

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.8:044.89

Т. Д. Польгуль

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПОБУДОВИ
ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІЯВЛЕННЯ
ШАХРАЙСТВА ПРИ ІНСТАЛЮВАННІ МОБІЛЬНИХ
ДОДАТКІВ

Вінницький національний технічний університет, Вінниця

Анотація. У роботі запропоновано інформаційну технологію побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків, яку бажано використовувати при розробці такого класу систем. Здійснено інтелектуальну обробку наявних даних по користувачу, на основі якої запропоновано шкалювання не по значенню ознаки, а по кінцевій інформації, яку несе ознака по користувачу. Запропоновано систему з інтелектуальною складовою – формуванням бази знань, яка дозволить визначити шахраїв, та в яку включатимуться правила аналізу аномалій, при чому так, щоб поява нової аномалії в даних дозволяла створити нове правило. Така база знань може розширюватись через можливість появи нового виду аномалії в даних (шахрайства). Отриманий набір правил, що у подальшому на основі розроблених в роботі алгоритмів дозволить створити узагальнений портрет шахрая, відзначивши навіть нові та невідомі експертам шахрайські властивості. Віднесення підозрілих користувачів до класу шахраїв або органічних відбувається з використанням нечіткої логіки. Завдяки запропонованій інтелектуальній обробці наявних даних про користувачів, шкалюванню по кінцевій інформації, яку несе ознака та створенню баз знань, що розвиваються, запропонована інформаційна технологія дозволяє побудувати інтелектуальні системи, що матимуть можливість адаптуватися до появи нових видів шахрайства. Відповідно до задач, які повинні вирішувати такі інтелектуальні системи, запропоновано їх структуру: підсистема виявлення характеристик користувача; підсистема подолання різноманітності даних; підсистема тренування класифікаційної моделі; підсистема класифікації; підсистема формування бази даних шахраїв; підсистема формування бази знань (для виявлення шахраїв); підсистема інтелектуального аналізу даних та формування шаблонів користувачів; підсистема прогнозування узагальненого шаблону шахрая. Запропонована інформаційна технологія побудови інтелектуальних систем дозволяє обробляти різноформатні вхідні дані, що у процесі дає можливість сформувати узагальнений шаблон шахрая.

Ключові слова: виявлення шахрайства, виявлення аномалій, інсталювання мобільних додатків, інтелектуальний аналіз даних, інформаційна технологія, інтелектуальні системи.

Аннотация. В работе предложена информационная технология построения интеллектуальных систем обнаружения мошенничества при инсталлировании мобильных приложений, которую желательно использовать при разработке такого класса систем. Осуществлено интеллектуальную обработку имеющихся данных по пользователю, на основе которой предложено шкалирование не по значению признака, а по конечной информации, которую несет признак по пользователю. Предложена система с интеллектуальной составляющей – формированием базы знаний, которая позволит определить мошенников, и в которую будут включаться правила анализа аномалий, причем так, чтобы появление новой аномалии в данных позволяло создать новое правило. Такая база знаний может расширяться из-за возможности появления нового вида аномалии в данных (мошенничества). Полученный набор правил, в дальнейшем на основе разработанных в работе алгоритмов позволит создать обобщенный портрет мошенника, отметив даже новые и неизвестные экспертам мошеннические свойства. Отнесение подозрительных пользователей к классу мошенников или органических происходит с использованием нечеткой логики. Благодаря предложенной интеллектуальной обработке имеющихся данных о пользователях, шкалирования по конечной информации, которую несет признак и созданию баз знаний развивающихся предложена информационная технология позволяет построить интеллектуальные системы, которые будут иметь возможность адаптироваться к появлению новых видов мошенничества. В соответствии с задачами, которые должны решать такие интеллектуальные системы, предложено их структуру: подсистема обнаружения характеристик пользователя; подсистема преодоления разнородности данных; подсистема тренировки классификационной модели; подсистема классификации; подсистема формирования базы данных мошенников; подсистема формирования базы знаний (для выявления мошенников); подсистема интеллектуального анализа данных и формирования шаблонов пользователей; подсистема прогнозирования обобщенного шаблона мошенника. Предложенная информационная технология построения интеллектуальных систем позволяет обрабатывать разноформатные входные данные, что в процессе дает возможность сформировать обобщенный шаблон мошенника.

Ключевые слова: определение мошенничества, определение аномалий, инсталлирование мобильных приложений, интеллектуальный анализ данных, информационная технология, интеллектуальные системы.

Abstract. Information technology for the construction of intelligent systems for detecting fraud during mobile applications installations, which is desirable to use in developing such a class of systems, is proposed in this paper. The intelligent processing of available data by the user is done. The scaling which is based not on the value of the feature, but on the end-point information of the feature, is proposed based on this intelligent processing of the data. A system with an intellectual component - the formation of a knowledge base that will allow fraudsters to be identified and which will include anomaly analysis rules - was proposed, so that the emergence of a new anomaly in the data allows for the creation of a new rule. Such knowledge base can be expanded due to the possibility of an emergence of a new kind of anomaly in data (fraud). The received set of rules will allow creating a generalized fraudster's fingerprint, noting even the new and unknown for experts fraudulent patterns, based on the algorithms developed in the work. The classification of suspicious users to a class of fraudsters or organic users is made using fuzzy logic. The information technology for the construction of intelligent systems that will be able to adapt to the emergence of new types of fraud is proposed based on the proposed intelligent processing of available user data, the scaling by end-point information, and the development of knowledge bases. According to the tasks which should be solved by such intelligent systems, their structure is proposed: subsystem of user data characteristics identifying; subsystem of overcoming heterogeneity; subsystem of classification model training; subsystem of classification; subsystem of fraudsters database formation; subsystem of knowledge base (for detecting fraud) formation; subsystem of data mining and user patterns formation; subsystem of general fraudster fingerprint prediction. The proposed information technology for the construction of intelligent systems allows processing of various input data, which in the process gives the opportunity to form a generalized fraudster fingerprint.

Keywords: fraud detection, anomaly detection, mobile application installation, data mining, information technology, intellectual systems.

DOI: <https://doi.org/10.31649/1999-9941-2019-44-1-4-16>.

Т. Д. Польгуль, 2019

Вступ

У зв'язку з появою на ринку величезної кількості мобільних додатків, якими користуються мільярди користувачів, компанії-розробники мобільних додатків користуються послугами маркетингових кампаній з метою залучення користувачів саме до їхнього додатку. Саме така потреба у маркетингових кампаніях стала однією з причин появи шахраїв та їх шахрайських способів інсталювання мобільних додатків. Шахраї у свою чергу приводять компаніям необхідну кількість «користувачів» та отримують за це відповідну грошову винагороду, проте їхні «користувачі» ніколи не повертаються у мобільний додаток, оскільки є фейковими, ми ж їх називатимемо шахрайськими.

На наш час вже існують такі відомі види шахрайства при інсталюванні додатків, як мобільне викрадення (mobile hijacking), кліковий спам (click spamming), ферми дій (action farms) [1-2], а також методи та системи виявлення шахрайства при інсталюванні мобільних додатків такі як Fraudlogix та Kraken, Adjust, Kochava та TCM Attribution Analytics, Protect360 від AppsFlyer, FraudScore та AppMetrica, що згадані у роботі [3]. Проте необхідно зазначити, що лише остання пара використовує інтелектуальну складову, серед них AppMetrica просто опирається на FraudScore та використовує їх алгоритми та API, але навіть вказані системи-аналоги виконують рейтингування користувачів на основі не всіх, а вибіркового вхідних даних, тому наявне упущення шахраїв системою [4]. Інші вказані системи використовують відомі бази з шахрайськими даними (наприклад, IP-адресами), що також призводить до упущення шахраїв, що мають інші властивості, шаблони, поведінку.

Очевидно, що причиною вищевказаних недоліків системи є відсутність єдиної концепції виявлення шахрайства на основі всіх наявних даних. Також, недоліком існуючих систем є те, що вони розпізнають лише відомі види шахрайства і не можуть розпізнавати нові шахрайські шаблони. А в сучасному світі важливою є можливість системи адаптуватись, тому необхідним є створення інтелектуальної системи, що матиме змогу самонавчатися.

Тому й виникає необхідність створення інформаційної технології побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків, яка б відстежувала та визначала шаблони шахраїв, що непомітні людині. Для вирішення поставленої мети в даній роботі запропонована інформаційна технологія побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків.

Мета

Метою статті є створення інформаційної технології побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків, особливістю якої була б можливість адаптуватись до появи нових видів шахрайства.

Задачі дослідження

У процесі розробки інформаційної технології побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків виникли наступні задачі:

- виявлення, аналіз та використання наявних даних різних шаблонів, розмірності, метрик методами класифікації та шкалювання;
- інтелектуальна обробка даних про користувачів методами класифікації, коефіцієнтів схожості та нечіткої логіки;
- класифікація користувачів з використанням моделі глибоких нейронних мереж;
- створення баз даних, що містять характеристики шахраїв не лише людини, а і різних програмних ботів, та баз знань з набором нечітких правил визначення шахраїв. При чому такі бази даних та бази знань повинні розвиватися в залежності від нових даних та нових шахраїв з метою створення узагальненого портрету шахрая.

Розв'язання вище перерахованих задач потребує розробки нових моделей, методів, алгоритмів та засобів і програмного забезпечення, що дозволить створити інформаційну технологію побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків, включаючи розробку структури, методів обробки даних та алгоритмів функціонування таких систем.

Розглянемо вирішення кожної задачі для побудови інформаційної технології побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків та проаналізуємо її ефективність на тестовій системі.

Визначення поняття шахрайства

Спочатку розглянемо, в чому полягає особливість систем виявлення шахрайства. Зазвичай результатом роботи таких систем є таблиця рейтингування користувачів, яка в процентному відношенні показує, відноситься користувач до шахрая чи ні, так наприклад працює система-аналог FraudScore [5]. Але як оцінювати користувача, який в такій таблиці має відсоток 49, чи є він шахраєм чи ні, чи система підозрює його? Тобто така таблиця дає достатньо нечітку інформацію, за результатом якої складно приймати

рішення, визначати такого користувача шахраєм чи ні. Тому для початку необхідно дати визначення поняття «шахрайство».

На наш погляд шахрайство можна розглядати як аномалію в даних. Розглянемо відоме поняття «аномалія в даних» у сфері інформаційних технологій, визначення якого представлені у роботі [6]. Так, вчені з університету Мінесота визначають у [7], що аномалія – це шаблон даних, який не відповідає визначеному поняттю нормальної поведінки (заданому шаблону). При цьому аномалії можуть бути наявними у вхідних наборах даних систем прийняття рішень та систем штучного інтелекту через неувважність персоналу, який вносив ці дані, через наявність похибок та некоректну роботу системи збору даних або ж через навмисні дії шахраїв (іншими словами – шахрайство). Наявність аномалій в даних приводить до помилок в процесі прийняття рішень, так наприклад:

- неправильне визначення діагнозу у медичних системах прийняття рішень та системах штучного інтелекту у медичній сфері, що може коштувати пацієнту життя;
- невизначення механічних несправностей у літаках, машинах тощо перед їх експлуатацією, що також може коштувати життя людям;
- неправильне визначення або невизначення шахрайства у банківських транзакціях. У випадку крадіжки картки та виконання незвичних транзакцій з неї, неправильно навчена система не заблокує шахрайську транзакцію.

Поняття аномалії згадується в літературі з аналізу даних (data mining) як нетипова поведінка, аномальність, викид (outliers), відхилення. Про це також зазначають вчені з Тернопільського національного економічного університету [8]. Існують визначення, які вважаються досить загальними. Так наприклад Хокінз (Hawkins, 1980) у [9] визначає викид (аномалію) як спостереження, яке відхиляється від інших спостережень настільки, що виникають підозри, що він був породжений іншим механізмом. Барнет і Льюїс (Barnet and Lewis, 1994) вказують у [10] на те, що викид (аномалія) є тим, що помітно відхиляється від інших зразків, в яких воно виявляється. Аналогічно, Джонсон (Johnson, 1992) визначає викид (аномалію) як спостереження у наборі даних, яке суперечить іншій частині цього набору даних. Але в даних прикладах не дається чітке визначення поняття аномальності, яке може бути використане для розробки математичних моделей та програмного забезпечення. З іншого боку, простий приклад аномалії у двовимірному просторі представлено на рисунку 1. На ньому показано, що найпростіший приклад аномалії в даних (множина A) – це відокремлена підмножина неаномальних даних X , яка містить свої властивості та підмножина аномальних даних Z , яка характеризується своїми властивостями.

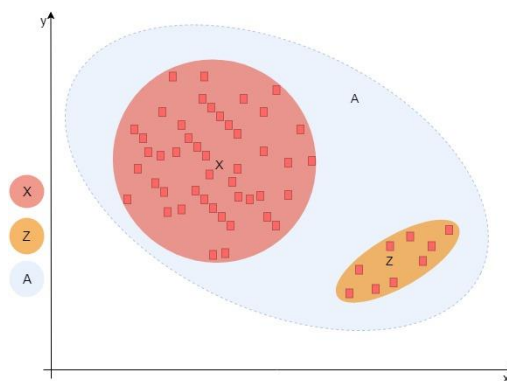


Рисунок 1 – Простий приклад аномалії у двовимірному просторі, де X – підмножина неаномальних даних, Z – підмножина аномальних даних, A – множина усіх вхідних даних

У даній роботі аномалію в даних розглядатимемо як групу (множину) даних $\langle a_1, a_2, \dots, a_n \rangle$, яка входить у множину вхідних даних A , що характеризується множиною властивостей $P(a)$, але виходить за задані межі цих властивостей. У задачі виявлення аномалій у вхідних наборах даних з мобільних додатків, аномальними будемо вважати ті дані (елементи множини), які:

- не мають властивостей $P_1(x), P_2(x), \dots, P_s(x)$, що визначають множину неаномальних даних X ;
- не входять в область гранично допустимих значень множини неаномальних даних X – задамо це властивістю $P2(x)$, яка має вигляд $(x \leq \max_value \text{ і } x \geq \min_value)$;
- не співпадають по розмірності;

– не співпадають по властивостям групи даних.

Шахрайство ж у свою чергу визначимо як навмисне породження аномалії в даних сторонньою особою (шахраєм) або механізмом з певною метою. Аномалії, як і шахрайство, можуть бути наявні у всіх наборах даних, а отже й у всіх областях, з якими працюють системи прийняття рішень та системи штучного інтелекту. Тому на наш погляд більш вдалим означенням шахраїв при розробці такого класу систем – це визначати наявність шахраїв як наявність аномалій в масивах вхідних даних. Проте як же визначати аномалії в даних? Спочатку розглянемо дані, які використовуються в системі.

Аналіз вхідних даних

Детальний аналіз даних проведений в роботі [6] показав, що дані в таких системах є різнорідними, а саме – різних шаблонів, метрик, розмірностей. На рис. 2 представлені всі дані, які використовуються в такому класі систем. Дані згруповані відносно груп подій, на рис. 3 всі наявні для такого класу систем дані зведено до вигляду таблиці і показано, що ці дані різняться не лише за метриками, розмірностями і шаблонами, але також є як якісні, кількісні дані, так і масиви якісних і кількісних даних, тому зрозуміло, що аналіз даних – це дуже складна задача.

Під різнорідністю розуміється, що усі дані, а саме дані з різних класів, неможливо порівняти між собою. Також слід зазначити, що серед наявних даних таких систем є не лише якісні і кількісні дані, але й масиви якісних та кількісних даних. Давайте поглянемо, які дані є (рис. 2, 3).

З рис. 3 також видно, що всі дані є різнорідними, а так як працювати з такими даними складно, багато існуючих систем, методів та моделей відкидають, наприклад, масиви якісних даних чи дані, всі значення яких завчасно невідомі тощо. Так наприклад, кожен з користувачів мобільного додатку має такий якісний параметр як IP-адресу – це і є однією з характеристик, якою часто нехтують. Зазначимо, що деякі з систем перевіряють наявність поточної IP-адреси у відомій базі даних з шахрайськими IP-адресами, але не подають її у якості ознаки (feature) в систему інтелектуального аналізу даних. Це відбувається через ряд причин: моделі інтелектуального аналізу даних в основному працюють лише з числовими значеннями; для перетворення якісних даних у кількісні зазвичай використовується метод one-hot encoding [11], але для його використання необхідна завчасно відома множина можливих значень ознак (feature), у випадку з IP-адресою – завчасно невідома вся множина IP-адрес майбутніх користувачів мобільного додатку. При цьому, можливо згенерувати всі можливі значення IP-адрес версій протоколів IPv4 та IPv6, проте це призведе до зберігання величезної кількості надлишкової інформації, що значно погіршить швидкість та ефективність роботи системи. Тому зазвичай такі дані відкидаються і не приймають рішення у процесі прийняття кінцевого рішення – користувач шахрай чи ні. Але ж чим більша кількість вхідних даних, тим більше залежностей, кореляцій можна з них виділити та тим більше різних шаблонів шахраїв можна буде помітити. Тобто чим більше даних для прийняття рішень, тим вища точність системи. Тому перед авторами постало питання як правильно та ефективно використовувати усі різнорідні дані про користувача, оскільки практично всі системи класифікації працюють з однорідними даними.

Зазвичай в різних областях науки і техніки для аналізу таких даних використовують різні методи шкалювання, так наприклад:

- за допомогою систем правил, побудованих з використанням нечіткої логіки;
- нормалізацією даних, що використовується наприклад у задачах статистичної обробки даних;
- звичайним шкалюванням вимірвальних пристроїв.

Проте, як можна для даних про користувачів при інсталюванні мобільних додатків, що представлені на рис. 2, 3, провести шкалювання? Відомо, що IP-адреса може мати вигляд наприклад такий як «127.0.0.1», «192.168.5.1». Нормалізувати дані такого типу неможливо. Аналогічно недоцільно використовувати систему правил для даних такого типу. Оскільки для того, щоб взяти до уваги всі ці дані, необхідно сформулювати 4–12 правил, що суттєво ускладнює процес аналізу. Отже, серед вказаних трьох варіантів залишається шкалювання. Проте на думку авторів при аналізі таких даних традиційне шкалювання всього набору даних не є можливим, оскільки значення у всіх цих даних різне (число, категорія якісних даних, масиви кількісних чи якісних даних), а інформація, яку вони несуть, однозначно визначає чи дана ознака характеризує шахрая чи має властивості органічного користувача. Оскільки важливим є здійснити не лише рейтингування користувача, але й зазначити причину, чому даного користувача помітили шахраєм, що є важливим при розгляді судових позовів, в яких необхідно чітко наводити аргументи. Так наприклад, це одна з найвагоміших причин, чому безпілотні автомобілі ще не доступні у продажу, адже в досліджуваній області таке обґрунтування є обов'язковим [6]. Тому в роботі [3] був запропонований метод шкалювання даних про користувача по цінності інформації, яку вони несуть.

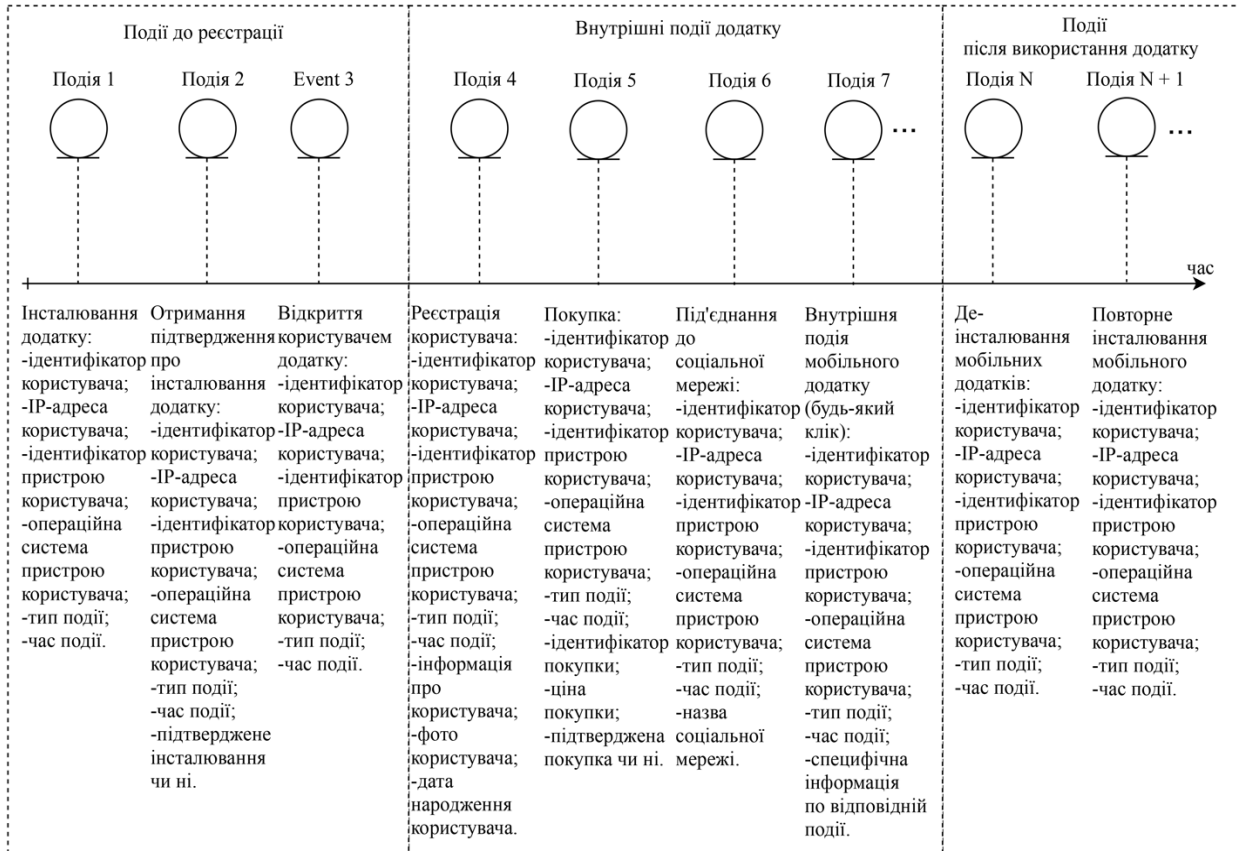


Рисунок 2 – Приклад вхідних даних про користувача в системах виявлення шахрайства при інсталюванні мобільних додатків

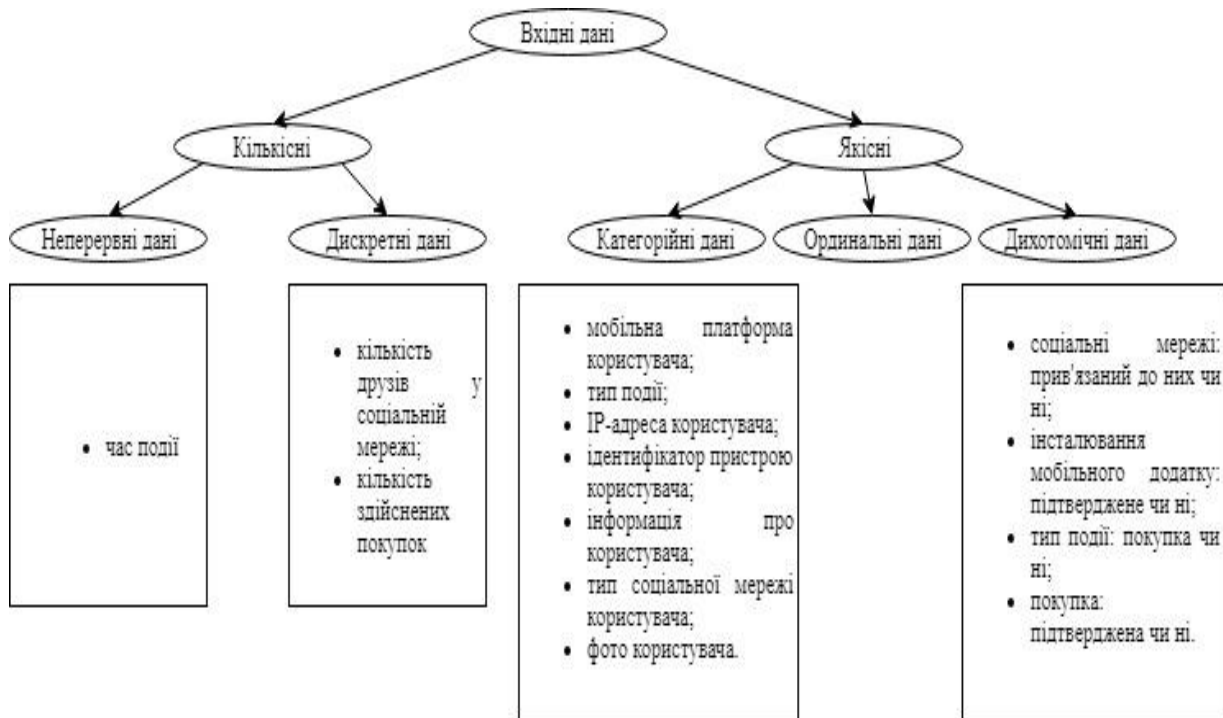


Рисунок 3 – Класифікація різномірних вхідних даних в системах виявлення шахрайства при інсталюванні мобільних додатків

Отже, для подолання різномірності даних використовується шкалювання по цінності інформації, яку несуть ці дані, що означає перетворення всіх даних (якісних і кількісних) до єдиної бінарної шкали зі значеннями 0 та 1 в залежності не від значення, а від інформації, яку несуть ці дані. Наприклад, розглянемо шкалу для переведення ознаки «IP-адреса» до бінарного значення, представлену на рис. 4. Після шкалювання за даною ознакою, деяких користувачів можна однозначно віднести до шахраїв. Вважатимемо, що значення 0 на шкалі означатиме, що користувач є шахраєм за даною ознакою, а значення 1 на шкалі означатиме, що користувач є органічним (тобто не є шахраєм) за даною ознакою. Це є особливістю запропонованого методу шкалювання різномірних даних.

