasni informatsiini tekhnologii ta innovatsiini metodyky navchannia u pidhotovtsi fakhivtsiv: metodolohiia, teoriia, dosvid, problemy*, Vypusk 36, s. 434-440. 2013 [in Ukrainian].
- [6] V. M. Mykhalevych, & O. I. Tiutiunyk, "Projektuvannia navchalnykh zadach z liniinoho prohramuvannia z vykorystanniam system kompiuternoї matematyky," *Informatsiini tekhnologii i zasoby navchannia*, t. 38, № 6, s. 24-33, 2013. [Elektronnyi resurs]. Rezhym dostupu: <https://journal.iitta.gov.ua/index.php/itlt/article/view/896/688>. Data zvernennia: Traven 20, 2022 [in Ukrainian].
- [7] V. M. Mykhalevych, Yu. V. Dobraniuk, & Ya. V. Krupskiy, "Frahmenty elektronnykh osvittikh resursiv z funktsii dvokh zminnykh v seredovyschi SKM Maple," na *Dystantsiini vseukr. nauk. konf. Matematyka u tekhnichnomu universyteti XXI storichchia, Kramatorsk: DDMA*, 2017, s. 20-22 [in Ukrainian].
- [8] V. M. Mykhalevych, Yu. V. Dobraniuk, & Ya. V. Krupskiy, "Rozrobka elektronnykh osvittikh resursiv v seredovyschi SKM Maple," na *Vseukr. nauk.-prakt. konf. Matematyka ta informatyka u vyshchii shkoli: vyklyky suchasnosti*, Vinnytsia, 2017, s. 69-72 [in Ukrainian].
- [9] O. I. Tiutiunyk, M. S. Sychova, & M. Yu. Dunskiy, "Zastosuvannia systemy MAPLE dlia znakhodzhennia dotychnoi do funktsii," na *LI naukovu-tekhnichnoi konferentsii pidrozdiliv VNTU*, Vinnytsia, 2022. [Elektronnyi resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15009/12678>. Data zvernennia: Traven 25, 2022 [in Ukrainian].
- [10] V. M. Mykhalevych, D. B. Rohachevskiy, D. Yu. Zhelnytskyi, & B. A. Balukh, "Navchalnyi MAPLE-trenazher z obchyslennia funktsii Eilera," na *LI naukovu-tekhnichnoi konferentsii pidrozdiliv VNTU*, Vinnytsia, 2022. [Elektronnyi resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15034/12681>. Data zvernennia: Traven 25, 2022 [in Ukrainian].
- [11] V. M. Mykhalevych, Yu. V. Dobraniuk, & A. A. Kashkanova, "Pobudova konformnykh vidobrazhen ta doslidzhennia yikh vlastyvostei za dopomohou SKM MAPLE," na *XLVI naukovu-tekhnichnoi konferentsii pidrozdiliv VNTU*, Vinnytsia, 2017. [Elektronnyi resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2192>. Data zvernennia: Traven 12, 2020 [in Ukrainian].
- [12] Yu. V. Dobraniuk, A. V. Vasylynych, & V. V. Hrybyk, "Zastosuvannia systemy kompiuternoї matematyky Maple dlia pobudovy 2D oblastei v zadachakh obchyslennia ploskhi fihur," na *LI naukovu-tekhnichnoi konferentsii pidrozdiliv VNTU*, Vinnytsia, 2022. [Elektronnyi resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15848/13315>. Data zvernennia: Traven 22, 2022 [in Ukrainian].

- [13] Yu. V. Dobraniuk, B. V. Malitskyi, & Ya. O. Hleba, "Zastosuvannia systemy kompiuternoї matematyky Maple dlia obchyslennia ploshchi fihury, yaka obmezheni kolom ta roztashovana poza kardoidoiu," na *III Mizhnarodnoi naukovo-metodychnoi Internet-konf. Problemy vyshchoi matematychnoi osvity: vyklyky suchasnosti*, Vinnytsia, 2022. [Elektronnyi resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/pmovc/pmovc22/paper/viewFile/16248/13686>. Data zvernennia: Cherven 11, 2022 [in Ukrainian].
- [14] Yu. V. Dobraniuk, & A. V. Vasylynch, "Pobudova traektorii deformuvannia vilnoi poverkhni pid chas tortsevoho stysnennia za dopomohoiu systemy kompiuternoї matematyky Maple," na *Vseukrainskoi naukovo-praktychnoi internet-konferentsii studentiv, aspirantiv ta molodykh naukovtsiv «Molod v nautsi: doslidzhennia, problemy, perspektyvy (MN-2022)»*, Vinnytsia, 2022. [Elektronnyi resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/16247/13731>. Data zvernennia: Cherven 16, 2022. [in Ukrainian].
- [15] V. O. Kraievskiy, Yu. V. Dobraniuk, & A. A. Kolomiets, *Kratni, kryvoliniini, poverkhnevi intehrally ta elementy teorii polia: navchalnyi posibnyk*. Vinnytsia, Ukraina: VNTU, 2022, 142 s. [in Ukrainian].