Шкалювання за IP-адресою

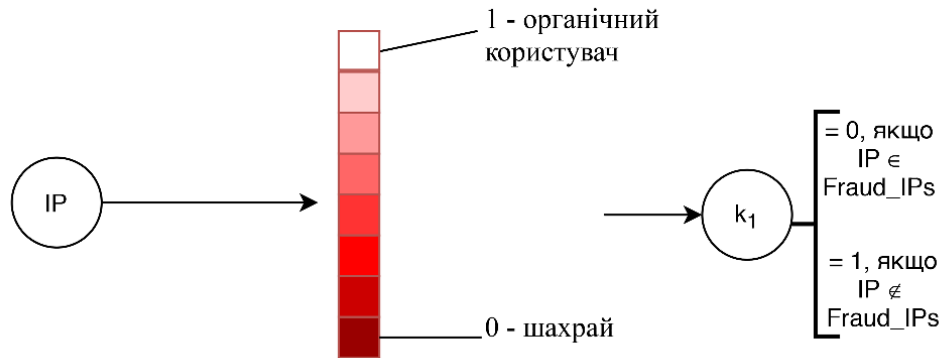


Рисунок 4 – Шкалювання за IP-адресою

Однак, при використанні такого шкалювання не всіх користувачів можна однозначно віднести або до шахраїв, або до органічних, оскільки ця IP-адреса може бути відсутня в базі даних, тому для таких користувачів необхідно додатково використати інтелектуальну обробку даних.

Інтелектуальна обробка наявних даних про користувачів

В залежності від існуючих даних і при використанні запропонованого методу шкалювання в роботі було розроблено 17 шкал, особливістю кожної шкали є те, що вони бінарні. Кількість шкал визначалася як кількістю вхідних даних, так і результатами експертного оцінювання, розглянутого у роботі [6], на основі якого розроблений метод подолання різномірності даних в системах, що розглядаються. Шкали у свою чергу відповідають конкретній інформації про користувача, так наприклад, важливими є IP-адреса користувача, покупки користувача, інформація про під'єднання користувача до соціальних мереж, час інсталювання мобільного додатку користувачем, час між внутрішніми подіями додатку у користувача тощо.

Для того, щоб кожен з даних ознак представити у бінарному вигляді, було сформовано коефіцієнти, за допомогою яких можна визначити значення цінної інформації за кожною із шкал. Тобто з використанням розроблених шкал і проводиться аналіз даних, в результаті якого сформовано 17 коефіцієнтів [3], які використовуються в алгоритмах прийняття рішень при виявленні шахрайства. З використанням запропонованих коефіцієнтів і кількісних, і якісних, і масиви кількісних та якісних даних шкалюються до однорідних бінарних значень без втрати інформації, оскільки шкалювання іде по кінцевій цілі.

Особливістю кожного з запропонованих коефіцієнту є те, що кожен з них відповідає одному типу даних та може приймати значення 0 або 1, що дозволяє від різномірних даних перейти до однорідних даних, тобто і кількісних, і якісних дані шкалюються до однорідних бінарних значень без втрати інформації, оскільки шкалювання іде по кінцевій цілі. Це є важливою особливістю, оскільки після перетворення усіх наявних даних до таких коефіцієнтів, буде можливість подати отримані однорідні дані до будь-якої моделі класифікації. Таким чином, отримаємо можливість використання будь-якої моделі класифікації з використанням усіх вхідних даних, що на даний момент є неможливим. Також, буде можливість відстежити, який з коефіцієнтів найбільше вплинув на віднесення користувача до певного класу, що дасть можливість дати відповідь на питання, чому інтелектуальна система прийняла саме таке рішення.

Для прикладу, розглянемо деякі із запропонованих коефіцієнтів: k_2 (куплена / не куплена покупка) – якщо кількість зроблених користувачем покупок $\geq K_{2_min}$, то k_2 попередньо рівне 1 та означає, що користувач не є шахраєм. Якщо кількість покупок $< K_{2_min}$, то k_2 попередньо рівне 0.5, що означає, що

користувач є підозрілим. Коефіцієнт K_{2_min} у даній роботі визначається на основі експертного опитування. Якщо користувач зробив покупку, яка недоступна для нього, то k_2 попередньо рівне 0 та означає, що користувач є шахраєм; k_1 (кількість кліків з одного пристрою за хвилину) – важливий коефіцієнт при виявленні шахрайства, проте маючи лише його, не можна однозначно виявити шахрая (аномалію в даних); а також k_8 (кількість друзів у соціальній мережі) – якщо користувач прив'язаний до соціальної мережі та в нього є достатня кількість друзів, а саме – $(K_{8_max} \times K_{8_opt}; \infty)$, то можна зробити перевірку на імена (чи друзі реальні) і фото друзів (аналогічно до визначення коефіцієнта k_{15}).

Деякі з коефіцієнтів дозволяють однозначно визначити користувача, що дозволяє сформувати базу даних шахраїв та базу знань з характеристиками шахраїв, а деякі коефіцієнти не дозволяють однозначно визначити клас користувача. Саме такий аналіз даних у процесі тестування розробленої системи, що відповідає основним положенням розглядуваної концепції дозволив здійснити розбиття коефіцієнтів на такі групи з використанням алгоритму 1, що детально представлений у роботі [6]:

– перша група охоплює коефіцієнти, які дозволяють провести попередній аналіз даних, а саме однозначно з множини користувачів визначити шахрайських користувачів, органічних та підозрілих. Дозволяє зробити первинну вибірку на основі Decision Tree. Так наприклад у першу групу входить 13 коефіцієнтів, більшість з яких представлено у роботі [6]. Серед коефіцієнтів першої групи є наприклад k_2 (куплена / не куплена покупка), який розглянуто вище. Тобто шкали першої групи дозволяють однозначно визначити клас користувача, що дозволить сформувати базу даних та базу знань з відомими визначеними користувачами в подальшому. Приклад шкал першої групи зображено на рис. 5 [3];

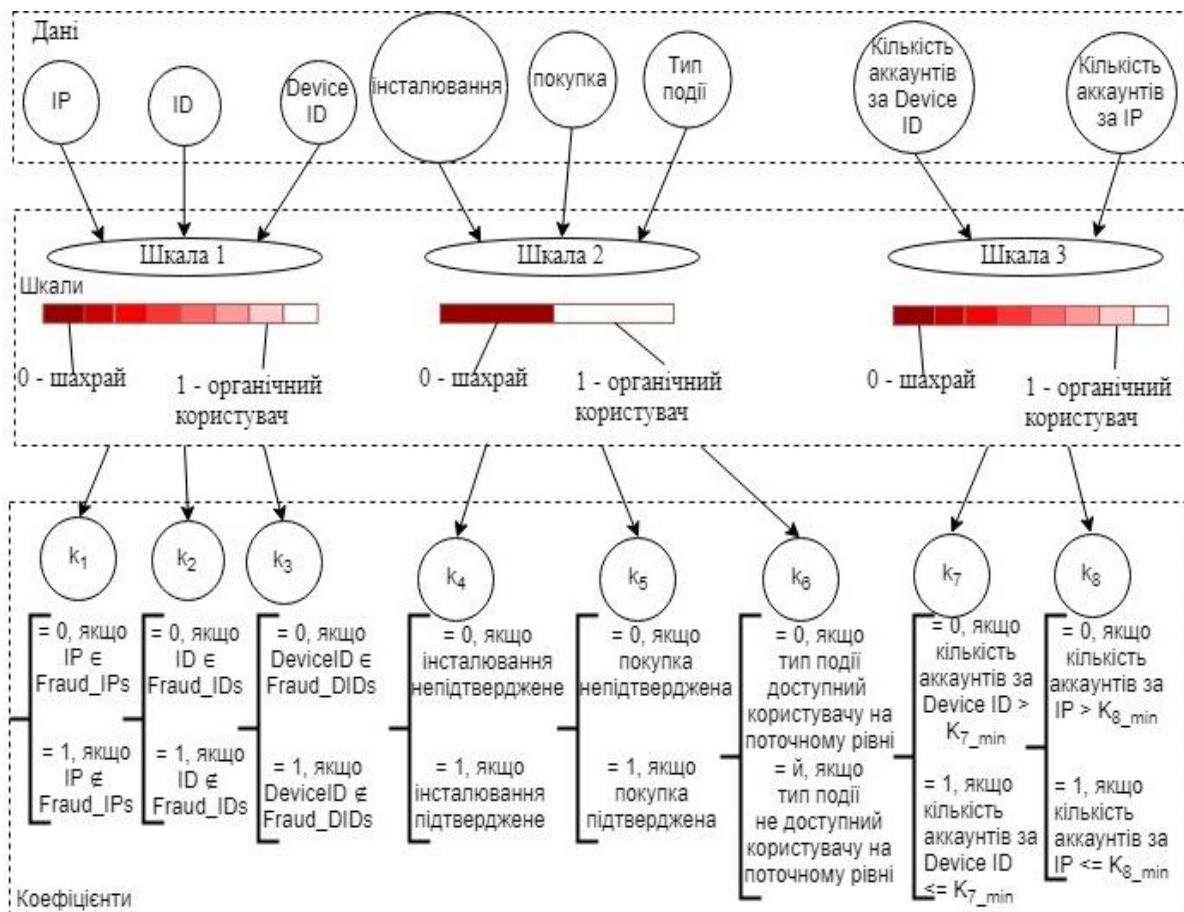


Рисунок 5 – Приклад шкал першої групи

– друга група охоплює коефіцієнти, за якими неможливо зробити первинний аналіз на основі дерева рішень (Decision Tree). Проте, на основі баз даних шахраїв, органічних та підозрілих користувачів та баз знань, сформованих на основі коефіцієнтів з першої групи, можна визначити коефіцієнти схожості усіх користувачів із визначеними користувачами з сформованої бази даних за кожною із характеристик дру-

гої групи. Так, до другої групи відноситься 6 коефіцієнтів, більшість з яких розглянуто у роботі [6]. Серед них можна виділити наприклад k_1 (кількість кліків з одного пристрою за хвилину); а також k_8 (кількість друзів у соціальній мережі). Слід зазначити, що при визначенні коефіцієнтів другої групи необхідно перевірити усі інші показники. Коефіцієнт K_{11_min} визначається на основі експертного опитування. Модель шкалювання коефіцієнтів другої групи зображено на рис. 6 [3].

Результатом шкалювання за першою групою представлена таблиця, фрагмент якої представлено у вигляді табл. 1. На основі таких таблиць створюється база даних шахраїв і тому перший етап – це визначення відомих шахраїв по цим таблицям.

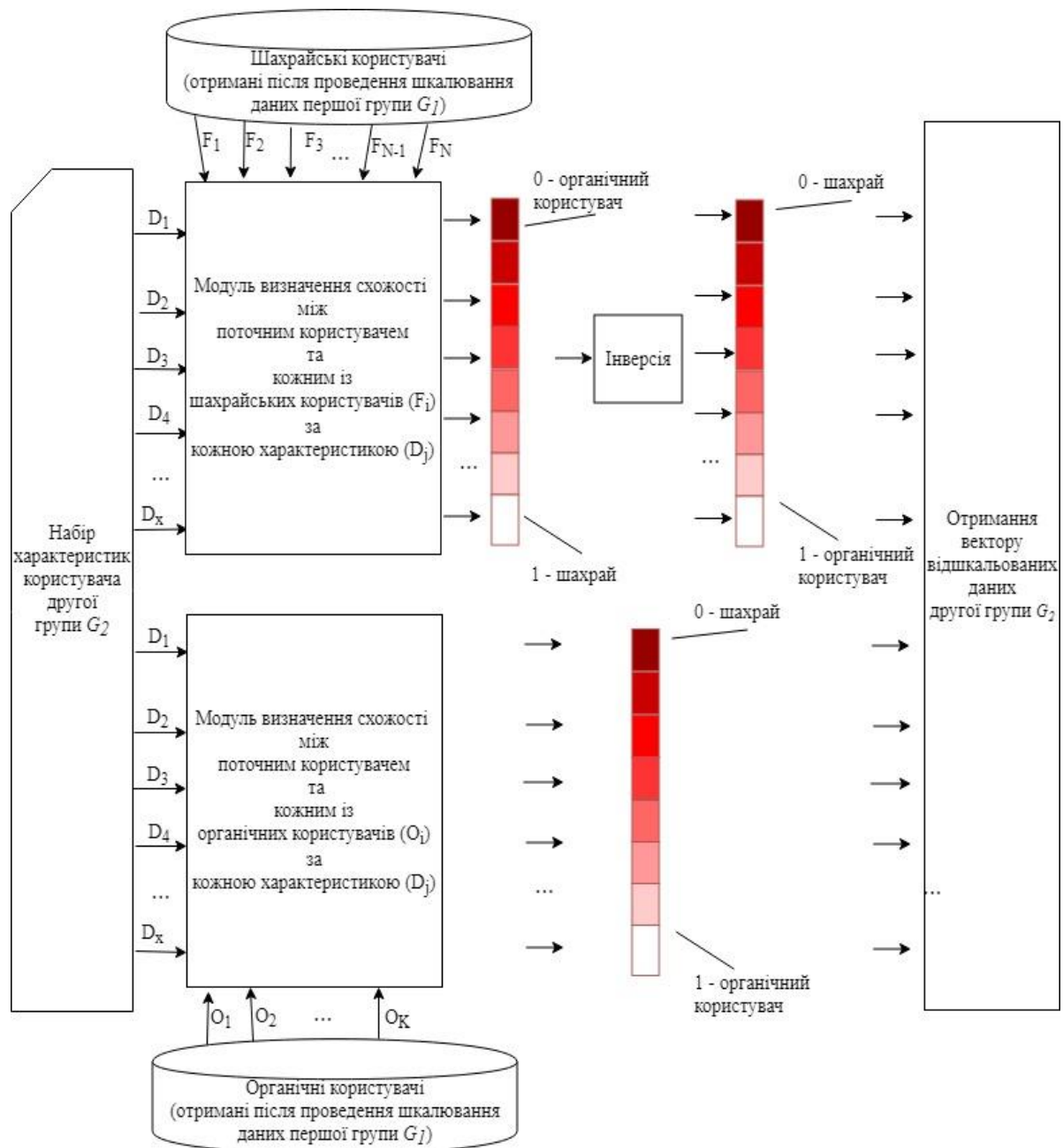


Рисунок 6 – Модель шкалювання даних другої групи

У процесі шкалювання першої групи характеристик і формування коефіцієнтів та формування баз даних і баз знань, можна виділити множини невизначених користувачів. Для цих множин і здійснюється шкалювання за другою групою коефіцієнтів, а саме, здійснюється визначення значень коефіцієнтів другої групи, використовуючи формули визначення коефіцієнтів подібності користувачів.

Таблиця 1 – Приклад принципу роботи запропонованого методу шкалювання

Ознака	До шкалювання	Після шкалювання	Коефіцієнт	Розпізнавання шахрайства
IP-адреса	127.0.0.1	1	$IP \notin FRAUD_DeviceID$	органічний користувач
ID пристрою	35 577678 5678735	0	$DeviceID \in FRAUD_DeviceID$	шахрай
ID покупки підтверджена чи ні	6cf9094a-6fbf-4898-bb3e-0cd895b1cafb	0	$PurchaseID.isConfirmed = false$	шахрай

Наступним етапом є визначення класів невизначених користувачів. Для цього для кожного з визначених коефіцієнтів другої групи з використанням алгоритму 2, що запропонований у роботі [6], виконуються наступні дії:

1. Визначаються коефіцієнти подібності невизначених користувачів з шахраями із сформованої бази даних, що утворює множину коефіцієнтів, значення яких від 0 до 1.
2. Визначаються коефіцієнти подібності невизначених користувачів з органічними користувачами із сформованої бази даних.
3. Визначаються коефіцієнти подібності невизначених користувачів з підозрілими користувачами із сформованої бази даних.
4. Здійснюється об'єднання отриманих множин значень коефіцієнтів в одну множину однорідних значень.

Зазначимо, що важливим є вибір коефіцієнту подібності, більш детально крок знаходження коефіцієнту подібності описано в роботі [3]. У даній роботі слід відмітити, що значення коефіцієнтів подібності належить проміжку $[0;1]$. Значення 1 означає, що користувачі ідентичні за даною ознакою (feature), 0 у свою чергу означає, що користувачі не мають нічого спільного за даною ознакою (feature). Так, наприклад, розглянувши ознаку по користувачам «час між подіями», матимемо множину часу між подіями поточного користувача $T_u = \{t \mid t \geq 0\}$ та множини часу між подіями кожного із однозначно визначених шахраїв $T_i = \{t \mid t > 0\}$. Маючи дві множини не бінарних, проте однорідних даних T_u та T_i , застосуємо відповідний коефіцієнт подібності користувачів. Для множин такого типу, зокрема для множин, що містять інформацію по ознаці «час між подіями», в роботі обрано коефіцієнт Танімото

$K_T(T_u, T_i)$ [1, 4, 12], який визначається як $K_T(T_u, T_i) = \frac{N_c}{N_a + N_b - N_c}$, де N_c – кількість спільних

для множин T_u та T_i елементів, N_a – кількість елементів у множині T_u , N_b – кількість елементів у множині T_i . У свою чергу, для множин бінарних даних, таких як множина з бінарними значеннями по кожному з існуючих типів подій мобільного додатку, де 0 означатиме, що користувач не використовував таку подію, а 1 означатиме, що використовував, коефіцієнти подібності користувачів визначаються з використанням коефіцієнту косинусної схожості $K_{\cos}(A_1, A_2)$ [1, 3, 12], який найефективніше працює з

бінарними даними. У свою чергу $K_{\cos}(A_1, A_2) = \cos(A_1, A_2) = \frac{(A_1 \cdot A_2)}{|A_1| \cdot |A_2|}$, де A_1, A_2 – множини з ви-

ще вказаними бінарними даними поточного користувача та шахрайського користувача відповідно.

Отримавши множину однорідних значень всіх наявних даних, отриманих з використанням запропонованих шкал, використаємо етап класифікації даних з використанням відомої моделі класифікації (екстремальне градієнтне підсилення XGBoost, випадковий ліс – random forest, глибокі нейронні мережі) з метою виявлення даних, які однозначно визначають шахраїв, і даних, які однозначно визначають органічних користувачів.

Створення баз знань, що розвиваються

З метою підвищення ефективності, швидкодії та точності інтелектуальних систем виявлення шахрайства недостатньо лише здійснити класифікацію користувачів на класи «шахрай» чи «органічний», важливим є ще використання баз знань на основі запропонованих вище методів, моделей та алгоритмів.

Крім того, слід зазначити, що в сучасних системах виявлення шахрайства є свої проблеми, однією з яких є відсутність інтелектуального аналізу даних, що не дозволяє таким системам адаптуватися до нових видів шахрайства. Для того, щоб системи мали змогу адаптуватися до нових видів та самонавчатися з використанням алгоритмів прогнозування, автором роботи пропонується система з інтелектуальною складовою – формуванням бази знань, яка дозволить визначити шахраїв, та в яку включатимуться правила аналізу аномалій, при чому так, щоб поява нової аномалії в даних дозволяла створити нове правило. Тобто така база знань може розширюватись через можливість появи нового виду аномалії в даних (шахрайства). Отриманий набір правил, що у подальшому на основі розроблених в роботі алгоритмів дозволить створити узагальнений портрет шахрая, відзначивши навіть нові та невідомі експертам шахрайські властивості. Віднесення підозрілих користувачів до класу шахраїв або органічних відбувається з використанням нечіткої логіки.