Відомості про авторів

Добранюк Юрій Володимирович – кандидат технічних наук, доцент кафедри вищої математики.

Михалевич Володимир Маркусович – доктор технічних наук, професор, завідувач кафедри вищої математики.

Коломієць Альона Анатоліївна – кандидат педагогічних наук, доцент, доцент кафедри вищої математики.

Козак Олександр Михайлович – студент групи ІБС-196.

Yu. V. Dobraniuk, V. M. Mikhalevich, A. A. Kolomiets, O. M. Kozak

APPLICATION OF CMS MAPLE FOR BUILD OF 3D GRAPHICS IN THE PROBLEMS OF CALCULATING THE VOLUME OF FIGURES

Vinnytsia National Technical University, Vinnytsia

УДК 681.327.11

Н. В. Сачанюк-Кавецька, О. П. Прозор, В. В. Хом'юк, І. О. Бондаренко

МАТЕМАТИЧНИЙ ОПИС ОПЕРАЦІЇ НЕРІВНОЗНАЧНОСТІ В ЛОГІКО-ЧАСОВОМУ СЕРЕДОВИЩІ

Вінницький національний технічний університет, Вінниця

Анотація. Нині є актуальною проблема інформаційної безпеки, яка пов'язана із збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах. Цілісність і конфіденційність інформації має вагомое значення для конкурентоспроможності та репутації організації чи підприємства. Аналітична обробка цифрових сигналів в графічному чи в чисто цифровому представленні дещо обмежена і не враховує динаміку сигналів та повідомлень. Щоб полегшити попередню обробку динамічних цифрових змінних та сигналів можна використати логіко-часову функцію багатозначної логіки. В статті зазначено, що обчислювальне математичне моделювання стає основним інструментом дослідження складних динамічних процесів і систем. Класичний апарат логіки є недостатнім для опису динаміки поведінки системи в часі. Тому актуальною є розробка моделей так званого булевого диференціального числення, оскільки даний підхід спирається на загальне поняття зміни логічної змінної, що призведе до універсальної, з точки зору динаміки, системи понять та операцій. Для полегшення попередньої обробки динамічних цифрових змінних та сигналів можна використати логіко-часову функцію багатозначної логіки. В роботі розглянуто одну з важливих операцій – операцію нерівнозначності та деякі її властивості. Показано, що для логіко-часової функції двійкової логіки дана операція співпадає з сумою по модулю два. Нерівнозначність дозволить, в подальшому, ввести більш складні операції над багатозначними логіко-часовими функціями, такими як похідна і первісна та здійснювати кодування, шифрування інформації в логіко-часовому середовищі. Продемонстровано можливість використання нерівнозначності при побудові індикаторних операцій та диференціала змінної. Змодельовано схему реалізації операції нерівнозначності.

Ключові слова: логіко-часова функція багатозначної логіки, нерівнозначність, сума за модулем 2, жвавість, диференціал.

Abstract. Currently, there is an urgent problem of information security, which is related to the preservation of the confidentiality of information processed and stored in computer systems. The integrity and confidentiality of information is of great importance for the competitiveness and reputation of an organization or enterprise. Analytical processing of digital signals in a graphical or purely digital representation is somewhat limited and does not take into account the dynamics of signals and messages. To facilitate the preprocessing of dynamic digital variables and signals, the logic-time function of multivalued logic can be used. The article notes that computational mathematical modeling is becoming the main tool for studying complex dynamic processes and systems. The classical apparatus of logic is insufficient to describe the dynamics of system behavior over time. Therefore, it is important to develop models of so-called Boolean differential calculus, as this approach is based on the general concept of changing the logical variable, which will lead to a universal, in terms of dynamics, system of concepts and operations. It is shown that for the logic-time function of binary logic, this operation coincides with the sum modulo two. You can use the logic-time function of multivalued logic to facilitate the pre-processing of dynamic digital variables and signals. The paper considers one of the important operations - the operation of inequality and some of its properties. Inequality will allow, in the future, to introduce more complex operations on multivalued logical-temporal functions, such as derivative and initial, and to perform encoding, encryption of information in the logical-temporal environment. The possibility of using inequality when constructing indicator operations and variable differential is demonstrated. The implementation scheme of the inequality operation is modeled.