Зазначимо, що зв'язок між функціями належності входу i_j з бази знань можна визначити нечіткими логічними рівняннями, сформованими у базі знань, виду:

$$\mu^{d_j}(y) = b_{j1} [\mu^{j1}(i_1) \wedge \mu^{j1}(i_2) \wedge \dots \wedge \mu^{j1}(i_n)] \vee b_{j2} [\mu^{j2}(i_1) \wedge \mu^{j2}(i_2) \wedge \dots \wedge \mu^{j2}(i_n)] \dots \\ b_{jp} [\mu^{jp}(i_1) \wedge \mu^{jp}(i_2) \wedge \dots \wedge \mu^{jp}(i_n)]$$

$j = \overline{1, m}$, які можна спростити до виразу $\mu^{d_j}(y) = \max_{p=1, k_j} \{a_{jp} \min_{i=1, n} [\mu^{jp}(i_j)]\}$, $j = \overline{1, m}$, де

b_i^p – нечіткий терм. Нечіткий терм у свою чергу визначається як $b_i^p = \int_{i_j}^{\bar{i}_j} \frac{\mu^p(i_j)}{i_j}$, де $\mu^p(i_j)$ – функція належності входу i_j нечіткому терму b_i^p , $p = k1$, $i = \overline{1, n}$, $j = \overline{1, m}$. Слід зазначити, що такі бази знань повинні розвиватися в залежності від нових даних та нових шахраїв з метою створення узагальненого портрету шахрая.

Класифікація користувачів з використанням глибоких мереж

Наступним етапом в методиці виявлення шахрайства є класифікація отриманої вибірки користувачів на органічних та шахрайських. Але оскільки усі моделі класифікації працюють з однорідними даними, то розробка методу подолання різномірності даних була необхідною. Тому після етапу подолання різномірних даних, отримавши відшкальовані та нормалізовані однорідні дані у межах від 0 до 1, може бути використана будь-яка з відомих моделей класифікації. З точки зору авторів для розв'язання такої задачі зручно використовувати моделі класифікації з використанням глибоких нейронних мереж (DNN – deep neural network). Необхідно зазначити, що використання моделей класифікації для поділу користувачів на два визначених класи є відомим та поширеним підходом. На наш погляд для розв'язання такої задачі достатньо використовувати DNN з трьома прихованими шарами.

Маючи множину однорідних значень, здійснимо тренування класифікаційної моделі на вибірці з розробленого мобільного додатку [1, 13-14]. Необхідно зауважити, що для коректного навчання та оцінки системи, а також для уникнення перенавчання системи, необхідно мати три набори даних: тренувальний, перевірочний (валідаційний) та контрольний. Також необхідно відзначити, що насамперед розроблена система повинна бути наділена прогностичною здатністю та добре узагальнюватися на нових для неї даних. Контрольна вибірка містить 56962 записи, 56657 з яких відповідають органічним користувачам, а 305 відповідають користувачам-шахраям. Вибіркі помічені, проте мітка використовується лише для подальшої оцінки адекватності моделі. У якості класифікаційної моделі обрано глибокі нейронні мережі із трьома прихованими шарами. На рис. 7 представлено побудовано матрицю невідповідності з використанням мови Python для оцінки адекватності реалізованої класифікаційної моделі. З рисунку 76 видно, що практично 100% органічних користувачів та 80% користувачів-шахраїв визначено правильно.

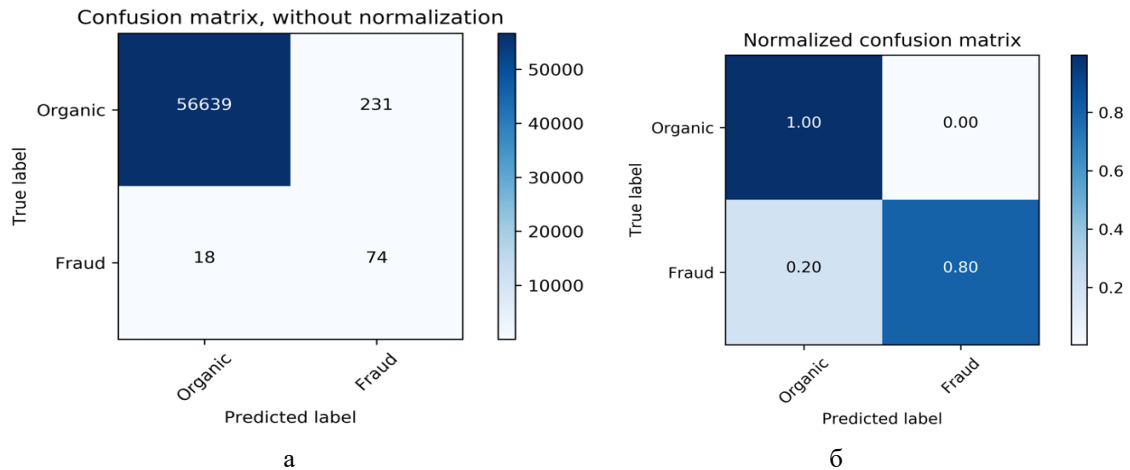


Рисунок 7 – Матриця невідповідності контрольної вибірки: а – без нормалізації, б – нормалізована

На основі запропонованих в роботі методів, моделей та алгоритмів була розроблена узагальнена структура інтелектуальної системи виявлення шахрайства (рис. 8), що складається з наступних підсистем: підсистема виявлення характеристик користувача; підсистема подолання різномірності даних; підсистема тренування класифікаційної моделі; підсистема класифікації; підсистема формування бази даних шахраїв; підсистема формування бази знань (для виявлення шахраїв); підсистема інтелектуального аналізу даних та формування шаблонів користувачів; підсистема прогнозування узагальненого шаблону шахрая. Слід зазначити, що це є базовий набір підсистем запропонованої узагальної структури інтелектуальної системи виявлення шахрайства та можливе розширення для прогнозування, передбачення, коли і звідки прийде наступний шахрай.

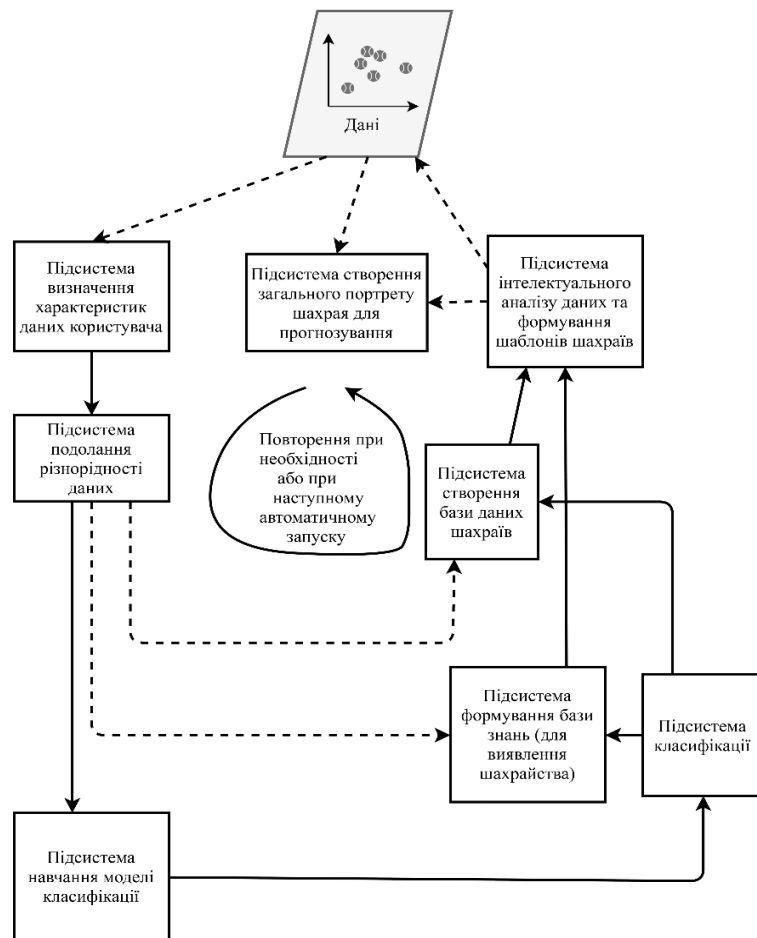


Рисунок 8 – Структура інтелектуальної системи виявлення шахрайства при інсталюванні мобільних додатків

Висновки

Отже, у роботі запропоновано інформаційну технологію побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків, яка включає:

– запропонований метод аналізу даних, який на відміну від існуючих дозволяє на базі запропонованих шкал подолати різномірність даних та здійснити інтелектуальну обробку наявних даних з використанням запропонованих алгоритмів 1 та 2 (шкалювання першої та другої групи), що дозволило суттєво підвищити точність отриманих результатів прийняття рішень по виявленню шахраїв;

– метод класифікації користувачів системи, який на відміну від існуючих використовує моделі глибоких нейронних мереж та запропонований метод подолання різномірності, що дозволило створити бази знань, що розвиваються, з набором нечітких правил та дозволило здійснювати створення узагальненого портрету шахрая в залежності від нових даних та нових шахраїв;

– проведено оцінку адекватності запропонованої класифікаційної моделі на вибірці з розробленого мобільного додатку [1, 13-14], що показала, що практично 100% органічних користувачів та 80% користувачів-шахраїв визначено правильно.

Усі вище розглянуті метод, модель та алгоритми, розроблені для вирішення виділених на початку статті задач, представляються собою технологію.

Список літератури

- [1] А. А. Яровий, О. Н. Романюк, І. Р. Арсенюк, Т. Д. Польгуль «Виявлення шахрайства при інсталюванні програмних додатків з використанням інтелектуального аналізу даних», *Наукові праці Донецького національного технічного університету. Серія: «Інформатика, кібернетика та обчислювальна техніка»*, № 2 (25), с. 126–131, 2017.
- [2] Т. Д. Польгуль, А. А. Яровий «Визначення шахрайських операцій при встановленні мобільних додатків з використанням інтелектуального аналізу даних», на *Сучасні тенденції розвитку системного програмування. Тези доповідей*, Київ, 2016, с. 55–56.
- [3] Т. Д. Польгуль, А. А. Яровий «Метод подолання різномірності даних для виявлення шахрайства при інсталюванні мобільних додатків», *Вісник СНУ ім. В. Даля – Северодонецьк: СНУ ім. В. Даля*. 2018, № 7 (248), с.60-69, 2018.
- [4] T. Polhul, “Development of an intelligent system for detecting mobile app install fraud”, in *Proceedings of the IRES 156th International Conference*, Bangkok, Thailand, 21st-22nd March 2019, pp. 25-29.
- [5] FraudScore: FraudScore fights ad fraud using Machine Learning [Online]. Available: <https://fraudscore.mobi/>
- [6] T. Polhul, A. Yaroviyi “Development of a method for fraud detection in heterogeneous data during installation of mobile applications”, *Eastern-European Journal of Enterprise Technologies*, № 1/2 (97), 2019. doi: 10.15587/1729-4061.2019.155060
- [7] V. Chandola, A. Banerjee, V. Kumar, “Anomaly Detection: A Survey”, *ACM Computing Surveys (CSUR)*, Volume 41, Issue 3, Article No. 15, New York, NY, USA, July 2009.
- [8] I. S. Ivaskiv “Machine-learning methods in tasks of detection the atypical behavior of complex system”, *Master Thesis*. Ternopil National Economy University, Ternopil, 2017. (Ukr.).
- [9] D. Hawkins, *Identification of Outliers*. Chapman and Hall, 1980.
- [10] V. Barnett, T. Lewis, *Outliers in Statistical Data*, Wiley, 1994.
- [11] A. Géron, *Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, O’Reilly Media, 2017, 574 p.
- [12] А. Г. Кюльян, Т. Д. Польгуль, М. Б. Хазін, «Математична модель рекомендаційного сервісу на основі методу колаборативної фільтрації», *Комп’ютерні технології та Інтернет в інформаційному суспільстві*, с. 226–227, 2012.
- [13] А. А. Яровий, Т. Д. Польгуль, Комп’ютерна програма «Програмний модуль збору даних інформаційної технології» виявлення шахрайства при інсталюванні програмних додатків. *Свідоцтво про реєстрацію авторського права на твір № 76348*. К.: Міністерство економічного розвитку і торгівлі України, 2018.
- [14] А. А. Яровий, Т. Д. Польгуль, Комп’ютерна програма «Програмний модуль визначення схожості користувачів інформаційної технології виявлення шахрайства при інсталюванні програмних додатків». *Свідоцтво про реєстрацію авторського права на твір № 76347*. К.: Міністерство економічного розвитку і торгівлі України, 2018.

References

- [1] A. A. Yaroviyi, O. N. Romaniuk, I. R. Arseniuk, T. D. Polhul «Vyivlennia shakhraistva pry instaliovanni prohramnykh dodatkov z vykorystanniam intelektualnoho analizu danykh», *Naukovi pratsi Donetskoho natsionalnoho tekhnichnoho universytetu. Serii: «Informatyka, kibernetyka ta obchysliualna tekhnika»*, № 2 (25), с. 126–131, 2017.

- [2] T. D. Polhul, A. A. Yarovyι «Vyznachennia shakhraiskyykh operatsii pry vstanovlenni mobilnykh dodatkov z vykorystanniam intelektualnoho analizu danykh», na Suchasni tendentsii rozvytku systemnoho prohramuvannia. Tezy dopovidei, Kyiv, 2016, s. 55–56.
- [3] T. D. Polhul, A. A. Yarovyι «Metod podolannia riznoridnosti danykh dlia vyjavlennia shakhraistva pry instaluiuvanni mobilnykh dodatkov», Visnyk SNU im. V. Dalia – Sievierodonetsk: SNU im. V. Dalia. 2018, № 7 (248), c.60-69, 2018.
- [4] T. Polhul, “Development of an intelligent system for detecting mobile app install fraud”, in Proceedings of the IRES 156th International Conference, Bangkok, Thailand, 21st-22nd March 2019, pp. 25-29.
- [5] FraudScore: FraudScore fights ad fraud using Machine Learning [Online]. Available: <https://fraudscore.mobi/>
- [6] T. Polhul, A. Yarovyι “Development of a method for fraud detection in heterogeneous data during installation of mobile applications”, Eastern-European Journal of Enterprise Technologies, № 1/2 (97), 2019. doi: 10.15587/1729-4061.2019.155060
- [7] V. Chandola, A. Banerjee, V. Kumar, “Anomaly Detection: A Survey”, ACM Computing Surveys (CSUR), Volume 41, Issue 3, Article No. 15, New York, NY, USA, July 2009.
- [8] I. S. Ivaskiv “Machine-learning methods in tasks of detection the atypical behavior of complex system”, Master Thesis. Ternopil National Economy University, Ternopil, 2017. (Ukr.).
- [9] D. Hawkins, Identification of Outliers. Chapman and Hall, 1980.
- [10] V. Barnett, T. Lewis, Outliers in Statistical Data, Wiley, 1994.
- [11] A. Géron, Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, OReilly Media, 2017, 574 p.
- [12] A. H. Kiulian, T. D. Polhul, M. B. Khazin, «Matematychna model rekomendatsiinoho servisu na osnovi metodu kolaboratyvnoi filtratsii», Kompiuterni tekhnolohii ta Internet v informatsiinomu suspilstvi, s. 226–227, 2012.
- [13] A. A. Yarovyι, T. D. Polhul, Kompiuterna prohrama «Prohramnyi modul zboru danykh informatsiinoi tekhnolohii» vyjavlennia shakhraistva pry instaluiuvanni prohramnykh dodatkov. Cvidotstvo pro reiestratsiiu avtorskoho prava na tvir № 76348. K.: Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy, 2018.
- [14] A. A. Yarovyι, T. D. Polhul, Kompiuterna prohrama «Prohramnyi modul vyznachennia skhozhosti korystuvachiv informatsiinoi tekhnolohii vyjavlennia shakhraistva pry instaluiuvanni prohramnykh dodatkov». Cvidotstvo pro reiestratsiiu avtorskoho prava na tvir № 76347. K.: Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy, 2018.

Відомості про авторів

Польгуль Тетяна Дмитрівна – аспірант кафедри Комп’ютерних наук ВНТУ.

T. D. Polhul

**INFORMATION TECHNOLOGY FOR THE CONSTRUCTION
OF INTELLIGENT SYSTEMS FOR DETECTING FRAUD
DURING MOBILE APPLICATIONS INSTALLATION**

Vinnitsia national technical University, Vinnitsia

Т. Д. Польгуль

**ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПОСТРОЕНИЯ
ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ОПРЕДЕЛЕНИЯ
МОШЕННИЧЕСТВА ПРИ ИНСТАЛЛИРОВАНИИ
МОБИЛЬНЫХ ПРИЛОЖЕНИЙ**

Винницкий национальный технический университет, Винница

КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 621.316

О. Д. Азаров, Р. М. Медяний, А. С. Фігас

ВИСОКОЛІНІЙНІ БУФЕРИ Й МАСШТАБАТОРИ НАПРУГИ НА БІПОЛЯРНИХ ТРАНЗИСТОРАХ ІЗ НИЗЬКИМ ВХІДНИМ СТРУМОМ

Вінницький національний технічний університет, м. Вінниця

Анотація. Буферні пристрої і масштабатори напруги широко застосовуються в різноманітних аналого-цифрових системах, коли потрібно узгодити сигнал у вигляді напруги від малопотужного дачача з навантаженням, яке споживає істотно більшу потужність. При цьому буфер напруги характеризується коефіцієнтом передачі напруги близьким до одиниці, а також повинен мати високий вхідний опір і достатню навантажувальну здатність. Масштабатори напруги на відміну від буферів напруги повинні додатково забезпечувати потрібний коефіцієнт передачі підсилення, який може бути істотно більшим за одиницю. Розглянуто схемотехнічні особливості трьох варіантів побудови ядер буферів напруги і масштабаторів напруги. Доведено, що вхідний струм зсуву нуля доцільно зменшувати шляхом застосуванням у вхідних каскадах підсилювальних n - p - n і p - n - p транзисторів, а також складених транзисторів Шиклаї. Статичні і динамічні характеристики буферів напруг і масштабаторів напруги повинні відповідати системним вимогам пристрою. До статичних характеристик треба віднести у першу чергу похибки передатної характеристики масштабу, зсуву нуля та лінійності. Динаміка цих пристроїв визначається АЧХ та перехідною характеристикою. Проаналізовано статичні і динамічні характеристики шляхом комп'ютерного моделювання де показано, що похибки масштабу буферів напруг і масштабаторів напруги не перевищують значень 10 мкВ у діапазоні відповідного сигналу ± 5 В, а похибки лінійності 300 нВ. Отримано перехідну характеристику яка свідчить, що швидкість наростання вихідної напруги буде не гірше 2000 В/мкс. Здійснено порівняння метрологічних характеристик буферів напруги і масштабаторів напруги у вигляді сукупності ядер і вихідних двотактних підсилювачів постійного струму. Доведено, що застосування цих підсилювачів дозволяє істотно (на 3-4 порядки) покращити навантажувальну здатність схем при збереженні рівня вхідного струму зсуву нуля, а також похибок масштабу і лінійності.

Ключові слова: буфер напруги, масштабатор напруги, двотактний підсилювач постійного струму, АЧХ.

Аннотация. Буферные устройства и масштабаторы напряжения широко применяются в различных аналого-цифровых системах, когда нужно согласовать сигнал в виде напряжения от маломощного датчика с нагрузкой, потребляет существенно большую мощность. При этом буфер напряжения характеризуется коэффициентом передачи напряжения близким к единице, а также должен иметь высокое входное сопротивление и достаточную нагрузочную способность. Масштабатором напряжения в отличие от буферов напряжения должен дополнительно обеспечивать нужный коэффициент передачи усиления, который может быть существенно больше единицы. Рассмотрены схемотехнические особенности трех вариантов построения ядер буферов напряжения и масштабатором напряжения. Доказано, что входной ток смещения нуля целесообразно уменьшать путем применением во входных каскадах усилительных n - p - n и p - n - p транзисторов, а также составленных транзисторов Шиклаи. Статические и динамические характеристики буферов напряжений и масштабатором напряжения должны соответствовать системным требованиям устройства. К статических характеристик следует отнести в первую очередь погрешности передаточной характеристики масштаба, смещения нуля и линейности. Динамика этих устройств определяется АЧХ и переходной характеристикой. Проанализированы статические и динамические характеристики путем компьютерного моделирования где показано, что погрешности масштаба буферов напряжений и масштабатором напряжения не превышают значений 10 мкВ в диапазоне соответствующего сигнала ± 5 В, а погрешности линейности 300 нВ. Получено переходную характеристику которая гласит, что скорость нарастания выходного напряжения будет не хуже 2000 В/мкс. Проведено сравнение метрологических характеристик буферов напряжения и масштабатором напряжения в виде совокупности ядер и выходных двухтактных усилителей постоянного тока. Доказано, что применение этих усилителей позволяет существенно (на 3-4 порядка) улучшить нагрузочную способность схем при сохранении уровня входного тока смещения нуля, а также погрешностей масштаба и линейности.

Ключевые слова: буфер напряжения, масштабатор напряжения, двухтактный усилитель постоянного тока, АЧХ.

Abstract. Buffer devices and voltage scalars are widely used in various analog-digital systems, when it is necessary to match the signal in the form of voltage from a low-power sensor to a load, it consumes significantly more power. In this case, the voltage buffer is characterized by a voltage transfer coefficient close to unity, and must also have a high input resistance and sufficient load capacity. The voltage scaler, in contrast to voltage buffers, must additionally provide the necessary gain transfer ratio, which can be substantially more than one. The circuit design features of three variants of the construction of voltage buffer cores and voltage scaling are considered. It is proved that it is advisable to reduce the input zero bias current by using amplifying n - p - n and p - n - p transistors, as well as Shiclay transistors in the input stages. The static and dynamic characteristics of the voltage buffers and the voltage scaler must meet the system requirements of the device. The static characteristics should be attributed primarily to the error of the transfer characteristics of the scale, zero offset and linearity. The dynamics of these devices is determined by the frequency response and transient response. Static and dynamic characteristics are analyzed by computer simulation where it is shown that the scale errors of the voltage buffers and the voltage scaler do not exceed 10 μ V in the range of the corresponding signal ± 5 V, and the linearity errors are 300 nV. A transient response was obtained which states that the slew rate of the output voltage will be no worse than 2000 V/ μ s. A comparison of the metrological characteristics of the voltage buffers and the voltage scaler in the form of a set of cores and output push-pull DC amplifiers. It is proved that the use of these amplifiers allows significantly (by 3-4 orders of magnitude) to improve the load capacity of the circuits while maintaining the level of the input zero bias current, as well as scale and linearity errors.

Key words: voltage buffer, voltage scaler, push-pull DC amplifier, frequency response. DOI: <https://doi.org/10.31649/1999-9941-2019-44-1-17-26>.

Вступ

Буферні пристрої і масштабатори напруги широко застосовуються в різноманітних аналого-цифрових системах, коли потрібно узгодити сигнал у вигляді напруги від малопотужного дачача з наван-

О. Д. Азаров, Р. М. Медяний, А. С. Фігас, 2019

таженням, яке споживає істотно більшу потужність. При цьому буфер напруги характеризується коефіцієнтом передачі напруги близьким до одиниці, а також повинен мати високий вхідний опір і достатню навантажувальну здатність. Масштабатори напруги на відміну від буферів напруги повинен додатково забезпечувати потрібний коефіцієнт передачі підсилення, який може бути істотно більшим за одиницю.

Актуальність

Слід зазначити, що статичні і динамічні характеристики буферів напруг (БН) і масштабаторів напруги (МН) повинні відповідати системним вимогам. До статичних характеристик треба віднести у першу чергу похибки передатної характеристики масштабу, зсуву нуля та лінійності. Динаміка цих пристроїв визначається АЧХ та перехідною характеристикою. Використання біполярних транзисторів порівняно з польовими дозволяє мінімізувати напругу живлення при заданому діапазоні змінення вхідного сигналу і досягти максимального коефіцієнту корненої дії вказаних схем. Водночас треба застосовувати спеціальні заходи щодо компенсації базових струмів, особливо якщо генератор вхідної напруги має збільшений опір, що може призвести до істотного збільшення похибки зсуву нуля. Підвищення точності роботи пристрою досягається за рахунок зменшення похибки лінійності. Лінійність передатної характеристики, а також швидкодію, доцільно забезпечувати застосуванням двотактних схем, а зменшення похибки масштабу – збільшенням коефіцієнта передачі вихідного двотактного підсилювача постійного струму (ДППС). Перспективним у цьому плані є застосування ДППС із внутрішніми балансними зворотними зв'язками [1-4], особливо, якщо сигнал вхідної напруги є двополярним.

Окремо слід зазначити, що під час проектування швидкодіючих інтегральних схем підсилювачі струму мають переваги порівняно з підсилювачами напруги, якщо операції над сигналом будуть виконуватися, представленням у вигляді струму [5-6]. При цьому можна усунути прикладення великих напруг до паразитних ємностей. Навіть у тих випадках, коли треба підсилити напругу, її треба перетворити у струм, підсилити його, а на виході пристрою зсуву перетворити у напругу. Системні вимоги, що висуваються до статичних і динамічних характеристик вузлів аналого-цифрових систем, зокрема, до БН і МН детально розглянуто в [7,8]. Водночас конкретних рекомендацій, а також прикладів щодо побудови вказаних пристроїв у вказаній науково-технічній літературі, а також в інших подібних публікаціях не наведено. У зв'язку з цим тема статті, що присвячена методам побудови високолінійних буферів і масштабаторів напруги із низьким вхідним струмом є актуальною.

Мета

Мета досліджень – аналіз запропонованих методів побудови високолінійних буферів і масштабаторів напруги із низьким вхідним струмом, що відрізняються від відомих застосуванням принципу перетворення струмів, що дає змогу покращити їх статичні й динамічні характеристики.

Задачі

1. Розглянути схемотехнічні особливості побудови «ядер» запропонованих БН і МН;
2. Аналіз їх статичних і динамічних характеристик;
3. Порівняння метрологічних характеристик БН і МН у вигляді сукупності ядер і вихідних двотактних підсилювачів струму.

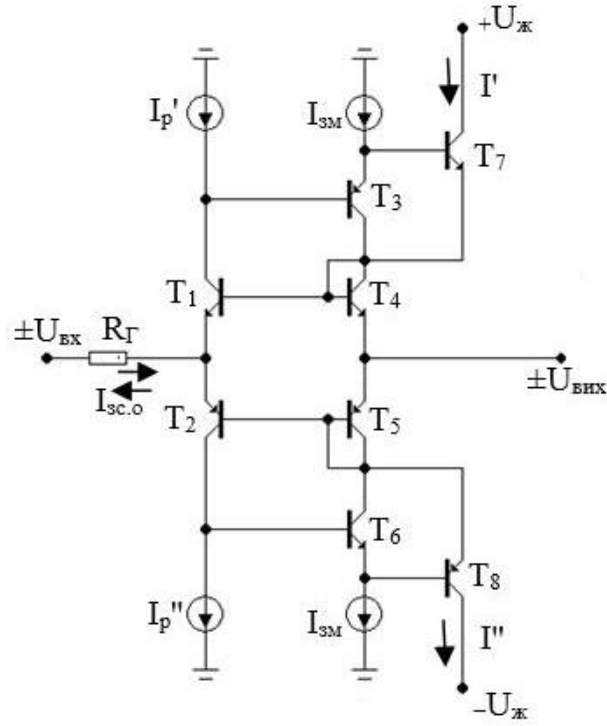
Розв'язання задач

Найпростіший варіант побудови ядер двотактних буферів або масштабаторів напруги зображено на рис. 1а).

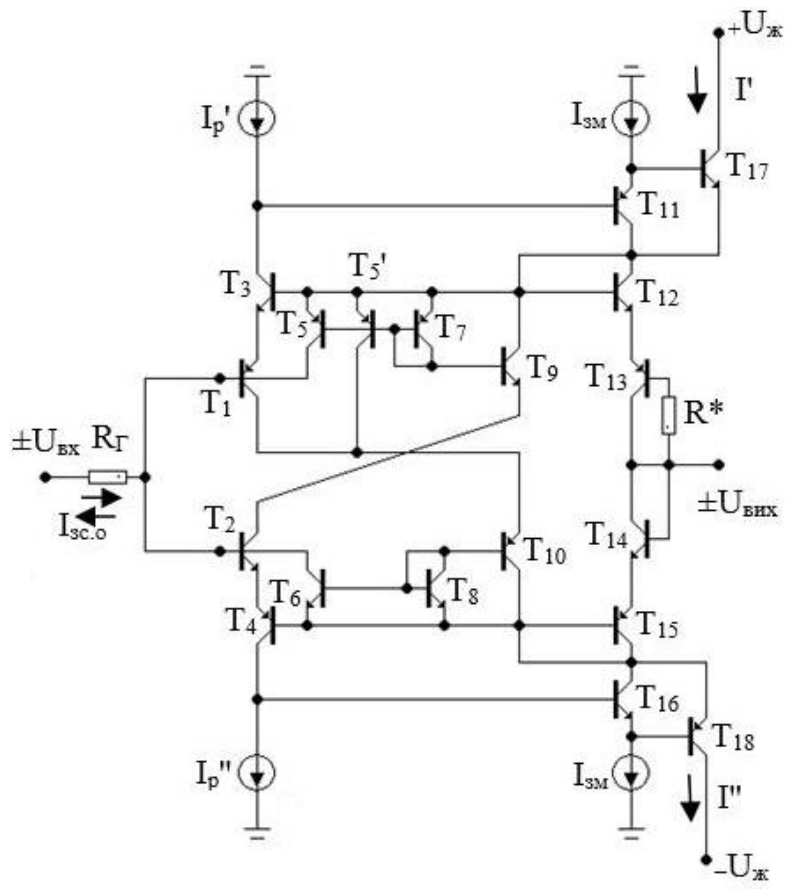
Схема містить два симетричних відбивачі струму, зібрані на транзисторах T_1, T_3, T_4, T_7 а також T_2, T_5, T_6, T_8 відповідно. На відміну від широко відомих відбивачів Уілсона запропоновані схеми мають значно більший (на один-два порядки) вихідний опір по колекторах T_7 і T_8 . У режимі балансу за умови $U_{вх} = 0$ колекторні струми I' і I'' будуть приблизно рівними з похибкою на різницю значень базових струмів вказаних транзисторів. Якщо робочі струми є рівними, тобто $I_p' = I_p''$, то на вході схеми виникає струм зсуву нуля

$$I_{зс.о} = \frac{I_{зМ}}{\beta_3} - \frac{I_{зМ}}{\beta_6},$$

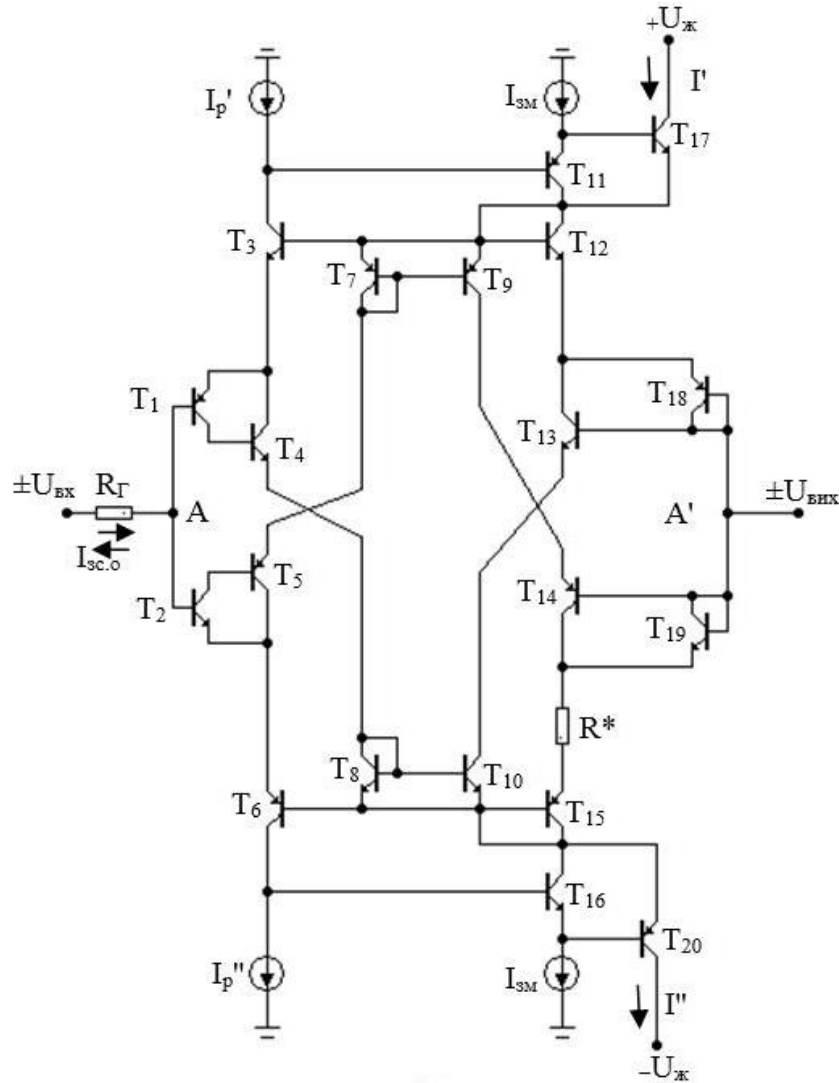
який протікає через генератор вхідної напруги $\pm U_{вх}$. Якщо внутрішній опір цього генератора ненулевий, то це призведе до появи похибки $\Delta U_{вх} = I_{зс.о} \cdot R_{Г}$.



a)



б)



в)

Рисунок 1 – Ядра двотактних БН та МН: а) найпростіша схема; б) із параметричною компенсацією $I_{zc.o}$; в) на складених транзисторах Шиклаї.

Істотним недоліком цієї схеми є жорстка вимога до рівності значень I_p' і I_p'' і якщо вони є нерівними, то різниця $\Delta I_p = I_p' - I_p''$ додається до $I_{zc.o}$. Важливою характеристикою такого БН є малосигнальний вихідний опір $r_{вих}$, оскільки саме він визначає навантажувальну здатність пристрою. Неважко показати, що ця характеристика залежить від рівнів I_p та I_{zm} .

Значення $r_{вих}$ дорівнює

$$r_{вих} = \frac{r_{e4} + \frac{r_{o4}}{1 + \beta_4}}{r_{e5} + \frac{r_{o5}}{1 + \beta_5}},$$

де r_{e4} і r_{e5} – емітерні опори транзисторів T_4 і T_5 , $r_{\beta4}$ і $r_{\beta5}$ – базові опори транзисторів T_4 і T_5 відповідно, β_4 і β_5 – малосигнальні коефіцієнти передачі струму у схемі із загальним емітером.

Кращі характеристики має схема ядра БН, наведена на рисунку 1б). Вона додатково містить вхідні транзистори T_1 і T_2 , за допомогою яких практично нівелюється вплив нерівності I_p' і I_p'' . Водночас у цьому випадку $I_{зс.о}$ починає формуватися як різниця базових струмів T_1 і T_2 . Для зменшення його застосовано параметричну компенсацію. При цьому $I_{зс.о} = I_{\beta1} - I_{\beta2} - I_{\beta9} - I_{\beta10}$, а його рівень залежить від ідентичності статичних характеристик інтегральних n-p-n і p-n-p транзисторів. Посилити ефект компенсації можна вводячи додатковий транзистор T_5' (за умови, що $\beta_{n-p-n} > \beta_{p-n-p}$). Такий підхід дозволяє зменшити $I_{зс.о}$ на один-два порядки. Вихідний опір ядра цього БН буде дорівнювати $r_{вих} \approx r_e$.

Подальшого зниження $I_{зс.о}$ можна досягти, використовувати схему ядра, побудовану на складених транзисторах Шиклаї, наведену на рисунку 1в). Вона містить вхідний каскад на p-n-p і n-p-n транзисторах T_1 , T_4 і T_2 , T_5 відповідно, та вихідний каскад на транзисторах T_{13} , T_{18} і T_{14} , T_{19} . До складу схеми входять також відбивачі струму на транзисторах T_2 , T_{12} і T_6 , T_{15} та регулятори на транзисторах T_{11} , T_{17} і T_{16} , T_{20} . Для задання робочих точок вихідного каскаду ідентичних до вхідного каскаду до схеми уведено внутрішній відбивачі струму на транзисторах T_7 , T_9 і T_8 , T_{10} . При цьому досягається умова рівності емітерних струмів $I_{e4} = I_{e5} = I_{e13} = I_{e14}$. Це дає змогу вирівняти базові струми

$$I_{\beta1} \approx I_{\beta2}, \text{ де } I_{\beta1} = \frac{I_p}{\beta_1 \cdot \beta_4}, I_{\beta2} = \frac{I_p}{\beta_2 \cdot \beta_5}, \text{ а } \beta_1 \cdot \beta_4 \approx \beta_2 \cdot \beta_5.$$

Похибка при цьому визначається технологічними можливостями досягнення ідентичності статичних характеристик інтегральних транзисторів.

Розглянутий схемотехнічний прийом дозволяє виконати умову $U_{\beta e1} = U_{\beta e18}$ а $U_{\beta e2} = U_{\beta e19}$. Таким чином потенціал точок U_A і U_A' також є рівними. Якщо падіння напруги U_{R_r} на R_r є незначним, то $U_{вих} = U_{вх}$. Слід зазначити, що оскільки значення $U_{R_r} = I_{зс.о} \cdot R_r$ то для зменшення цієї складової загальної похибки $\Delta U_{вих} = U_{вих} - U_{вх}$ задачею проєктантів є зменшення саме $I_{зс.о}$.

У таблиці 1 наведено деякі статистичні характеристики ядер БН, котрі зібрано на інтегральних транзисторах типу NUHFARRY і PUHFARRY [11] при $U_{жс} = \pm 10V$, $I_p = 1mA$, $U_{вх} = \pm 5V$.

Таблиця 1 – Статистичні характеристики ядер БН

Схеми	$I_{зм} (mA)$	$I_{зс.о} (nA)$	$\Delta U_m (mKB)$	$\Delta U (nB)$	$r_{вих} (Om)$
1а)	0,5	6200	6,2	185	14,2
1б)	1,5	390	8,8	280	28
1в)	2,5	10	6,1	200	730

Найкращі показники має схема, показана на рисунку 1в). Тут при заданих $I_p = 1mA$, $I_{зм} = 2,5mA$ струм зсуву нуля має найменше значення $I_{зс.о} = 10nA$. Похибки масштабу ΔU_m для всіх трьох схем мають один порядок і значення від $6,2mKB \div 8,8mKB$. Абсолютні похибки лінійності ΔU_l в діапазоні $10,0V$ також мають один порядок на рівні $180 - 280nB$, а відносні менше рівне $0,3 \cdot 10^{-5}\%$. Окремо треба відзначити недостатньо низький вихідний опір схем, особливо третьої, що свідчить про невисоку навантажувальну здатність розглянутих ядер. Для покращення цієї характеристики до складу БН і МН треба увести двотактні підсилювачі постійного струму (ДППС). Схема таких пристроїв наведена на рисунку 2. Розглянемо функціональну схему БН у комплексі з ДППС, зображено на рисунку 2а). Вона містить ядро БН, струмові виходи якого підключено до входів відбивачів струму в ВС1 і ВС2. Виходи цих відбивачів з'єднано зі входом ДППС, побудованого на транзисторах T_1 , T_2 і T_3 , T_4 .

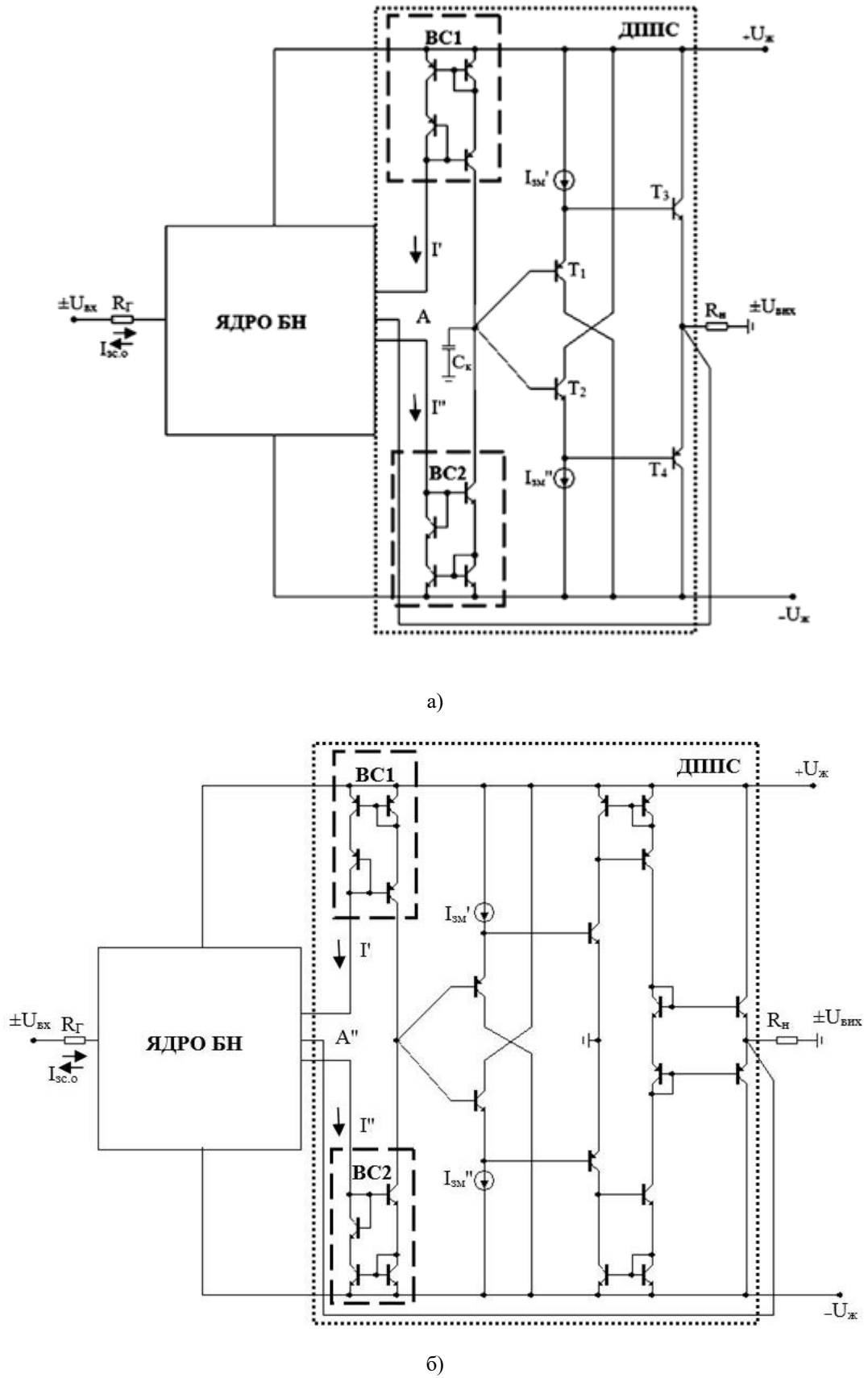


Рисунок 2 – Варіанти підключення ДПНС для буфера напруги: а) з ядрами 1а) і 1б); б) з ядром 1в).

При цьому різницевий струм $\Delta I_p = I' - I''$ подається на вхід ДППС і підсилюється в $K_I = h \cdot \beta_{n-p-n} \cdot \beta_{p-n-p}$ разів, де h – коефіцієнт передачі ΔI із виходів BC1 і BC2 на бази транзисторів T_1 і T_2 , який залежить від співвідношення вихідних опорів цих відбивачів струму і вхідного опору власне ДППС з урахуванням R_n ; β_{n-p-n} і β_{p-n-p} – коефіцієнти передачі струмів n-p-n і p-n-p транзисторів відповідно.

Статичні характеристики БН, побудованих із застосуванням таких ДППС наведено у таблиці 2.

Таблиця 2 – Статичні характеристики БН, побудованих із застосуванням ДППС

Ядра БН	$I_{з.о.} (нА)$	$\Delta U_m (мкВ)$	$\Delta U (нВ)$	$r_{вих} (Ом)$	$f(0дб)(мГц)$
1а)	6200	7,5	250	0,0028	125
1б)	400	8,3	390	0,0056	112
1в)	10	15,2	660	0,0026	216

Вказані дані отримано шляхом моделювання при $R_n = 5 \text{ кОм}$ (1 кОм). Аналіз показників передатних характеристик показує що уведення ДППС практично не впливає на такий параметр як $I_{з.о.}$. Водночас, дещо збільшується похибка масштабу, зокрема для схеми БН, наведеної на рисунку 1 в). Що стосується похибок лінійності, то вони переважно визначаються статистичними характеристиками ДППС. Навантажувальна здатність БН цілком залежить від вихідного опору $r_{вих}$ підсилювача, вхід і вихід якого охоплені глибоким від'ємним зворотним зв'язком, а також від коефіцієнта підсилення струму

$K_I = \frac{I_{вих}}{I_{вх}}$. Тут, чим більше K_I , тим менше $r_{вих}$. Водночас слід зауважити, що збільшення підсилення

погіршує швидкодію схеми, а також вимагає коригування АЧХ для забезпечення стійкості роботи. Для БН із ДППС смуги пропускання на рівні 0дб ($K_I(f) = 1,0$) мають значення 115 мГц, 112 мГц і 120 мГц відповідно.