Keywords: logic-time function of multivalued logic, inequality, sum by module 2, liveliness, differential.

DOI: <https://doi.org/10.31649/1999-9941-2022-54-2-124-130>.

Вступ

Використання методів математичного моделювання та автоматизованих рішень інженерно-наукових завдань дозволяє значно підвищити ефективність процесів проектування, реконструкції, обробки та управління. Обчислювальне математичне моделювання стає основним інструментом дослідження складних динамічних процесів і систем. Загально прийнятним математичним апаратом дослідження цифрових сигналів є алгебра логіки. З її допомогою було сформульовано та розв'язано безліч задач опису, перетворення та побудови логічних систем. Класичний апарат логіки, що достатньо точно описує структуру та функціональні зв'язки між входами та виходами таких систем, є недостатнім для опису динаміки поведінки системи в часі. Питання «динаміки у великому» досить легко розв'язуються за допомогою теорії автоматів, однак вона не відображає динаміку перехідних процесів, пов'язану із часовими характеристиками елементів системи, що вимірюються в реальному часі. Тому актуальною є розробка моделей так званого булевого диференціального числення, оскільки даний підхід спирається на загальне поняття зміни логічної змінної, що призведе до універсальної, з точки зору динаміки, системи понять та операцій за допомогою яких можна ставити та розв'язувати задачі типові як для теорії автоматів, так і для дискретної «динаміки в малому».

Огляд та постановка задачі

З появою та розвитком інформаційних технологій актуальною проблема інформаційної безпеки, яка пов'язана із збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах. Саме цілісність і конфіденційність інформації має вагомое значення для конкурентоспроможності та репутації підприємства. Аналітична обробка цифрових сигналів в графічному чи в чисто цифровому представленні дещо обмежена і не враховує динаміку сигналів та повідомлень. Тому, щоб полегшити попередню обробку динамічних цифрових змінних та сигналів можна використати логіко-часову

функцію багатозначної логіки (БЛЧФ) [1]. Для комп'ютерної обробки в режимі реального часу аналого-вий сигнал повинен бути оцифрований шляхом його вибірки за одиничними Δ - інтервалами та реалізовано квантування на k рівнів амплітуди. В роботі [2] було розглянуто індексну форму подання БЛЧФ, поняття продукууючого слова та базові операції над функціями, які дозволяють розробляти більш складні операції. Зокрема такі операції, які дозволяють кодувати інформацію та будувати крипто-ключі, оскільки це є одним із ключових моментів розробки політики інформаційної безпеки [3].

Тому актуальною буде розробка математичного апарату, який в простій і доступній формі дозволить здійснювати аналітичну обробку динамічних цифрових сигналів та здійснювати прогнозування змін параметрів сигналів суто засобами математики. В роботі [1] було введено операцію нерівнозначного віднімання, що визначалась різницею по модулю значень та була досить громіздкою при використанні. Враховуючи подання БЛЧФ, яке було запропоновано [2] та узагальнюючи логіко-часові функції (ЛЧФ) двійкової та багатозначної логіки таку операцію більш доцільно вважати логічною операцією нерівнозначності, а модуль різниці амплітуд змінних є мірою цієї нерівнозначності.

Мета

Метою даної статті є представлення операції нерівнозначності логіко-часових функцій багатозначної логіки з використанням моделювання її схеми.

Основні положення

Для позначення нерівнозначності $\left| \begin{matrix} x \\ k \end{matrix} a_t - \begin{matrix} y \\ k \end{matrix} d_t \right|$ використаємо символ « \ominus » і запишемо нерівнозначність БЛЧФ у вигляді:

$$\left(\begin{matrix} x \\ k \end{matrix} a_{t_x}^{T_x} \ominus \begin{matrix} y \\ k \end{matrix} a_{t_y}^{T_y} \right) = \bigg| \begin{matrix} x \\ k \end{matrix} a_i \ominus \begin{matrix} y \\ k \end{matrix} c_i \bigg|_{k} (x \ominus y)_{\min(t_x, t_y)}^{T_{\max}}$$

де W – оператор впорядкування за часом та розбиття значень аргументів БЛЧФ на одиничні Δ -інтервали.