Крім буферів напруги в різноманітних аналого-цифровій системах виникає потреба в застосуванні масштабаторів напруги, які б також мали низькі відносні похибки масштабу $\partial U_m \leq 0,01\%$ і лінійності

$\partial U_n \leq 0,001\%$, де $\partial U_m = \frac{\Delta U_m}{U_{макс}}$ і $\partial U_n = \frac{\Delta U_n}{U_{макс}}$. Тут U_m – максимальне значення вихідної напруги

по краях діапазона. Слід зазначити, що оскільки на відміну від БН масштабатори повинні заздалегідь мати коефіцієнт передачі більше 1,0, то ДППС треба застосовувати із внутрішнім K_I , значення якого потрібно збільшити на один два порядки. Функціональну схему таких МН наведено на рисунку 3.

Вона містить: ядро МН, яке схемотехнічно може збігатись з ядром БН, відбивачі струму Уілсона (BCY1) і (BCY2); вхідний каскад ДППС на транзисторах $T_1 - T_6$; прості відбивачі струму BC1 і BC2; двотактний підсилювальний каскад на транзисторах $T_7 - T_{12}$ і відбивачах струму BC3 та BC4, а також вихідний двотактний каскад на транзисторах $T_{13} - T_{16}$. Для задання коефіцієнта передачі по напрузі K_U слугує дільник напруги на резисторах R_m і R_{\perp} включений в коло зворотного зв'язку (33). При цьому, якщо ДППС має внутрішній $K_I \geq 10^5$, то значення K_U дорівнює $K_U = 1 + \frac{R_m}{R_{\perp}}$. Такий підсилювач

буде задовольняти системним вимогам, якщо рівень K_U не перевищує 10–100. У випадку потреби збільшення K_U потрібно відповідно збільшувати K_I підсилювача. Для отримання $K_U = 10$ доцільно задати $R_m = 9 \text{ кОм}$, і $R_{\perp} = 1 \text{ кОм}$, $K_U = 100$ відповідно $R_m = 9,9 \text{ кОм}$, і $R_{\perp} = 100 \text{ Ом}$.

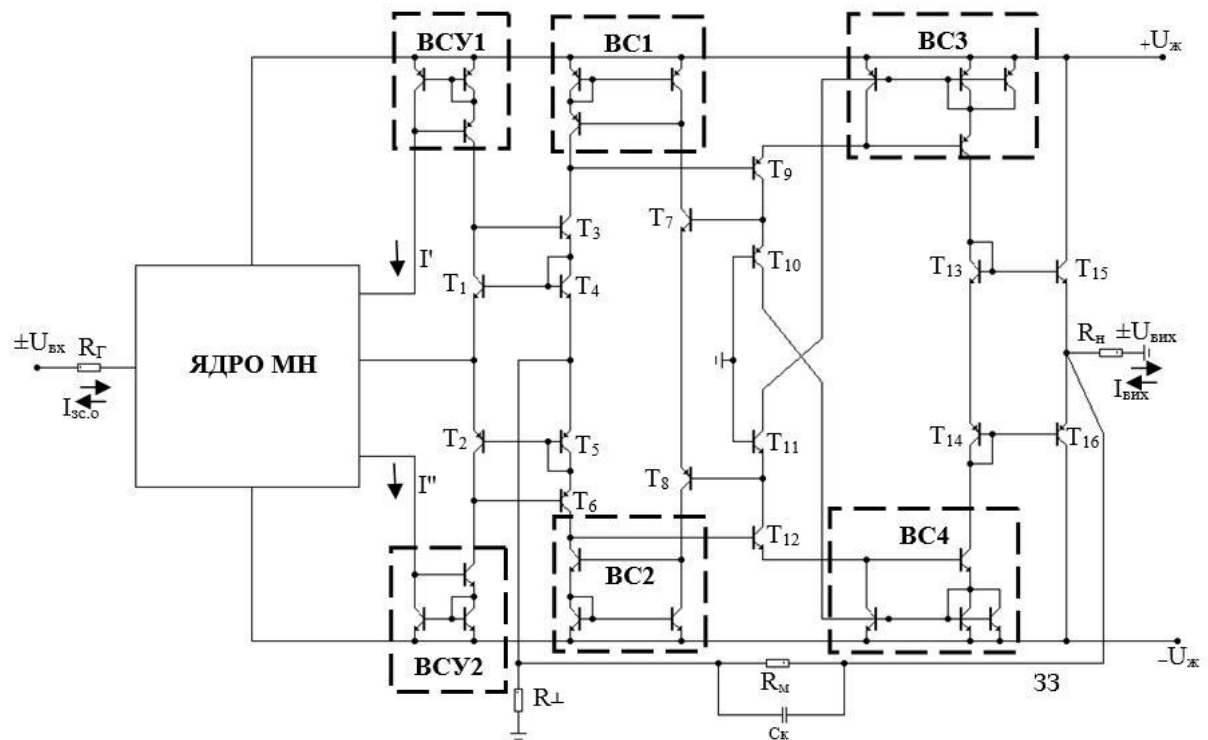


Рисунок 3 – Функціональна схема МН із низькими похибками масштабу й лінійності.

Під час визначення динамічних характеристик БН і МН слід мати на увазі, що максимальну швидкість має ядро цих пристроїв, водночас як загальна швидкість визначається властивостями переважно ДППС, а також значеннями K_I і K_U , які істотно впливають, наприклад, на перехідну характеристику на рисунку 4, та амплітудно-частотну характеристику на рисунку 5. В ідеальному випадку буферний елемент напруги на виході цілком повторює напругу на вході. Слід зауважити, що притаким заданих параметрах імпульса вхідного сигналу на виході схеми практично відсутні часові і фазові спотворення вихідного сигналу. Це свідчить про досить високу швидкість БН.

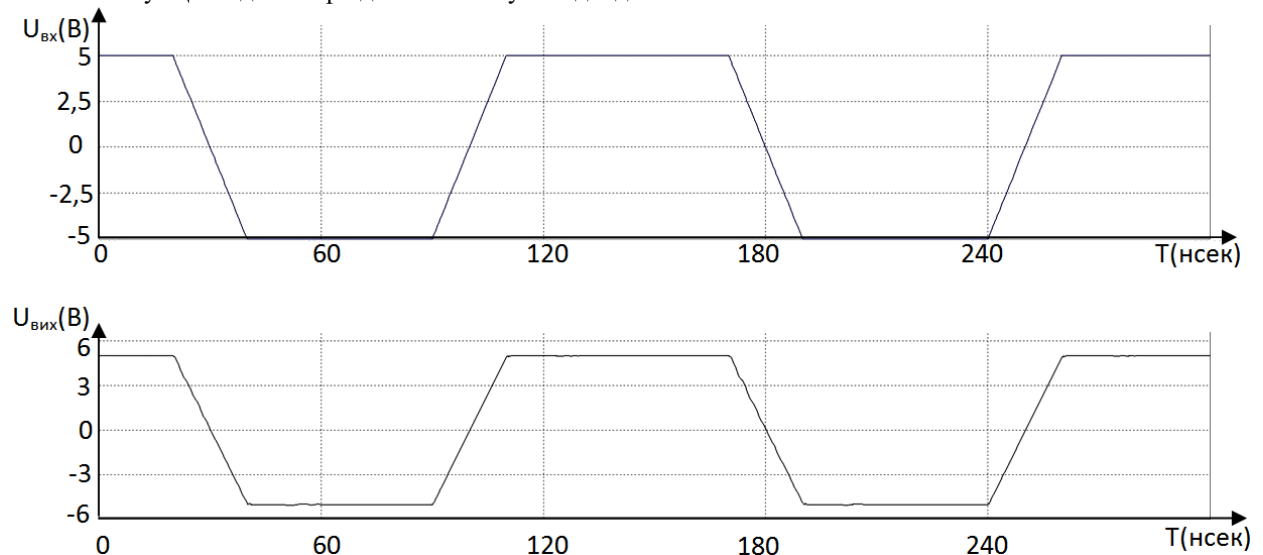


Рисунок 4 – Перехідна характеристика ДППС з ядром 1а).

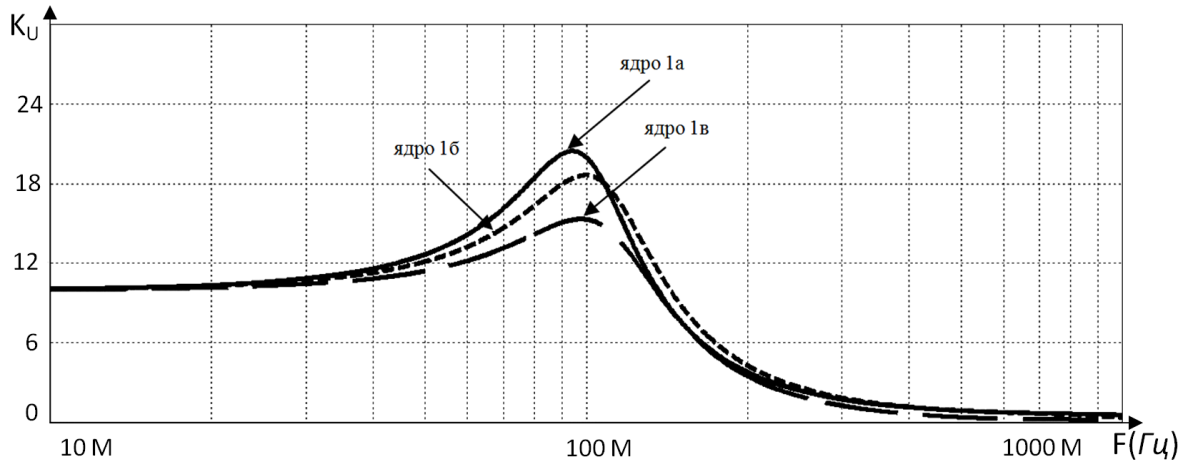


Рисунок 5– Амплітудно частотна характеристика МН з ядрами 1а), 1б) та 1в).

Висновки

1. Розглянуто схемотехнічні особливості трьох варіантів побудови ядер БН і МН. Доведено, що вхідний струм зсуву нуля доцільно зменшувати шляхом застосування у вхідних каскадах підсилювальних *p-n-p* і *r-n-p* транзисторів, а також складених транзисторів Шиклаї;

2. Проаналізовано статичні і динамічні характеристики шляхом комп'ютерного моделювання показано, що похибки масштаби БН і МН не перевищують значень 10 мкВ у діапазоні відповідного сигналу $\pm 5,0 \text{ В}$, а похибки лінійності 300 нВ . Отримана перехідна характеристика свідчить, що швидкість наростання вихідної напруги буде не гірше 2000 В / мкс .

3. Здійснено порівняння метрологічних характеристик БН і МН у вигляді сукупності ядер і вихідних ДППС. Доведено, що застосування цих підсилювачів дозволяє істотно (на 3-4 порядки) покращити навантажувальну здатність схем при збереженні рівня вхідного струму зсуву нуля, а також похибок масштабу і лінійності.

Список літератури

- [1] О.Д. Азаров, В.А. Гарнага, *Двотактні підсилювачі постійного струму для багаторозрядних перетворювачів форми інформації, що самокалібруються*, Вінниця, Україна УНІВЕРСУМ-Вінниця, 2011, 156 с.
- [2] О. Д. Азаров, М. Ю. Теплицький, Н. О. Біліченко, *Швидкодійні двотактні підсилювачі постійного струму з балансним зворотним зв'язком*,. Вінниця, Україна, ВНТУ, 2016, 136 с.
- [3] О.Д. Азаров, С.В. Богомолів, *Основи теорії високолінійних аналогових пристроїв на базі двотактних підсилювальних схем*, Вінниця, Україна, УНІВЕРСУМ-Вінниця, 2013, 142 с.
- [4] О.Д. Азаров, О.В. Дудник, *Методи та засоби високоточного слідкувального аналого-цифрового перетворення з вагою надлишковістю*, Вінниця, Україна - УНІВЕРСУМ-Вінниця, 2014, 120 с.
- [5] А. Б. Гребен *Проектирование аналоговых интегральных схем*, Москва, Россия: Энергия, 1976, 256 с
- [6] В. Grebene, *Bipolar and MOS analog integrated circuit design*, New Jersey, John Wiley & Sons Technology & Industrial Arts, 2002, 912 p.
- [7] О.Д. Азаров, Л.В. Крупельницький, *Аналого-цифрові пристрої систем, що самокоригуються, для вимірювань і оброблення низькочастотних сигналів*, Вінниця, Україна, УНІВЕРСУМ-Вінниця, 2005, 167 с.
- [8] Азаров О. Д., *Основи теорії аналого-цифрового перетворення на основі надлишкових позиційних систем числення*, Вінниця, Україна, УНІВЕРСУМ-Вінниця, 2004, 257 с.
- [9] Г. Д. Бахтиаров, В. В. Малинин, В. П. Школин, *Аналого-цифровые преобразователи*, Москва, Росія, Сов. радио, 1980, 278 с.
- [10] Буферизация ОП для збільшення вихідного струму, Robert Keim, Опубліковано 16.07.2016 [Електронний ресурс]. Режим доступу: <http://infotabula.com/elektronika/buferizaciya-op-dlya-zbilshennya-vixidnogo-strumu.html>. Дата звернення: квітень, 1, 2019.
- [11] М. А. Амелина, и С. А. Амелин, *Программа схемотехнического моделирования Micro-Cap. Версия 9, 10*, Смоленск, Россия: Смоленский филиал НИУ МЭИ, 2013, 618 с.

References

- [1] O.D. Azarov, V.A. Harnaha, Dvotaktni pidsyliuvachi postiinoho strumu dlia bahatorozriadnykh

- peretvoriuvachiv formy informatsii, shcho samokalibriuetsia, Vinnytsia, Ukraina UNIVERSUM-Vinnytsia, 2011, 156 s.
- [2] O. D. Azarov, M. Yu. Teplytskyi, N. O. Bilichenko, Shvydkodiini dvotaktni pidsylyuvachi pos-tiinoho strumu z balansnym zvorotnym zviazkom., Vinnytsia, Ukraina, VNTU, 2016, 136 s.
- [3] O.D. Azarov, S.V. Bohomolov, Osnovy teorii vysokoliniinykh analohovykh prystroiv na bazi dvotaktnykh pidsylyvalnykh skhem, Vinnytsia, Ukraina, UNIVERSUM-Vinnytsia, 2013, 142 s.
- [4] O.D. Azarov, O.V. Dudnyk, Metody ta zasoby vysokotochnoho slidkuvalnoho analoho-tsyfrovoho peretvorennya z vahovoiu nadlyshkovistiu, Vinnytsia, Ukraina - UNIVERSUM-Vinnytsia, 2014, 120 s.
- [5] A. B. Hreben Proektyrovanye analohovykh yntehralnykh skhem, Moskva, Rossyia: Enerhyia, 1976, 256 s
- [6] B. Grebene, Bipolar and MOS analog integrated circuit design, New Jersey, John Wiley & Sons Technology & Industrial Arts, 2002, 912 p.
- [7] O.D. Azarov, L.V. Krupelnytskyi, Analoho-tsyfrovi prystroi system, shcho samokoryhuiut-sia, dlia vymiriuvan i obrobliannia nyzkochastotnykh syhnaliv, Vinnytsia, Ukraina, UNIVERSUM-Vinnytsia, 2005, 167 s.
- [8] Azarov O. D., Osnovy teorii analoho-tsyfrovoho peretvorennya na osnovi nadlyshkovykh pozy-tsiinykh system chyslennia, Vinnytsia, Ukraina, UNIVERSUM-Vinnytsia, 2004, 257 s.
- [9] H. D. Bakhtyarov, V. V. Malynyn, V. P. Shkolyn, Analoho-tsyfrovye preobrazovateli, Mosk-va, Rosiia, Sov. radyo, 1980, 278 s.
- [10] Buferyzatsiia OP dlia zbilshennia vykhidnoho strumu, Robert Keim, Opublikovano 16.07.2016 [Elektronnyi resurs]. Rezhym dostupa: <http://infotabula.com/elektronika/buferizatsiya-op-dlya-zbilshennya-vixidnogo-strumu.html>. Data zvernennia: kviten, 1, 2019.
- [11] M. A. Amelyna, y S. A. Amelyn, Prohramma skhemotekhnicheskoho modelyrovanyia Micro-Cap. Versyia 9, 10, Smolensk, Rossyia: Smolenskyi fylyal NYU MEY, 2013, 618 s.

Відомості про авторів

Азаров Олександр Дмитрович – д-р. техн. наук, професор, декан факультету інформаційних технологій та комп'ютерної інженерії.

Медяний Роман Михайлович – аспірант кафедри обчислювальної техніки.

Фігас Анна Сергіївна – аспірант групи 1 АС-18.

O. D. Azarov, R. M. Medyanii, A. S. Figas

HIGH-LINKED BUFFER AND VOLTAGE SCALE FOR BIPOLAR TRANSISTORS WITH LOW INPUT CURRENT

Vinnytsia National Technical University, Vinnytsia

А. Д. Азаров, Р. М. Медяный, А. С. Фигас

ВЫСОКОЛИНЕЙНЫЕ БУФЕРЫ И МАСШТАБОРЫ НАПРЯЖЕНИЯ НА БИПОЛЯРНЫХ ТРАНЗИСТОРАХ С НИЗКИМ ВХОДНЫМ ТОКОМ

Винницкий национальный технический университет, г. Винница

УДК 004.272

Т. Б. Мартинюк, Н. О. Денисюк, Б. І. Круківський
**АСОЦІАТИВНІ ПРОЦЕСОРИ З ПАРАЛЕЛЬНО-
 ПОСЛІДОВНОЮ ОБРОБКОЮ ДАНИХ**

Вінницький національний технічний університет, м. Вінниця

Анотація. Розробка асоціативної пам'яті та паралельних методів асоціативної обробки масивів даних дозволяє подолати обмеження адресного (послідовного) доступу до пам'яті та збільшити швидкодію необчислювальних операцій. Серед методів асоціативної обробки найбільше розповсюдження отримав метод обробки по розрядних зрізах (слайзах), тобто з одночасною обробкою однойменних розрядів усіх слів. В роботі проаналізовано відомі варіанти побудови асоціативних процесорів, базовим вузлом яких є асоціативна пам'ять. Обрано асоціативний процесор з паралельно-послідовним способом обробки елементів числового масиву. Запропоновано дві структури асоціативних процесорів з можливістю виконання операцій пошуку за ключем і пошуку мінімуму/максимуму у числовому масиві. У першому запропонованому варіанті в асоціативному процесорі для пошуку у масиві даних за ключем паралельно-послідовна обробка дозволяє зафіксувати співвідношення n операндів з ключем у вигляді бінарних ознак ($=$, \neq) в пам'яті результатів на триггерах. У другому запропонованому варіанті в асоціативному процесорі для пошуку екстремальних чисел розширення функціональних можливостей досягається за рахунок роботи в двох режимах: пошук мінімального або максимального числа у масиві n чисел. Особливістю таких процесорів є використання швидкої регістрової пам'яті на лічильниках та паралельної обробки без операції порівняння елементів числового масиву. В цьому випадку можна об'єднати функціональні можливості двох типів запропонованих асоціативних процесорів в одному асоціативному процесорі через подібність їх структурної організації та принципу обробки елементів числового масиву через використання операції декременту у регістровій пам'яті на лічильниках. Розраховано основні параметри запропонованих асоціативних процесорів. Виконано порівняльний аналіз відомих та запропонованих асоціативних процесорів за такими показниками, як апаратна складність та часові витрати. Значною перевагою запропонованих асоціативних процесорів є регулярність структури та менша кількість апаратних витрат. Виграш в апаратних витратах є важливим при реалізації асоціативних процесорів на перспективній елементній базі – ПЛІС.
Ключові слова: асоціативна пам'ять, асоціативний процесор, пошук за ключем, пошук мінімуму/максимуму, операції інкременту/декременту.

Аннотация. Разработка ассоциативной памяти и параллельных методов ассоциативной обработки массивов данных позволяет преодолеть ограничения адресного (последовательного) доступа к памяти и увеличить быстродействие невычислительных операций. Среди методов ассоциативной обработки наибольшее распространение получил метод обработки по разрядным срезам (слайзам), то есть с одновременной обработкой одноименных разрядов всех слов. В работе проанализированы известные варианты построения ассоциативных процессоров, базовым узлом которых является ассоциативная память. Выбран ассоциативный процессор с параллельно-последовательным способом обработки элементов числового массива. Предложены две структуры ассоциативных процессоров с возможностью выполнения операций поиска по ключу и поиска минимума / максимума в числовом массиве. В первом предложенном варианте в ассоциативном процессоре для поиска в массиве данных по ключу параллельно-последовательная обработка позволяет зафиксировать соотношение n операндов с ключом в виде бинарных признаков ($=$, \neq) в памяти результатов на триггерах. Во втором предложенном варианте в ассоциативном процессоре для поиска экстремальных чисел расширение функциональных возможностей достигается за счет работы в двух режимах: поиск минимального или максимального числа в массиве n чисел. Особенностью таких процессоров является использование быстрой регистровой памяти на счетчиках и параллельной обработки без операции сравнения элементов числового массива. В этом случае можно объединить функциональные возможности двух типов предлагаемых ассоциативных процессоров в одном ассоциативном процессоре из-за сходства их структурной организации и принципа обработки элементов числового массива с использованием операции декремента в регистровой памяти на счетчиках. Рассчитаны основные параметры предложенных ассоциативных процессоров. Выполнен сравнительный анализ известных и предложенных ассоциативных процессоров по таким показателям, как аппаратная сложность и временные затраты. Значительным преимуществом предложенных ассоциативных процессоров является регулярность структуры и меньшее количество аппаратных затрат. Вывыгрыш в аппаратных затратах является важным при реализации ассоциативных процессоров на перспективной элементной базе - ПЛИС.
Ключевые слова: ассоциативная память, ассоциативный процессор, поиск по ключу, поиск минимума / максимума, операции инкремента / декремента.

Abstract. Development of associative memory and parallel methods of associative processing of numerical arrays allows to overcome the limitations of address (serial) access to memory and increase the speed of non-calculating operations. Among the methods of associative processing the most commonly used methods is processing method by bit cuts (slices), that is the simultaneous processing of the same names of bits of all words. In this paper the known variants of constructing associative processors, the base block of which is associative memory, is analyzed. An associative processor with a parallel-serial method of elements processing of a numerical array is selected. Two structures of associative processors with the ability to perform searches by key and search for a minimum / maximum in a numerical array are proposed. In the first proposed variant of the associative processor for the search by key in the numerical array, parallel-serial processing allows fixing the ratio of n operands with the key in the form of binary attributes ($=$, \neq) in the memory of the results on the triggers. In the second proposed version of the associative processor for search extreme numbers, the expansion of functionality is achieved by working in two modes: the search for a minimum or maximum number in an array of numbers. The feature of such processors is the using of fast register memory on counters and parallel processing without the operation of comparing elements of a numerical array. In this case, it's possibly to combine the functionality of the two types of proposed associative processors in one associative processor due to the similarity of their structural organization and the principle of the elements processing of a numerical array using the operation of a decrement in the register memory on the counters. The basic parameters of the proposed associative processors are calculated. A comparative analysis of known and proposed associative processors is performed on indicators such as hardware complexity and time costs. A significant advantage of the proposed associative processor is the regularity of the structure and the smaller amount of hardware costs. The gain in hardware costs is important for the implementing of associative processor on promising element base - FPGA.

Keywords: associative memory, associative processor, search by key, search for minimum / maximum, operations increment / decrement.

DOI: <https://doi.org/10.31649/1999-9941-2019-44-1-27-36>.

Т. Б. Мартинюк, Н. О. Денисюк, Б. І. Круківський, 2019

Вступ

Розвиток обчислювальної техніки та створення інформаційно-пошукових систем вимагає застосування паралельної та асоціативної обробки значних масивів інформації [1], оскільки це дозволяє підвищити продуктивність інформаційних систем, забезпечити швидкий паралельний пошук інформації в пам'яті великого об'єму, здійснити заміну значної частини програмних засобів апаратними засобами, спростити програмування і скоротити час, що витрачається на вирішення таких задач [2,3].

Актуальність

Більшість прикладних задач, що існують в даний час, переважно орієнтовані на традиційну адресну обробку, що супроводжується зменшенням швидкодії через незначний рівень паралелізму пошуку та вибірки з пам'яті даних. Тому актуальним є науково-технічний напрямок, що пов'язаний з розробкою асоціативної пам'яті та паралельних методів асоціативної обробки, який дозволяє подолати обмеження, властиві адресному (последовному) доступу до пам'яті [3-6]. При цьому, до переваг асоціативних процесорів, що використовують асоціативну пам'ять, можна віднести: високий рівень паралелізму через обробку по розрядних зрізах (слайзах), паралельний пошук за вмістом пам'яті в процесі порівняння за ключем, виконання базових операцій пошуку, що відбуваються за час, пропорційний кількості бітових стовпців в заданому масиві даних або у ключі [2-6].

Про перспективність такого підходу свідчать розробки асоціативної пам'яті як на сучасній елементній базі, зокрема на ПЛІС, так і оптичні та оптоелектронні варіанти асоціативної пам'яті [7,8].

Мета

Метою даної роботи є вдосконалення структури асоціативних процесорів з розширеними функціональними можливостями на базі швидкої регістрової пам'яті, а саме з можливістю виконання таких базових масових операцій, як пошук даних за ключем та пошук мінімуму/максимуму серед елементів масиву без паралельного порозрядного логічного порівняння.

Огляд першоджерел

Асоціативна пам'ять або асоціативний запам'ятовуючий пристрій (АЗП) є особливим видом машинної пам'яті, що використовується для швидкого паралельного пошуку інформації [2-6]. Вона відома також як пам'ять, що адресується за змістом (англ. Content-addressable memory, CAM) або асоціативний масив [9].

Аналіз досліджень показав, що одним з найвідоміших асоціативних процесорів є CAM 2000 [9], що об'єднує можливості асоціативного процесора, асоціативної та динамічної пам'яті в одному кристалі. Цей кристал крім функцій динамічної пам'яті також реалізує просту масово-паралельну обробку вмісту, що зберігається в динамічній пам'яті. Такий процесор може виконувати такі операції, як визначення суми компонент вектора, мінімальної чи максимальної компоненти вектора, середнього k чисел та інші [9].

Асоціативний процесор (АП) – це спеціалізований процесор, що реалізується на базі АЗП і призначений для одночасного виконання операцій над масивами даних [2,10]. АП можуть бути розділені на чотири категорії відповідно до організації процесу порівняння елементів масиву даних: повністю паралельні, порозрядно-последовні (паралельно-последовні), послівно-последовні (последовні) та блочно-орієнтовані асоціативні процесори [4,11]. Прикладами паралельних АЗП є відомі оптичні ЗП з дискретним представленням інформації, які розглядаються як однопортова [12] та багатопортова асоціативна пам'ять [13], що можуть бути використані в системах на основі нейронних мереж та в пристроях для обробки зображень [13]. Разом з тим АП з паралельно – последовним пошуком займають проміжне положення між суто паралельними та последовними і є компромісним рішенням, адже паралельні АП, наприклад, у вигляді ітеративної мережі [2] – швидкі, але багатозатратні апаратно, а последовні АП [3,4] – малозатратні, але мають низьку швидкодію.

Особливість паралельно-последовного АП або вертикального АП полягає в тому, що він забезпечує паралельно-последовний пошук інформації по розрядних зрізах (слайзах), тобто по однойменних розрядах всіх слів у великих масивах даних, які знаходяться в АЗП [2-4]. У склад вертикального АП [4], що представлений на рис.1, входять такі елементи: модуль АЗП, регістр аргументу пошуку, регістр маски, пам'ять фіксації реакцій, аналізатор багатократного співпадіння, а також допоміжні лінії керування і передачі даних. Регістр маски, що призначений для зберігання коду маскуванню, і регістр аргументу пошуку об'єднані в один блок.

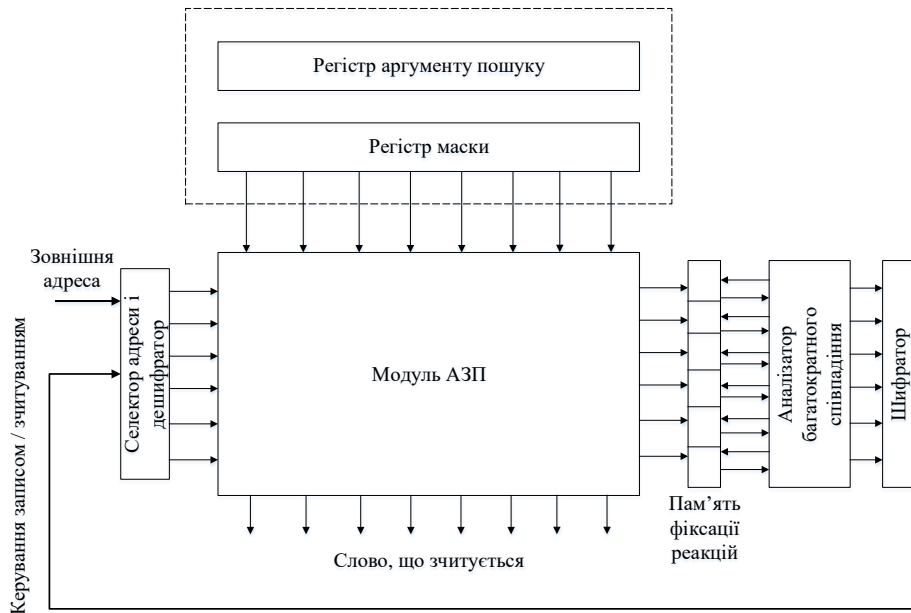


Рисунок 1 – Організація асоціативного процесора[4]

Таким чином, окрім основних функцій АЗП, пов'язаних зі збереженням ключів і даних, їх довільним адресним записом і зчитуванням даних, АП має виконувати певні логічні функції. Ці функції, в даному випадку, містять порозрядне логічне порівняння кожного аргументу пошуку зі всіма збереженими ключами і логічне виявлення співпадіння аргументу пошуку або ключа. Але наведена структура вертикального АП не виконує таку базову масову операцію, як пошук мінімуму/максимуму.

Разом з тим, використання лічильників замість регістрів в АЗП дозволяє перейти від розрядно-зрівнювального порівняння в процесі пошуку за ключем до використання швидкісної операції декременту паралельно для всіх елементів числового масиву в АЗП.

Асоціативний процесор з пошуком за ключем у регістровій пам'яті

Структуру запропонованого АП для порівняння масиву даних за ключем представлено на рис.2. АП складається з таких основних блоків, як регістрова пам'ять на лічильниках, регістр ключа, вузол керування, логічний вузол і пам'ять результатів (ПР) [14]. На рис.2 прийнято такі позначення: A_1, \dots, A_n – вхідні дані (операнди); Y_1, \dots, Y_n – виходи ознак процесора; K – ключ; P_{0i} – ознака нульового вмісту i -го елемента регістрової пам'яті ($i=1, \dots, n$).

При виконанні операції пошуку за ключем АП працює таким чином. У швидку регістрову (локальну) пам'ять процесора записується масив даних A_1, \dots, A_n із загальної (зовнішньої) пам'яті, в регістр ключа записується аргумент пошуку (ключ) K , а всі тригери ознак ПР встановлюються в одиничний стан. У регістровій пам'яті та у регістрі ключа відбувається одночасне зменшення всіх операндів (чисел) на одиницю з надходженням кожного тактового імпульсу, тобто виконується операція декременту [15]. Коли будь-який з регістрів, наприклад, i -й регістр обнулється повністю, на його ознаковому виході з'явиться одиничний сигнал P_{0i} – сигнал ознаки нульового вмісту відповідного i -го регістра. В подальшому поточні сигнали ознак P_{01}, \dots, P_{0n} проходять по відповідній гілці логічного вузла, що складається з елемента затримки, елементів АБО-НІ, І та АБО, і надходять на R-входи відповідних RS-тригерів ознак ПР (рис.3) [14], скидаючи їх у нульовий стан.

В процесі роботи процесора можуть мати місце три випадки співвідношення кожного з операндів A_i ($i=1, \dots, n$) з ключем K [16,17]: а) коли операнд A_i менший за значенням, ніж ключ K : $A_i < K$; б) коли операнд A_i більший за значенням, ніж ключ K : $A_i > K$; в) коли операнд A_i дорівнює ключеві K : $A_i = K$.

У випадку коли виконується співвідношення $A_i = K$, тобто інформація відсутня в i -му регістрі за відсутності інформації у регістрі ключа, про це свідчить наявність двох одиничних сигналів P_{0i} і P_{0k} . Ці сигнали, проходячи через елементи відповідної гілки, на її виході формують нульовий сигнал, який надходить на R-вхід i -го RS-тригера ознак ПР. В результаті на його прямому виході Y_i ознаки залишається одиничний сигнал.

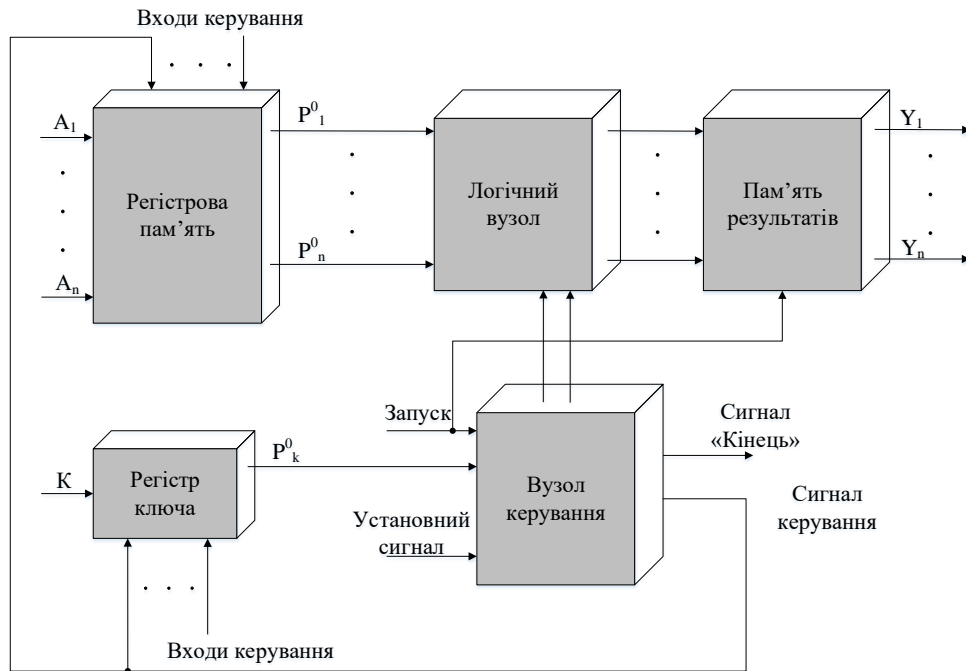


Рисунок 2 – Структура асоціативного процесора для пошуку за ключем

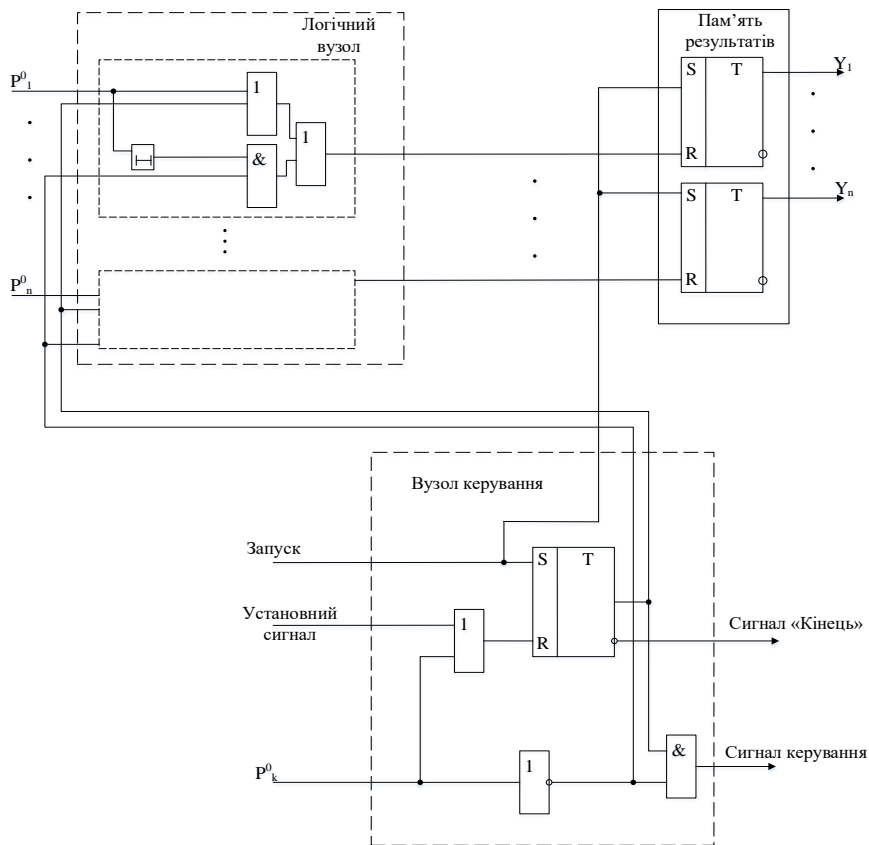


Рисунок 3 – Функціональна схема логічного вузла, вузла керування та пам'яті результатів на тригерах

Таким чином, лише у випадку, коли будь-який з операндів A_1, \dots, A_n співпадає з ключем K , тобто виконується співвідношення $(=)$, на відповідному виході Y_1, \dots, Y_n ознаки формується одиничний сигнал, у протилежному випадку (\neq) на відповідному виході фіксується нульовий сигнал [16,17].

Отже в процесі зчитування (зменшення) кодів у n регістрах пам'яті та регістрі ключа на лічильниках виконується порівняння n операндів A_1, \dots, A_n з ключем K з фіксуванням їх співвідношення $(=), (\neq)$ у вигляді бінарних ознак на відповідних виходах Y_1, \dots, Y_n процесора. Особлива відмінність даного процесу пошуку в АП полягає в тому, що операнди в його регістровій пам'яті не зберігаються в процесі зменшення на одиницю вмісту кожного регістра, а визначається лише місцезнаходження (адреса) операндів, що співпали з ключем. В подальшому ця адреса з виходів ПР використовується для зчитування інформації із загальної пам'яті. При цьому час пошуку інформації за асоціативною ознакою в регістровій пам'яті залежить тільки від кількості розрядів ключа і від швидкості опитування (декременту) його вмісту, але не залежить від розмірності регістрової пам'яті (кількості слів), оскільки при опитуванні аналізується паралельно вміст всіх регістрів [14-17].

Асоціативний процесор для пошуку екстремальних чисел

На рис.4 представлено структурну схему запропонованого АП для пошуку мінімуму/максимуму серед чисел масиву. Він складається з таких основних блоків, як регістрова пам'ять на лічильниках, вихідний регістр, вузол керування, логічний вузол та пам'ять результатів ПР [18].

АП для пошуку мінімуму/максимуму (рис.4) працює таким чином. В регістрову пам'ять записується масив чисел A_1, \dots, A_n , обирається режим пошуку або мінімального, або максимального числа, усі тригери ПР встановлюються в одиничний стан. Після закінчення процесу пошуку одиничний сигнал на i -му виході ознаки Y_1, \dots, Y_n вказує на місцезнаходження мінімального чи максимального елемента масиву, а саме відшукане число зчитується з виходу Авих вихідного регістра. Функціональну схему логічного вузла, вузла керування та ПР в АП представлено на рис. 5.

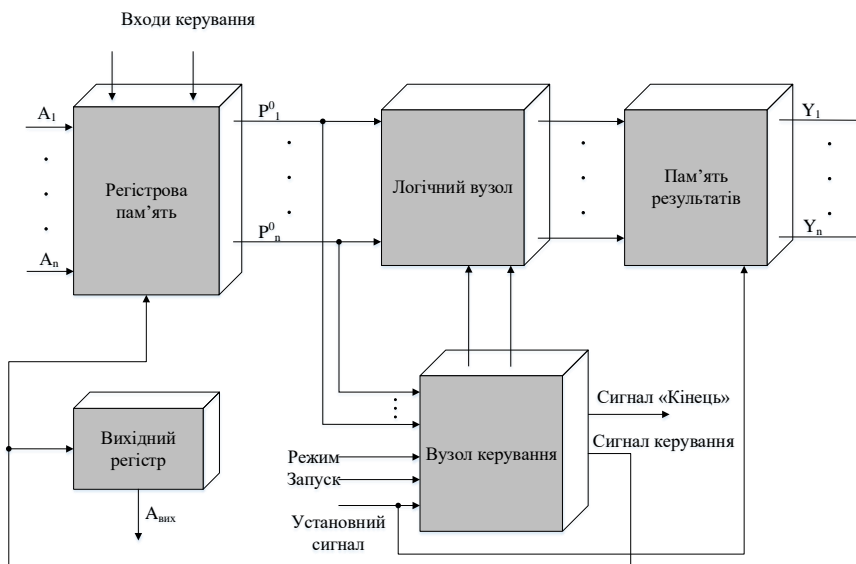


Рисунок 4 – Структура асоціативного процесора для пошуку екстремальних чисел

У режимі пошуку мінімального числа RS-тригер режиму вузла керування встановлюється в нульовий стан, в результаті одиничний сигнал з його інверсного виходу відкриває елементи гілки MIN – пошуку мінімального числа та закриває елементи гілки MAX – пошуку максимального числа у логічному вузлі (див. рис.5). У регістровій пам'яті за аналогією з попереднім процесом пошуку в АП (рис.2) відбувається одночасне зменшення усіх операндів (чисел) на одиницю з надходженням кожного тактового імпульсу (операція декременту), а у вихідному регістрі одночасно відбувається порозрядне збільшення вмісту (операція інкременту). Коли будь-який з регістрів, наприклад, i -й регістр обнулиться повністю, на його ознаковому виході з'явиться одиничний сигнал P_{0i} – сигнал ознаки його нульового вмісту.

При роботі процесора у режимі пошуку максимального числа RS-тригер режиму у вузлі керування встановлюється в одиничний стан, в результаті одиничний сигнал з його прямого виходу відкриває елементи гілки MAX – пошуку максимального числа і закриває елементи гілки MIN – пошуку мінімального числа в логічному вузлі (рис.5). У регістровій пам'яті аналогічно виконується операція декременту, а у вихідному регістрі – операція інкременту. Цей процес відбувається доти, поки усі регістри не обнуляться повністю, після чого на їхніх ознакових виходах з'являться одиничні сигнали P_{01}, \dots, P_{0n} , крім одного, що обнулиться останнім. Одиничне значення на конкретному виході Y_1, \dots, Y_n

ознаки вказує на місцезнаходження мінімального/максимального числа у масиві за умови, що це одне мінімальне або максимальне число.

Особливістю асоціативної обробки у даному АП, як і в АП для пошуку за ключем є те, що інформація в регістровій пам'яті теж не зберігається (через застосування процедури декременту в усіх регістрах одночасно), а визначається лише місце знаходження мінімального або максимального елемента масиву чисел. В подальшому ця адреса з виходів ПР використовується для зчитування інформації із загальної пам'яті. Сформоване мінімальне чи максимальне число зчитується з виходу Авих вихідного регістра [18].