Операція нерівнозначності має властивість комутативності: $\begin{matrix} k \end{matrix} x(t) \ominus \begin{matrix} k \end{matrix} y(t) = \begin{matrix} k \end{matrix} y(t) \ominus \begin{matrix} k \end{matrix} x(t)$. Для ілюстрації справедливості даної властивості проаналізуємо таблиці Келлі, наприклад для $k = 2, 3, \text{ та } 4$ (див. рис. 1). Оскільки всі таблиці симетричні відносно головної діагоналі, то це означає, що операція нерівнозначності комутативна.

Можна показати, що дана операція не має властивості асоціативності:

$$\left(\begin{matrix} x \ominus y \end{matrix} \right) \ominus z \neq x \ominus \left(\begin{matrix} y \ominus z \end{matrix} \right),$$

і також немає властивості дистрибутивності кон'юнкції (диз'юнкції) відносно операції нерівнозначності. Зокрема, $\left(\begin{matrix} x_t \triangle \left(\begin{matrix} y_t \ominus z_t \end{matrix} \right) \right) \neq \left(\begin{matrix} x_t \triangle y_t \end{matrix} \right) \ominus \left(\begin{matrix} x_t \triangle z_t \end{matrix} \right)$, де « \triangle » – операція кон'юнкції БЛЧФ:

$$\left(\begin{matrix} x \\ k \end{matrix} a_{t_x}^{T_x} \triangle \begin{matrix} y \\ k \end{matrix} a_{t_y}^{T_y} \right) = \bigg| \begin{matrix} x \\ k \end{matrix} a_i, \begin{matrix} y \\ k \end{matrix} c_i \bigg|_{k} (x \triangle y)_{\max(t_x, t_y)}^{\min(t_x + T_x, t_y + T_y) - \max(t_x, t_y)}$$

Індекси типу \min , \max з параметрами, визначають інтервали існування функції, а значення власне самої функції, кон'юнкцію $\begin{matrix} x \\ k \end{matrix} a_t$ та $\begin{matrix} y \\ k \end{matrix} c_t$, потрібно вираховувати для кожного t з кроком рівним одиниці від $\max(t_x, t_y)$ до $\left(\min(t_x + T_x, t_y + T_y) - \max(t_x, t_y) \right)$.

k -значної алгебри при $k = 2$. Тоді взаємна еквівалентність справедлива і для логічних виразів. Побудуємо таблицю істинності для $x \oplus y$ та $x \ominus y$ (див. табл. 1).

Таблиця 1 – Таблиця істинності

x	y	\bar{x}	\tilde{x}	\bar{y}	\tilde{y}	$x \sqcap \bar{y}$	$\bar{x} \sqcap y$	$x \sqcap \tilde{y}$	$\tilde{x} \sqcap y$	$x \sqcap \bar{y} \vee \bar{x} \sqcap y$	$x \sqcap \tilde{y} \vee \tilde{x} \sqcap y$
0	0	1	1	1	1	0	0	0	0	0	0
0	1	1	1	0	0	0	1	0	1	1	1
1	0	0	0	1	1	1	0	1	0	1	1
1	1	0	0	0	0	0	0	0	0	0	0

З таблиці зрозуміло, що $x \sqcap \bar{y} \vee \bar{x} \sqcap y$ рівний $x \sqcap \tilde{y} \vee \tilde{x} \sqcap y$.

Якщо вхідні змінні x та $y \in$ ЛЧФ, що мають по одному відрізку існування $x(t) = x_{t_x}^{T_x}$, $y(t) = y_{t_y}^{T_y}$, тоді $\tilde{x}(t) = x_0^{t_x} \oplus x_{t_x+T_x}^\infty$, $\tilde{y}(t) = y_0^{t_y} \oplus y_{t_y+T_y}^\infty$ відповідно. Використавши досконалу диз'юнктивну нормальну форму отримаємо:

$$\begin{aligned}
 x(t) \ominus y(t) &= (x_0^{t_x} \oplus x_{t_x+T_x}^\infty) \sqcap y_{t_y}^{T_y} \vee x_{t_x}^{T_x} \sqcap (y_0^{t_y} \oplus y_{t_y+T_y}^\infty) = \\
 &= \left(x_0^{t_x} \sqcap y_{t_y}^{T_y} \oplus x_{t_x+T_x}^\infty \sqcap y_{t_y}^{T_y} \right) \vee \left(x_{t_x}^{T_x} \sqcap y_0^{t_y} \oplus x_{t_x}^{T_x} \sqcap y_{t_y+T_y}^\infty \right) = \\
 &= \left((x \ominus y)_{t_y}^{\min(t_x, t_y+T_y)-t_y} \oplus (x \ominus y)_{\max(t_x+T_x, t_y)}^{(t_y+T_y)-\max(t_x+T_x, t_y)} \right) \vee \\
 &\vee \left((x \ominus y)_{t_x}^{\min(t_x+T_x, t_y)-t_x} \oplus (x \ominus y)_{\max(t_x, t_y+T_y)}^{(t_x+T_x)-\max(t_x, t_y+T_y)} \right)
 \end{aligned}$$

Подальший аналітичний запис вимагає використання формули для диз'юнкції БЛЧФ:

$$\left({}_k x_{t_x}^{T_x} \vee {}_k y_{t_y}^{T_y} \right) = \bigvee_{i=0}^{T_{\max}-1} \max \left({}^x a_i, {}^y c_i \right) \Big|_k (x \vee y)_{\min(t_x, t_y)}^{T_{\max}},$$

де « \vee » – операція диз'юнкції БЛЧФ, а $T_{\max} = \left(\max(t_x + T_x, t_y + T_y) - \min(t_x, t_y) \right)$.

Аналітично це трохи громіздкий варіант, але для конкретних реальних змінних все набагато простіше. Звичайно аналітичні дослідження зручніше робити через продукуючі слова повної форми запису БЛЧФ.

На рис. 3 наведено графічні результати операції додавання по модулю 2 або нерівнозначності. Тоді аналітичне обчислення відповідних функцій, зображених на рис. 3:

$$\begin{aligned}
 x_1^2 \oplus y_2^4 &= (x \oplus y)_2^{-1} \vee (x \oplus y)_3^3 \vee (x \oplus y)_1^1 \vee (x \oplus y)_6^{-3} = \\
 &= (x \oplus y)_1^1 \vee (x \oplus y)_3^3; \\
 x_1^2 \oplus z_5^3 &= (x \oplus z)_5^{-4} \vee (x \oplus z)_5^3 \vee (x \oplus z)_1^2 \vee (x \oplus z)_8^{-5} = \\
 &= (x \oplus z)_1^2 \vee (x \oplus z)_5^3.
 \end{aligned}$$

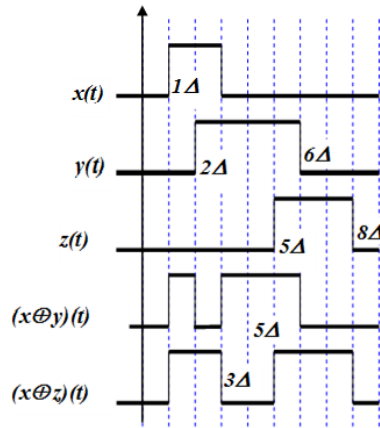


Рисунок 3 – Двійкова нерівнозначність

Операцію нерівнозначності можна застосувати при побудові так званих індикаторних операцій. Зокрема, для оцінки інтенсивності зміни БЛЧФ введемо поняття жвавості. Жвавість (V) це число, що показує сумарно як інтенсивно змінюється значення функції протягом всього відрізка її існування, який може включати нульові підінтервали і визначається за формулою:

$$V(a_0, a_1, \dots, a_N | {}_k x_{t_x}^{T_x}) = \sum_{i=0}^{N+1} (a_i \ominus a_{i+1}).$$

Для функції ${}_4 x(t) = 1^2 2^1 1^2 2^1 3^1 2^2 | {}_4 x_1^8$ жвавість $V = 8$. Максимальне значення жвавості на відріжку існування обчислюється за формулою: $V_{\max}({}_k x_{t_x}^{T_x}) = [(k-1) \times (T_x + 1)]$. Відповідно мінімальне значення жвавості $V_{\min} = 1$ і описує перехід БЛЧФ з однієї константи на сусідню вверх або вниз на логічну одиницю, а при $V = 0$ маємо справу з константою. Якщо для бінарної ЛЧФ з N відрізками існування, використати індексний запис БЛЧФ і додати нульові підінтервали, отримаємо оцінку жвавості двійкової багатоінтервальної ЛЧФ. Такий підхід об'єднує всі $k \geq 2$ і дає можливість все розглядати як багатозначність. Бінарний варіант це окремий випадок загального k – значного варіанту.