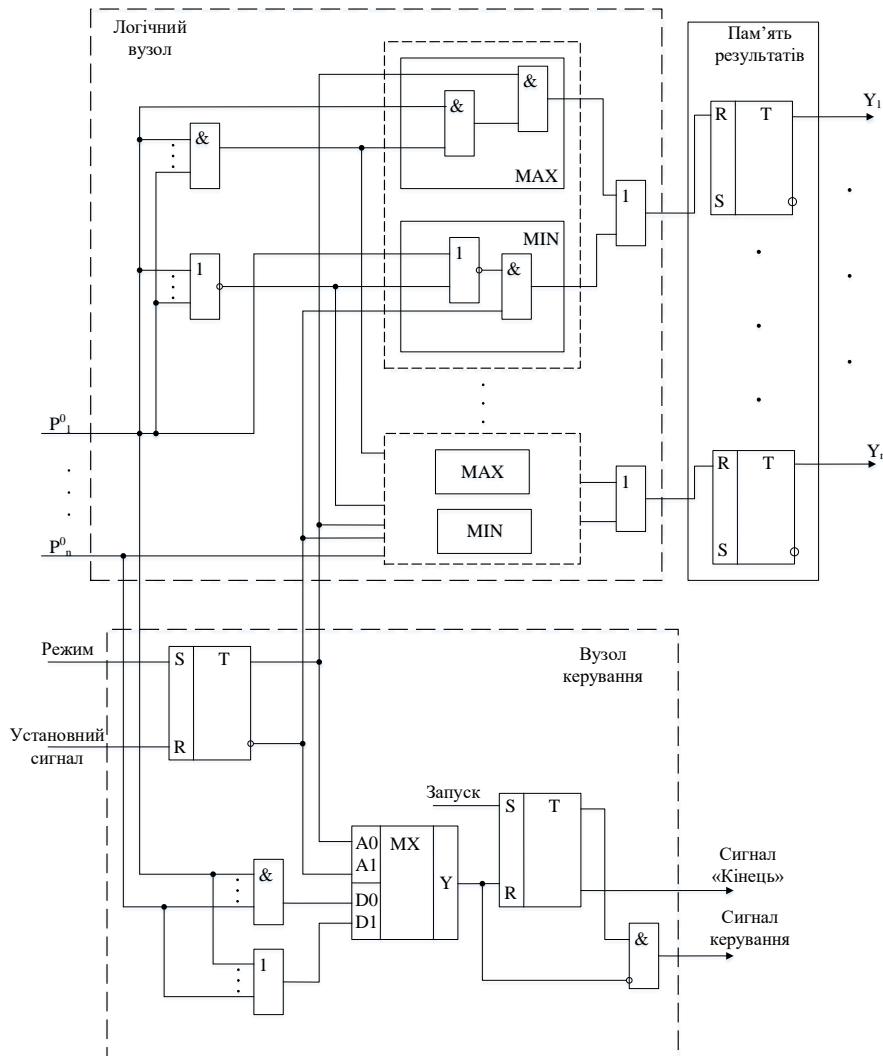


Рисунок 5 – Функціональна схема логічного вузла, вузла керування та пам'яті результатів

Основні параметри асоціативних процесорів

Основними параметрами асоціативної пам'яті у складі АП є інформаційна ємність даних $N \cdot R$, де N – кількість слів, R – розрядність даних, а також час асоціативної вибірки даних t_a , необхідний для виявлення співпадінь [12, 13].

Для відомого АП [4] загальний час асоціативної вибірки масивів даних визначається наступним чином:

$$t_a = t_{com} + t_{wr} + t_{rd} + t_{cd}, \quad (1)$$

де t_{com} , t_{rd} , t_{wr} , t_{cd} – час, що витрачається відповідно на операцію порівняння, зчитування з регістрової пам'яті, запис результату у тригер ознак та шифрацію адреси (рис.1).

Якщо врахувати, що

$$t_{com} + t_{rd} + t_{cd} \gg t_{wr}, \quad (2)$$

то вираз (1) матиме наступний вигляд для випадку паралельної вибірки слів з регістрової пам'яті:

$$t_a = t_{com} + t_{rd} + t_{cd}, \quad (3)$$

У випадку вибірки слів по зрізах (слайзах) з регістрової пам'яті час асоціативної вибірки становитиме:

$$t_a = R(t_{com} + t_{rd}) + t_{cd}, \quad (4)$$

Для запропонованого АП з пошуком за ключем час асоціативної вибірки визначається таким чином (рис.2):

$$t_a = t_{ct} + t_{lg} + t_{wr}, \quad (5)$$

де t_{ct} , t_{lg} – час, що витрачається відповідно на операцію інкременту/декременту та логічні операції. Враховуючи, що

$$t_{ct}^{\max} = (2^R - 1) \cdot \tau_{ct} \gg t_{lg} + t_{wr}, \quad (6)$$

в подальшому використовуємо для розрахунку часових витрат запропонованого АП формулу (6), де τ_{ct} – час затримки при лічбі двійкового лічильника.

Оскільки для будь-якої асоціативної операції бажано визначити її максимальну часову характеристику, то прийmemo, що кількість слів $N=32$, а розрядність даних та ключа дорівнюють $R=L=8$. Формули для розрахунку часових і апаратних витрат для трьох типів АП наведено у табл.1, де враховано, що максимальне 8-розрядне двійкове число потребує 255 тактів операції декременту.

Таблиця 1 – Характеристики асоціативних процесорів

Тип АП	Апаратна складність, K	Часові витрати, t_a	Функціональні можливості
АП з паралельною вибіркою слів з регістрової пам'яті	$K = (K_{com}(8) + K_{rg} + K_t + K_{cd})N$	$t_a = t_{com} + t_{rd} + t_{cd}$	Пошук за ключем
АП з вибіркою слів по зрізах (слайзах) з регістрової пам'яті	$K = (K_{com}(1) + K_{rg} + K_t + K_{cd})N$	$t_a = 8(t_{com} + t_{rd}) + t_{cd}$	Пошук за ключем
АП з паралельно-послідовною обробкою з пам'яттю на лічильниках	$K = (K_{ct} + K_t)N$	$T_s = 255 \cdot \tau_{ct}$	Пошук за ключем, визначення екстремальних чисел
$K_{com}(8)$, $K_{com}(1)$ – складність відповідно 8-розрядного і 1-розрядного компаратора, K_{rg} – складність регістра; K_t – складність тригера; K_{cd} – складність шифратора; K_{ct} – складність лічильника			

Аналіз даних табл.1 показав, що максимальний час асоціативної вибірки у запропонованому АП більший за час, що витрачається на обробку у розглянутих прототипах. Але враховуючи наносекундний діапазон спрацювання базових вузлів обчислювальної техніки [19], ці часові витрати вкладаються у мікросекундний діапазон. Разом з тим значною перевагою запропонованого АП є регулярність структури та менша кількість апаратних витрат, адже у розглянутих прототипах для кожного елемента масиву

застосовується пам'ять фіксування співпадінь, яка складається з компаратора і тригера, та шифратора на кожний елемент масиву (рис.1), не враховуючи апаратних витрат на аналізатор багатократного співпадіння. А у запропонованому АП для операції декременту використовуються тільки лічильники з фіксуванням ознаки нуля без необхідності використання компаратора і регістра.

Отже, маємо вигреш в апаратних витратах, що є важливим при реалізації АП на перспективній елементній базі – ПЛІС. Крім того, виконання регістрової пам'яті у складі асоціативних процесорів можливе як на базі цифрових лічильників, так на оптоелектронних регістрах [16-18, 20].

Висновки

1. Проведений огляд сучасних методів і засобів асоціативної обробки масивів даних показав, що за організацією процесу такої обробки найбільше розповсюдження отримали паралельно-послідовні асоціативні процесори, як компромісні між дорогими паралельними і низькошвидкісними послідовними асоціативними процесорами. В результаті, серед методів асоціативної обробки найбільше розповсюдження отримав метод обробки по розрядних зрізах (слайзах), тобто з одночасною обробкою однойменних розрядів усіх слів.

2. Запропоновані структури двох асоціативних процесорів з дискретним поданням даних містять швидку регістрову пам'ять на лічильниках з паралельним пошуком по словах і послідовним по вмісту. Основними перевагами такого методу обробки є природний рівень паралелізму і те, що час виконання базових операцій пошуку пропорційний максимальному значенню серед чисел у заданому масиві даних або ключі.

3. У першому запропонованому варіанті в асоціативному процесорі для пошуку у масиві даних за ключем паралельно-послідовна обробка дозволяє зафіксувати співвідношення n операндів з ключем у вигляді бінарних ознак ($=$, \neq) в пам'яті результатів на тригерах. У другому запропонованому варіанті в асоціативному процесорі для пошуку екстремальних чисел розширення функціональних можливостей досягається за рахунок роботи в двох режимах: пошук мінімального або максимального числа у масиві n чисел. Особливістю запропонованих асоціативних процесорів є те, що кількість n операндів, що обробляються, може бути значною, а час виконання операції залежить тільки від їх інформативної ємності. Крім того, в обох випадках пошук виконується без паралельного порозрядного логічного порівняння, а в процесі швидкісної паралельної операції декременту, що виконується апаратно на лічильниках.

4. Однаковий підхід до обробки масивів даних у регістровій пам'яті на лічильниках дозволяє об'єднати функціональні можливості двох типів запропонованих асоціативних процесорів в одному асоціативному процесорі через подібність їх структурної організації за рахунок вдосконалення схем логічного вузла і вузла керування.

Список літератури

- [1] Ассоциативная обработка, [Электронный ресурс]. Режим доступа: <http://www.ngpedia.ru/id97447pl.html>. Дата звернення: Лют. 20, 2019.
- [2] Я. И. Фет, *Параллельные процессоры для управляющих систем*. М., Россия: Энергоиздат, 1981.
- [3] К. Дж. Тербер, *Архитектура высокопроизводительных вычислительных систем*. М., Россия: Наука. Гл. ред. физ.-мат. лит.-ры, 1985.
- [4] Т. Кохонен, *Ассоциативные запоминающие устройства*. М., Россия: Мир, 1982.
- [5] А. П. Писарев., и А. П. Ремонтов, *Вычислительные машины и системы: учебн. пособие*. Пенза, Россия: 2006.
- [6] М. Амамия, Ю. Танака, *Архитектура ЭВМ, искусственный интеллект*. М., Россия: Мир, 1993.
- [7] В. И. Козик, П. Е. Твердохлеб, «3-D оптические интегральные схемы ассоциативной памяти», *Автометрия*, № 3, с.44-52. 1993.
- [8] В. С. Бурцев, В. Б. Федоров, «Оптическая ассоциативная память для систем управления базами данных и вычислительных машин с нетрадиционной архитектурой», *Радиотехника*, № 7-8, с.79-89. 1992.
- [9] Smith D., Hall J., and Miyake K. The CAM2000 Chip Architecture. Rutgers University [Online]. Available: <http://ntrs.nasa.gov/19930017905.pdf>. Accessed on: Feb. 25, 2019.
- [10] А. А. Дерюгин, *Электронные вычислительные машины и системы: Основные термины, определения и обозначения*. М., Россия: Изд-во МЭИ(ТУ), 1992.
- [11] А. В. Богданов, В. В. Корхов, В. В. Мареев, и Е. Н. Станкова, *Архитектуры и топологии многопроцессорных вычислительных систем*. М., Россия: ИНТУИТ.РУ, 2009.
- [12] А. А. Вербовецкий, и В. Б. Федоров, «Оптические системы памяти с ассоциативно-адресной выборкой информации», *Квантовая электроника*, т.7, №8, с.1769-1777. 1980.
- [13] В.Б. Федоров, «Принципы создания многопортовой ассоциативной памяти с использованием элементной базы квантовой электроники», *Квантовая электроника*, №11, с.1155 - 1160. 1995.
- [14] А. В. Кожем'яко, Н. О. Денисюк, і С. В. Сидорук, «Аспекти реалізації асоціативного процесора», *на Всеукр. наук.-практ. конф. Проблеми інформатики та комп'ютерної техніки (ПІКТ-2014)*, Чернівці, 2014, с.106-107.
- [15] Л. М. Куперштейн, Н. О. Денисюк, і М. В. Повидало, «Особливості реалізації асоціативних операцій» *на IV*

міжнар. наук.-практ. конф. Методи та засоби кодування, захисту й ущільнення інформації, Вінниця, 2013, с.344-346.

- [16] Т. Б. Мартинюк, Н. О. Денисюк і С. П. Любич, «Оптоелектронний пристрій порівняння чисел», *Патент України* G06F7/00. №89886 МПК7 (2014), 12.05.2014.
- [17] Т. Б. Мартинюк, Н. О. Денисюк і Н. І. Кокряцька, «Оптоелектронний пристрій порівняння чисел», *Патент України* G06F7/00. №91393 МПК7 (2014), 10.07.2014.
- [18] Т. Б. Мартинюк, С. В. Павлов, А. В. Кожем'яко і Н. О. Денисюк, «Оптоелектронний пристрій для визначення екстремальних чисел», *Патент України* G 06F7/00. №91152 МПК7 (2014), 10.12.2014.
- [19] Electronic Components Datasheet Search [Online]. Available: <http://www.alldatasheet.com/> Accessed on: Mar. 10, 2019.
- [20] Т. Б. Мартинюк, Д. В. Кордон, і Н. О. Денисюк, «Асоціативна регістрова пам'ять», на VI міжнар. наук.-техн. конф. *Оптоелектронні інформаційні технології «Фотоніка ОДС - 2012»*, Вінниця, 2012, с.55.

References

- [1] Assotsyativnaia obrabotka, [Elektronnyi resurs]. Rezhym dostupu: <http://www.ngpedia.ru/id97447pl.html>. Data zvernennia: Liut. 20, 2019.
- [2] Ya. Y. Fet, *Parallelnye protsessory dlia upravliaiushchikh system*. M., Rossyia: Enerhoizdat, 1981.
- [3] K. Dzh. Terber, *Arkhytektura vysokoproizvoditelnykh vychyslytelnykh system*. M., Rossyia: Nauka. Hl. red. fiz.-mat. lyt-ry, 1985.
- [4] T. Kokhonen, *Assotsyativnye zapomynaiushchye ustroistva*. M., Rossyia: Myr, 1982.
- [5] A. P. Pysarev., y A. P. Remontov, *Vychyslytelnye mashyny y systemy: uchebn. posobie*. Penza, Rossyia: 2006.
- [6] M. Amamyia, Yu. Tanaka, *Arkhytektura ЭВМ, yskusstvennyi yntelekt*. M., Rossyia: Myr, 1993.
- [7] V. Y. Kozyk, P. E. Tverdokhle, «3-D opticheskiye yntehralnye skhemy assotsyativnoi pamiaty», *Avtometriya*, № 3, s.44-52. 1993.
- [8] V. S. Burtsev, V. B. Fedorov, «Opticheskaia assotsyativnaia pamiat dlia system upravleniya bazamy dannykh y vychyslytelnykh mashyn s netradytsyonnoi arkhytekturoi», *Radyotekhnika*, № 7-8, s.79-89. 1992.
- [9] Smith D., Hall J., and Miyake K. The CAM2000 Chip Architecture. Rutgers University [Online]. Available: <http://ntrs.nasa.gov/19930017905.pdf>. Accessed on: Feb. 25, 2019.
- [10] A. A. Deriuhyn, *Ehlektronnye vychyslytelnye mashyny y systemy: Osnovnye terminy, opredeleniya y oboznacheniya*. M., Rossyia: Yzd-vo MЭY(TU), 1992.
- [11] A. V. Bohdanov, V. V. Korkhov, V. V. Mareev, y E. N. Stankova, *Arkhytektury y topolohyy mnohoprotsessornykh vychyslytelnykh system*. M., Rossyia: YNTUYT.RU, 2009.
- [12] A. A. Verbovetskyi, y V. B. Fedorov, «Opticheskiye systemy pamiaty s assotsyativno-adresnoi vyborkoi ynformatsyy», *Kvantovaia ehlektronyka*, t.7, №8, s.1769-1777. 1980.
- [13] V. B. Fedorov, «Pryntsypy sozdaniya mnohoportovoi assotsyativnoi pamiaty s yspolzvanym elementnoi bazy kvantovoi ehlektronyky», *Kvantovaia ehlektronyka*, №11, s.1155 - 1160. 1995.
- [14] A. V. Kozhemiako, N. O. Denysiuk, i S. V. Sydoruk, «Aspekty realizatsii asotsyativnoho protsesora», *na Vseukr. nauk.-prakt. konf. Problemy informatyky ta kompiuternoї tekhniki (PIKT-2014)*, Chernivtsi, 2014, s.106-107.
- [15] L. M. Kupershtein, N. O. Denysiuk, i M. V. Povydalo, «Osoblyvosti realizatsii asotsyativnykh operatsii» *na IV mizhnar. nauk.-prakt. konf. Metody ta zasoby koduvannia, zakhystu y ushchilnennia informatsii*, Vinnytsia, 2013, s.344-346.
- [16] Т. В. Мартинюк, Н. О. Денисюк і С. П. Любич, «Оптоелектронний пристрій порівняння чисел», *Patent Ukrainy* G06F7/00. №89886 МПК7 (2014), 12.05.2014.
- [17] Т. В. Мартинюк, Н. О. Денисюк і Н. І. Кокриятська, «Оптоелектронний пристрій порівняння чисел», *Patent Ukrainy* G06F7/00. №91393 МПК7 (2014), 10.07.2014.
- [18] Т. В. Мартинюк, С. В. Павлов, А. В. Козем'яко і Н. О. Денисюк, «Оптоелектронний пристрій для визначення екстремальних чисел», *Patent Ukrainy* G 06F7/00. №91152 МПК7 (2014), 10.12.2014.
- [19] Electronic Components Datasheet Search [Online]. Available: <http://www.alldatasheet.com/> Accessed on: Mar. 10, 2019.
- [20] Т. В. Мартинюк, Д. В. Кордон, і Н. О. Денисюк, «Асоціативна регістрова пам'ять», *na VI mizhnar. nauk.-tekh. konf. Optoelektronni informatsiini tekhnolohii «Fotonika ODS - 2012»*, Vinnytsia, 2012, s.55.

Мартинюк Тетяна Борисівна - д.т.н., професор кафедри обчислювальної техніки, Вінницький національний технічний університет.

Денисюк Наталія Олексіївна - магістр факультету комп'ютерних систем і автоматики, Вінницький національний технічний університет.

Круківський Богдан Ігорович - магістр факультету комп'ютерних систем і автоматики, Вінницький національний технічний університет.

T. B. Martyniuk, N. O. Denysiuk, B. I. Krukivskyi

**ASSOCIATIVE PROCESSORS WITH PARALLEL-SERIAL
DATA PROCESSING**

Vinnitsia National Technical University, Vinnitsia

Т. Б. Мартынюк, Н. А. Денисюк, Б. И. Круковский

**АССОЦИАТИВНЫЕ ПРОЦЕССОРЫ С ПАРАЛЛЕЛЬНО-
ПОСЛЕДОВАТЕЛЬНОЙ ОБРАБОТКОЙ ДАННЫХ**

Винницкий национальный технический университет, г. Винница

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 519.6

Я. В. Іванчук, А. А. Яровий, К. О. Коваль

МЕТОД ЧИСЕЛЬНОГО МОДЕЛЮВАННЯ
ГІДРОДИНАМІЧНИХ ПРОЦЕСІВ

Вінницький національний технічний університет, м. Вінниця

Анотація. У даній статті наведений чисельний метод моделювання, який застосовується при дослідженні динаміки суцільних в'язких слабостиснених рідин на основі системи рівнянь нерозривності і Нав'є-Стокса. У запропонованому методі використовується комплексний підхід використання чисельного розв'язку рівняння нерозривності методом кінцевих об'ємів, а для розв'язку рівняння Нав'є-Стокса метод розщеплення по фізичним факторам. У статті показано, що метод кінцевих об'ємів, який застосовувався для опису течії як стисненої, так і нестисненої рідин володіє такими важливими перевагами, як наявність хороших консервативних властивостей і допущення дискретизації складних обчислювальних областей в більш прості, чим це дозволяє ізопараметричне кінцево-елементне формулювання задачі або введення узагальнених координат. У метод розщеплення по фізичним факторам вводиться складова, яка враховує штучну стислість досліджуваної рідини, що дозволяє спочатку розрахувати проміжкове поле швидкостей, яке потім підправляється із врахуванням градієнти тиску. Різницева схема даного методу дозволяє розраховувати поле течії без використання значень вихору і тиску на твердій поверхні. У рамках запропонованого підходу не потрібно розраховувати значення вихору на твердій поверхні. Останнє може бути знайдене по обчисленому полю швидкостей із використанням якогонебудь із різницьких представлень виразу для вихору в граничних точках. Для підтвердження ефективності запропонованого методу, в CFD-програмі FlowVision були отримані розв'язки цілого ряду задач зовнішньої гідродинаміки, на прикладі оптикання циліндричної поверхні, які підтвердили стійкість отриманих результатів. Даний метод дозволяє проводити по єдиному алгоритму розрахунки оптикання плоских, осесиметричних і тривимірних тіл складної конфігурації потоком в'язкої слабостисненої рідини, а також внутрішніх течій в широкому діапазоні чисел Рейнольдса.

Ключові слова: рівняння Нав'є-Стокса, чисельне моделювання, алгоритм, тиск, швидкість, різницева схема.

Аннотация. В данной статье приведен численный метод моделирования, который применяется при исследовании динамики сплошных вязких слабосжатых жидкостей на основе системы уравнений неразрывности и Навье-Стокса. В предложенном методе используется комплексный подход использования численного решения уравнения неразрывности методом конечных объемов, а для решения уравнения Навье-Стокса метод расщепления по физическим факторам. В статье показано, что метод конечных объемов, который применялся для описания течения как сжатой, так и несжатой жидкостей обладает такими важными преимуществами, как наличие хороших консервативных свойств и допущения дискретизации сложных вычислительных областей в более простые, чем это позволяет изопараметрическая конечно-элементная формулировка задачи или введение обобщенных координат. В метод расщепления по физическим факторам вводится составляющая, которая учитывает искусственную сжимаемость исследуемой жидкости, что позволяет сначала рассчитать промежуточное поле скоростей, которое затем подправляется с учетом градиенты давления. Разностная схема данного метода позволяет рассчитывать поле течения без использования значений вихря и давления на твердой поверхности. В рамках предложенного подхода не нужно рассчитывать значение вихря на твердой поверхности. Последнее может быть найдено по вычисленному полю скоростей с использованием какого-либо из разностных представлений выражения для вихря в граничных точках. Для подтверждения эффективности предложенного метода, в CFD-программе FlowVision были получены решения целого ряда задач внешней гидродинамики, на примере оптиканья цилиндрической поверхности, которые подтвердили устойчивость полученных результатов. Данный метод позволяет проводить по единому алгоритму расчеты обтекания плоских, осесимметричных и трехмерных тел сложной конфигурации потоком вязкой слабосжатой жидкости, а также внутренних течений в широком диапазоне чисел Рейнольдса.

Ключевые слова: уравнения Навье-Стокса, численное моделирование, алгоритм, давление, скорость, разностная схема.

Abstract. This article presents a numerical simulation method that is used in the study of the dynamics of continuous viscous weakly compressed fluids based on the system of equations of continuity and Navier-Stokes. The proposed method uses a complex approach using the numerical solution of the continuity equation by the finite-volume method, and for solving the Navier-Stokes equation the splitting method by physical factors. The article shows that the finite volume method, which was used to describe the flow of both compressed and uncompressed liquids, has such important advantages as the presence of good conservative properties and assumptions of discretization of complex computational domains into simpler ones than isoparametric finite element formulation of the problem or the introduction of generalized coordinates. A component is introduced into the method of splitting according to physical factors, which takes into account the artificial compressibility of the test liquid, which allows you to first calculate the intermediate velocity field, which is then corrected taking into account the pressure gradients. The difference scheme of this method allows one to calculate the flow field without using the values of the vortex and pressure on a solid surface. In the framework of the proposed approach, it is not necessary to calculate the value of the vortex on a solid surface. The latter can be found from the calculated velocity field using any of the difference representations of the expression for the vortex at the boundary points. To confirm the effectiveness of the proposed method, in the FlowVision CFD program, solutions were obtained for a number of problems in external hydrodynamics, using the example of a cylindrical surface optics, which confirmed the stability of the results obtained. This method allows one to compute the flow of flat, axisymmetric, and three-dimensional bodies of a complex configuration with a flow of a viscous weakly compressed fluid, as well as internal flows in a wide range of Reynolds numbers using a single algorithm.