Для повної форми представлення БЛЧФ:

$$V(x_{t_x}^{T_x}) = V\left(\begin{matrix} T_x-1 \\ W \\ i=0 \end{matrix} a_i \middle| x_{t_x}^{T_x}\right) = \sum_{i=0}^{T_x-1} \frac{T_x-1}{W} (a_i \ominus a_{i+1}) = \left[\sum_{i=0}^{T_x-1} (a_i \ominus a_{i+1}) \right]$$

В роботі [4] було введено змінну dx , що названа диференціалом змінної x . Вона описує зміну x^* по заданому значенні x та значенню dx із співвідношення $x^* = x \oplus dx$. Якщо згадати, що функція додавання по модулю 2 фактично представляє собою нерівнозначність, то для k -значних змінних згадане співвідношення матиме вигляд:

$${}_k x^* = {}_k x \ominus_k dx$$

Значення ${}_k dx \in \{1, 2, \dots, k-1\}$ описує величину і факт зміни ${}_k x$, а ${}_k dx = 0$, подібно до булевих змінних, описує незмінність значення ${}_k x$. Для логіко-часових функцій можна записати $t^* = t + dt$ і відповідно, для загального випадку, маємо диференціал по часі ЛЧФ ${}_k z(t)$:

$${}_k dz(t) = {}_k z(t) \ominus {}_k z(t + dt).$$

Для $dt = \Delta = 1$ отримаємо

$$[dz(t) = z(t) \ominus z(t + \Delta) = z(t) \ominus z(t + 1)];$$

$$dz(t) = z(t) \ominus Dz(t).$$

Схему нерівнозначності синтезовано на двійкових логічних елементах з використання двійкового кодування: «0» – 00, «1» – 01 та «2» – 10 (див. рис. 4). Вхід «A» стробуючий.

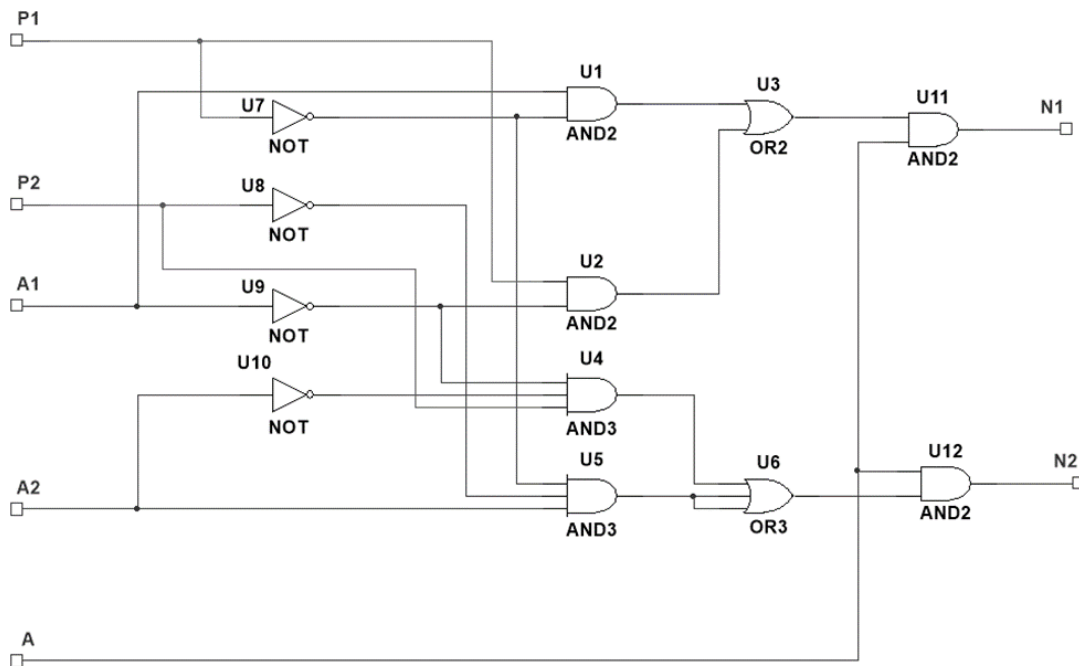


Рисунок 4 – Схема реалізації операції нерівнозначності

Висновки

1. Розглянуто одну з важливих операцій – операцію нерівнозначності, яка дозволить, в подальшому, ввести більш складні операції над БЛЧФ, такі як похідна та первісна.
2. Розглянуто окремі властивості операції нерівнозначності та показано, що для ЛЧФ двійкової логіки дана операція співпадає з сумою по модулю два, що дозволить створювати схемотехнічні варіанти реалізації математичних операцій в логіко-часовому середовищі на двійкових елементах.
3. Продемонстровано можливість використання нерівнозначності при побудові індикаторних операцій та диференціала змінної.
4. Змодельовано схему реалізації операції нерівнозначності.
5. Для кращого приховування інформації та її захисту від модифікацій, підробки або викривлення, операція нерівнозначності дозволить здійснювати кодування та шифрування інформації в логіко-часовому середовищі, створювати графічні паролі, будувати крипто-ключі і т ін.

Список літератури

- [1] Н. В. Сачанюк-Кавецька, В. П. Кожем'яко, *Елементи око-процесорної обробки зображень в логіко-часовому середовищі. Монографія.* Вінниця, Україна: УНІВЕРСУМ, 2004, 135 с.
 - [2] Н. В. Сачанюк-Кавецька, О. П. Прозор, "Елементи математичного опису логіко-часових функцій багатозначної логіки та окремих операцій над ними," *Інформаційні технології та комп'ютерна інженерія*, том 53 (№ 1), с. 111-118. 2022.
 - [3] Н. В. Сачанюк-Кавецька, "Кодування як засіб захисту інформації у системах контролю доступу з використанням логіко-часових функцій у формі поліномів і біометричних даних суб'єктів," *Ресстрація, зберігання і обробка даних. – Інститут проблем ресстрації інформації НАН України*, том 20, № 2, с. 60-68. 2018.
 - [4] D. Bochmann, C. Posthoff, *Binare dynamische systeme.* Akademie-Verlag, Berlin, 1981, 400 p.
- Стаття надійшла 04.04.2022.

References

- [1] N. V. Sachaniuk-Kavetska, V. P. Kozhemiako, *Elementy oko-protsesornoї obrobky zobrazhen v lohiko-chasovomu seredovyshchi. Monohrafiia*. Vinnytsia, Ukraina: UNIVERSUM, 2004, 135 s. [in Ukrainian].
- [2] N. V. Sachaniuk-Kavetska, O. P. Prozor, "Mathematical description of logic-time functions of multiple-valued logic and some operations over them," *Information technology and computer engineering*, tom 53 (№ 1), pp. 111-118. 2022 [in Ukrainian].
- [3] N. V. Sachaniuk-Kavetska, "Koduvannia yak zasib zakhystu informatsii u systemakh kontroliu dostupu z vykorystanniam lohiko-chasovykh funktsii u formi polinomiv i biometrychnykh danykh subiektiv," *Reyestratsiia, zberihannia i obrobka danykh. – Instytut problem reiestratsii informatsii NAN Ukrainy*, tom 20, № 2, pp. 60-68. 2018 [in Ukrainian].
- [4] D. Bochmann, C. Posthoff, *Binare dynamische systeme*. Akademie-Verlag, Berlin, 1981, 400 p.

Відомості про авторів

Сачанюк-Кавецька Наталія Василівна – кандидат технічних наук, доцент, доцент кафедри вищої математики.

Прозор Олена Петрівна – кандидат педагогічних наук, доцент, доцент кафедри вищої математики.

Хом'юк Віктор Вікторович – кандидат технічних наук, доцент, доцент кафедри вищої математики.

Бондаренко Ірина Олексіївна – кафедра менеджменту безпеки інформаційних систем.

N. Sachaniuk-Kavets'ka, O. Prozor, V. Khomyuk, I. Bondarenko

MATHEMATICAL DESCRIPTION OF THE INEQUALITY OPERATION IN A LOGIC-TIME ENVIRONMENT

Vinnytsia National Technical University, Vinnytsia

ДО ВІДОМА АВТОРІВ

Найновіші правила оформлення і подання статей знаходяться на сайті журналу
<http://itce.vntu.edu.ua/>