Key words: Navier-Stokes equations, numerical simulation, algorithm, pressure, speed, difference scheme.

DOI: <https://doi.org/10.31649/1999-9941-2019-44-1-37-45>.

Вступ

Сучасний етап розвитку нелінійної механіки характеризується широким і глибоким використанням самих тонких ефектів; вона все більше взаємодіє з іншими областями науки і техніки. Однією із характерних рис сучасних досліджень є математизація фізичного пізнання, інтенсивне застосування методів математичного моделювання в різних галузях науки і техніки. Поява сучасних потужних комп'ютерних

систем (КС) [1] значно підвищило інтерес до різних чисельних методів і алгоритмів, реалізація яких межує із проведенням чисельного експерименту, який відображає процес отримання результатів при чисельному моделюванні. Потреба у такому підході до розв'язку задач математичної фізики диктується все більш ускладнюючими запитами практики, а також зв'язана із спробою створення більш раціональних загальних теоретичних моделей для вивчення складних фізичних явищ.

Актуальність

Однією із сучасних актуальних наукових проблем в гідромеханіці є опис руху в'язкої слабостисненої рідини, яка описується рівняннями нерозривності і Нав'є-Стокса [2]. Сюди відносяться задачі руху рідини при ламінарному і турбулентному обтіканні тіл кінцевих розмірів; течії в зоні сліду і областях зриву потоку, в шарах змішування; в пограничних шарах у поверхні тіла тощо [3]. Поява сучасних потужних КС надало новий імпульс цим дослідженням, що дозволило отримати кількісні результати при розв'язку практично важливих задач про рух реальної рідини при помірних числах Рейнольдса. Нелінійність рівнянь Нав'є-Стокса і наявність малих параметрів при старших похідних в них створюють серйозні труднощі, як при аналітичному дослідженні так і при чисельному інтегруванні цих рівнянь за допомогою КС. Таким чином, проблема побудови чисельних алгоритмів для розв'язку системи рівнянь нерозривності і Нав'є-Стокса з високою точністю (особливо в багатомірному випадку) залишається на сьогодні актуальною задачею.

У роботах [4, 5] був розроблений чисельний метод стосовно до (ψ, ω) – системи рівнянь для функції току ψ і вихору ω . Загальним недоліком цих методів є використання в тому чи іншому вигляді граничної умови для вихору на твердій поверхні, яке відсутнє у фізичній постановці задачі. Наявність додаткового ітераційного процесу, зв'язаного із цією граничною умовою, обмежує швидкість збіжності чисельних алгоритмів. Крім того, очевидна обмеженість методів розв'язку (ψ, ω) – системи, зв'язана із неможливістю розвитку їх на випадок просторових течій в'язкої рідини і течій стисненого газу.

У роботі [6] був запропонований оригінальний метод «частинок в комірках», який в собі поєднує переваги лагранжева і ейлерова підходів [4]. Область розв'язку в даному методі розбиваються нерухомою (ейлеровою) сіткою; проте суцільне середовище трактується дискретною моделлю – розглядається сукупність «частинок» фіксованої маси (лагранжева сітка частинок), які і рухаються через ейлерову сітку комірок. Частинки служать для визначення параметрів самої рідини (маси, енергії, швидкості), в той час як ейлерова сітка використовується для визначення параметрів поля (тиску, густини, температури). Даний метод дозволяє досліджувати складні явища в динаміці багатокомпонентних середовищ, частинки добре слідкують за вільними поверхнями і лініями розділу середовищ тощо. Але основним недоліком даного методу є дискретне представлення суцільного середовища наслідком чого є чисельна нестійкість (флуктуації). Також важко отримати інформацію для областей із значним розрідженням, звідки практично уходять усі частинки.

Мета

Метою даної роботи є розробка ефективного чисельного методу розв'язку багатомірної системи рівнянь нерозривності і Нав'є-Стокса при помірних числах Рейнольдса, який має хороші консервативні властивості і допущення дискретизації складних обчислювальних областей, що призводить до стійкості результатів розрахунку і здатний досить точно описати локальні властивості течій.

Задачі

Для досягнення поставленої мети вирішувалися наступні задачі:

1. Розглянути постановку задачі динаміки суцільної в'язкої слабостисненої рідини;
2. Розробити ефективний метод який дозволить досліджувати широкий клас плоских, вісесиметричних і просторових задач динаміки в'язкої слабостисненої рідини;
3. За допомогою розробленого метода виконати розрахунок задачі просторово-нестационарного обтікання тіла потоком в'язкої слабостисненої рідини.

Розв'язання задач

Як було показано любий реальний гідродинамічний процес може бути описаний системою диференціальних рівнянь в частинних похідних, яка складається із рівняння нерозривності [2, 7] і рівняння Нав'є-Стокса [8].

Для розв'язку рівняння нерозривності [2] використаємо метод кінцевих об'ємів. Представимо рівняння нерозривності невстановленого руху рідини у загальному вигляді для площини Oxy :

$$\frac{\partial \bar{q}}{\partial t} + \frac{\partial \bar{F}}{\partial t} + \frac{\partial \bar{G}}{\partial t} = 0, \quad (1)$$

де $\bar{q} = \bar{\rho}$ – густина рідини, $\bar{F} = \bar{\rho}\bar{u}_x$ – компонента швидкості рідини по вісі x , $\bar{G} = \bar{\rho}\bar{u}_y$ – компонента швидкості рідини по вісі y .

Застосовуючи метод підобластей [8] до рівняння (1) в середині кінцевого об'єму, що показаний на рисунку 1, отримуємо:

$$\int_{ABCD} 1 \left(\frac{\partial \bar{q}}{\partial t} + \frac{\partial \bar{F}}{\partial t} + \frac{\partial \bar{G}}{\partial t} \right) dx dy = 0, \quad (2)$$

або, якщо застосувати теорему Гріна [9]:

$$\frac{d}{dt} \int \bar{q} dV + \int_{ABCD} \bar{H} \cdot \bar{n} ds = 0, \quad (3)$$

де $\bar{H} = (\bar{F}, \bar{G})$. У декартових координатах маємо:

$$\bar{H} \cdot \bar{n} ds = \bar{F} dy - \bar{G} dx. \quad (4)$$

Рівняння (3) є констатацією консервативності [3, 8]. У частинному випадку, якщо обрати $\bar{q} = \bar{\rho}$, $\bar{F} = \bar{\rho}\bar{u}_x$, $\bar{G} = \bar{\rho}\bar{u}_y$, рівняння (3) співпадає з інтегральним формулюванням закону збереження маси [3]. Відповідно, метод кінцевих об'ємів зводиться до дискретизації вихідного рівняння, представленого в інтегральній формі [10], у протилежність методу кінцевих різниць [4, 9], який застосовується до вихідного рівняння в його диференційній формі.

Одним із приблизних представлень рівняння (3) може бути рівняння:

$$\frac{d}{dt} (\Lambda q_{j,k}) + \sum_{AB}^{DA} (F \Delta y - G \Delta x) = 0, \quad (5)$$

де Λ – площа чотирикутника $ABCD$, показаного на рисунку 1, причому $q_{j,k}$ є величина, яка зв'язана із середнім значенням q в середині чотирикутника. У рівнянні (5):

$$\Delta y_{AB} = y_B - y_A; \Delta x_{AB} = x_B - x_A; F_{AB} = 0,5(F_{j,k-1} + F_{j,k}); G_{AB} = 0,5(G_{j,k-1} + G_{j,k}), \quad (6)$$

І аналогічні вирази для Δy_{BC} і т. д. Якщо Λ не є функцією часу, тоді рівняння (5) приймає вигляд:

$$\begin{aligned} \Lambda \frac{dq_{j,k}}{dt} + 0,5(F_{j,k-1} + F_{j,k})\Delta y_{AB} - 0,5(G_{j,k-1} + G_{j,k})\Delta x_{AB} + 0,5(F_{j,k-1} + F_{j+1,k})\Delta y_{BC} - \\ - 0,5(G_{j,k} + G_{j+1,k})\Delta x_{BC} + 0,5(F_{j,k} + F_{j,k+1})\Delta y_{CD} - 0,5(G_{j,k} + G_{j,k+1})\Delta x_{CD} + \\ + 0,5(F_{j-1,k} + F_{j,k})\Delta y_{DA} - 0,5(G_{j-1,k} + G_{j,k})\Delta x_{DA} = 0. \end{aligned} \quad (7)$$

Якщо глобальна сітка (j, k) є нерегульованою, тоді записане для кінцевих об'ємів рівняння (7) забезпечує дискретизацію в декартових координатах, без необхідності введення узагальнених координат [9]. Якщо загальна сітка є однорідною і її лінії співпадають із лініями постійних x і y , тоді рівняння (7) приймає вигляд:

$$\begin{aligned} \Delta x \Delta y \frac{d}{dt} q_{j,k} - 0,5(G_{j,k-1} + G_{j,k})\Delta x + 0,5(F_{j,k} + F_{j+1,k})\Delta y + \\ + 0,5(G_{j,k} + G_{j,k+1})\Delta x - 0,5(F_{j-1,k} + F_{j,k})\Delta y = 0, \end{aligned}$$

або

$$\frac{d}{dt} q_{j,k} + \frac{F_{j,k} + F_{j+1,k}}{2\Delta x} + \frac{G_{j,k+1} + G_{j,k-1}}{2\Delta y} = 0, \quad (8)$$

що співпадає із апроксимацією, отриманою при представленні просторових кривих похідних в (1) за допомогою центральних різниць.

Метод кінцевих об'ємів, який застосовувався для опису течії як стисненої, так і нестисненої рідин володіє двома важливими перевагами. По-перше, він володіє хорошими консервативними властивостями (збереження маси тощо). По-друге, він допускає дискретизацію складних обчислювальних областей в більш простій, хоча і не обов'язково в такій же точній формі, чим це дозволяє ізопараметричне кінцево-елементне формулювання [11] або введення узагальнених координат [9].

Розглянемо рівняння Нав'є-Стокса в природних змінних:

$$\frac{\partial \bar{V}}{\partial t} + (\bar{V} \nabla) \bar{V} = -\nabla p + \nu \Delta \bar{V}, \quad \nabla \bar{V} = 0. \quad (9)$$

де ν – кінематична в'язкість досліджуваної рідини.

Для рішення проблеми із розрахунком поля тиску необхідно в рівняння нерозривності ввести член, який відповідає за шгучну стисливість, а саме: $(\partial / \partial t)(p + V^2 / 2)$. У результаті ми отримуємо модифіковану систему рівнянь:

$$\begin{cases} \frac{\partial \bar{V}}{\partial t} + (\bar{V} \nabla) \bar{V} = -\nabla p + \nu \Delta \bar{V}; \\ \frac{\partial \left(p + \frac{V^2}{2} \right)}{\partial t} + \nabla V = 0, \end{cases} \quad (10)$$

для розв'язку якої використаємо метод розщеплення по фізичним факторам.

Введемо наступні позначення: $\nabla \times \bar{V} = \omega$, $\nabla \bar{V} = D$, $\nabla \bar{V} = \tilde{D}$. Нехай у деякий момент часу $t_n = n\tau$ (τ – крок по часу, n – число кроків) відомі поля швидкості \bar{V} і тиску p рідини. Тоді схему визначення невідомих функцій в момент часу $t_{n+1} = (n+1)\tau$ можна представити у вигляді триетапної схеми розщеплення:

Етап I:

$$\frac{\bar{V} - \bar{V}^n}{\tau} = -(\bar{V}^n \nabla) \bar{V}^n + \nu \Delta \bar{V}^n. \quad (11)$$

Етап II:

$$\Delta p = -\frac{\tilde{D}}{\tau}, \quad \text{так як } D^{n+1} = 0. \quad (12)$$

Етап III:

$$\frac{\bar{V}^{n+1} - \bar{V}}{\tau} = -\nabla p. \quad (13)$$

Рівняння (13) отримуємо шляхом взяття дивергенції від обох частин рівності (9) із урахуванням рівняння нерозривності (умова соленоїдності [13] $\text{div} \bar{V}^{n+1} = 0$).

Розглянемо наступну фізичну інтерпретацію схеми розщеплення. На етапі I припускається, що перенос кількості руху (імпульсу одиниці маси) здійснюється тільки за рахунок конвекції або дифузії.

Отримане таким чином проміжне поле швидкості \bar{V} , не задовольняє умові нестисливості ($\tilde{D} \neq 0$). Слід

відмітити, що проміжне поле швидкості \bar{V} має досить визначений фізичний зміст. Дійсно, якщо застосувати оператор rot до вихідного рівняння (9) і до рівняння (11), а також врахувати, що $\text{rot} \bar{V} = \text{rot} \bar{V}^{n+1} = \omega^{n+1}$, тобто вже на етапі I проміжне поле швидкості у внутрішніх точках досліджуваної області течії зберігає вихрові характеристики.

На етапі II по знайденому проміжному полю швидкості із врахуванням умови соленоїдності вектору швидкості \bar{V}^{n+1} знаходиться поле тиску.

На етапі III пропонується, що перенос здійснюється тільки за рахунок градієнта тиску (конвекція або дифузія відсутні).

Таким чином, обчислювальний цикл має наступний вигляд: I – по відомому в початковий (або попередній) момент часу полю швидкості із рівняння (11) знаходиться проміжне поле швидкості, визначаючи тим самим праву частину рівняння (12); II – розв'язується рівняння Пуассона (12) для визначення тиску; III – підправляється остаточно (на даному шарі рідини по часу) поле швидкості (13). Цикл повторюється до виконання деякого критерію встановлення (якщо існує стаціонарний розв'язок) або до заданого моменту часу.

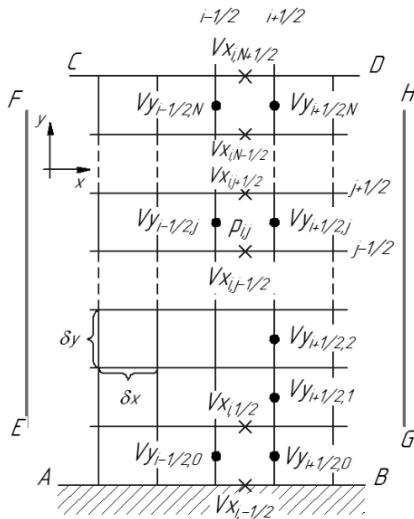


Рисунок 2 – Схема сіткового шаблону для метода розщеплення (двовірний випадок)

Для випадку декартової системи координат і рівномірної сітки (рис. 2) двовірний різницевий вигляд має наступний вигляд:

$$\begin{aligned} \frac{\tilde{V}_{y_{i+1/2,j}} - V_{y_{i+1/2,j}}^n}{\tau} = & \frac{(V_{y_{i,j}}^n)^2 - (V_{y_{i+1,j}}^n)^2}{h_1} + \\ & + \frac{(V_y V_x)_{i+1/2,j-1/2}^n - (V_y V_x)_{i+1/2,j+1/2}^n}{h_2} - \\ & - \frac{\nu}{\Delta y} \left[\left(\frac{V_{x_{i+1,j+1/2}}^n - V_{x_{i,j+1/2}}^n}{h_1} - \frac{V_{y_{i+1/2,j+1}}^n - V_{y_{i+1/2,j}}^n}{h_2} \right) - \right. \\ & \left. - \left(\frac{V_{x_{i+1,j-1/2}}^n - V_{x_{i,j-1/2}}^n}{h_1} - \frac{V_{y_{i+1/2,j}}^n - V_{y_{i+1/2,j-1}}^n}{h_2} \right) \right]; \end{aligned} \quad (14)$$

$$\begin{aligned} \frac{\tilde{V}_{x_{i,j+1/2}} - V_{x_{i,j+1/2}}^n}{\tau} = & \frac{(V_{x_{i,j}}^n)^2 - (V_{x_{i,j+1}}^n)^2}{h_2} + \frac{(V_y V_x)_{i-1/2,j+1/2}^n - (V_y V_x)_{i+1/2,j+1/2}^n}{h_1} + \\ & + \frac{\nu}{h_1} \left[\left(\frac{V_{x_{i+1,j+1/2}}^n - V_{x_{i,j+1/2}}^n}{h_1} - \frac{V_{y_{i+1/2,j+1}}^n - V_{y_{i+1/2,j}}^n}{h_2} \right) - \right. \\ & \left. - \left(\frac{V_{x_{i,j+1/2}}^n - V_{x_{i-1,j+1/2}}^n}{h_1} - \frac{V_{y_{i-1/2,j+1}}^n - V_{y_{i-1/2,j}}^n}{h_2} \right) \right]; \end{aligned} \quad (15)$$

$$\begin{cases} \frac{p_{i+1,j} - 2p_{i,j} + p_{i-1,j}}{h_1^2} + \frac{p_{i,j+1} - 2p_{i,j} + p_{i,j-1}}{h_2^2} = \frac{D_{i,j}}{\tau}, \\ D_{i,j}^{n+1} = 0, \end{cases} \quad (16)$$

$$\begin{cases} V_{y_{i+1/2,j}}^{n+1} = \tilde{V}_{y_{i+1/2,j}} - \frac{\tau}{h_1} (p_{i+1,j} - p_{i,j}), \\ V_{x_{i,j+1/2}}^{n+1} = \tilde{V}_{x_{i,j+1/2}} - \frac{\tau}{h_2} (p_{i,j+1} - p_{i,j}). \end{cases} \quad (17)$$

Схема (14) – (17) легко апроксимує рівняння (11) – (13) із другим порядком точності по просторовим змінним похибка апроксимації порядку $O(\tau, h^2)$, де $h = \max(\Delta x, \Delta y)$, де $h_1 = \Delta x$, $h_2 = \Delta y$.

Суттєвим моментом запропонованого метода є вибір граничних умов. Із-за наявності задач обтікання тіл кінцевих розмірів потоком в'язкої нестисненої рідини, можна виділити два основних типи граничних умов: умова на твердій поверхні і умова на лінії, достатньо віддаленій від обтікаючого тіла. Тобто, граничні умови на твердій поверхні (див. рис. 2):

$$\begin{cases} V_{x_{i,j-1/2}}^n = 0; \quad (\text{умова неперотікання}) \\ V_{y_{i+1/2,j-1/2}}^n = 0, \quad (\text{умова прилипання}) \end{cases} \quad (18)$$

із останнього випливає:

$$\tilde{V}_{y_{i+1/2,0}} = \frac{V_{y_{i+1/2,0}}^n}{2} + \frac{V_{y_{i+1/2,1}}^n}{6} + O(h_2^3). \quad (19)$$

Умова (19) дозволяє звільнитися від необхідного введення шару фіктивних комірок (усередині твердого тіла), що в багатьох розрахункових схемах [5] приводить до неявного обчислення значення вихору на твердій поверхні з першим порядком точності.

Замітимо, що у рамках запропонованого підходу не потрібно розраховувати значення вихору на твердій поверхні. Останнє може бути знайдене по обчисленому полю швидкостей із використанням якогось-небудь із різницевих представлень виразу для вихору в граничних точках:

$$\omega = \frac{\partial V_y}{\partial y} - \frac{\partial V_x}{\partial x}. \quad (20)$$

Граничні умови на лінії, віддалені від обтікаючого тіла (EF , CD , GH) (див. рис. 2), є умови у незбуреному потоці, які у випадку $U_\infty \parallel OX$ мають вигляд (наприклад, на CD):

$$V_{x_{i,N+1/2}}^n = 0, \quad V_{y_{i+1/2,N}}^n = 0. \quad (21)$$

При розрахунку поля тиску отримання однорідних граничних умов забезпечується із використанням підходу [7], який заключається в наступному. Вважаючи $V_{x_{i,N-1/2}}^{n+1} = 0$ (для випадку твердої поверхні) і $V_{x_{i,N+1/2}}^{n+1} = 0$ (для випадку лінії, яка віддалена від тіла), із (17) маємо:

$$\tilde{V}_{x_{i,N-1/2}} = \frac{\tau}{h_2} (p_{i,0} - p_{i,N-1}), \quad \tilde{V}_{x_{i,N+1/2}} = \frac{\tau}{h_2} (p_{i,N+1} - p_{i,N}). \quad (22)$$

Із урахуванням (22) різницеве рівняння для розрахунку тиску в пограничних комірках прийме вигляд:

$$p_{i,0} = \frac{1}{\frac{2\tau_0}{h_1^2} + \frac{2\tau}{h_2^2}} \left(\tau_0 \frac{p_{i-1,0} + p_{i+1,0}}{h_1^2} + \frac{p_{i,1} + p_{i,0}}{h_2^2} - \tilde{D}_{i,0'} \right), \quad (23)$$

де

$$\tilde{D}_{i,0'} = \frac{\tilde{V}_{y_{i+1/2,0}} - \tilde{V}_{y_{i-1/2,0}}}{h_1} + \frac{\tilde{V}_{x_{i,j+1/2}}}{h_2}, \quad \tau_0 = \frac{h_2^2}{8\nu}. \quad (24)$$

Аналогічно виписується співвідношення для $p_{i,N}$.

Чисельна реалізація запропонованого метода включає наступні три етапи.

Етап I. Із рівняння (14) визначаються значення $\tilde{V}_{y_{i+1/2,j}}$, $\tilde{V}_{x_{i,j+1/2}}$ із використанням умов (18) (за виключенням пограничних значень $\tilde{V}_{y_{i+1/2,0}}$). По розрахованим значенням $V_{y_{i+1/2,j}}^n$ у внутрішніх вузлах області із (19) знаходяться $\tilde{V}_{y_{i+1/2,0}}$.

Етап II. Поле тиску визначається із (16). У пограничних комірках використовуються співвідношення (23).

Етап III. Із (17) знаходяться значення $V_{y_{i+1/2,j}}^{n+1}$, $V_{x_{i,j+1/2}}^{n+1}$. У якості початкового наближення $V_{y_{i+1/2,j}}^{n+1}$, $V_{x_{i,j+1/2}}^{n+1}$ вибираються довільні функції, які задовольняють необхідні граничні умови.

Стаціонарний розв'язок системи рівнянь (14) – (17) отримуємо в результаті повторення вказаних етапів до виконання наступного критерію встановлення:

$$\max_{i,j} \left| V_{y_{i+1/2,j}}^{n+k} - V_{y_{i+1/2,j}}^n \right| \leq \varepsilon. \quad (25)$$

Дослідження стійкості можна провести поетапно. Критерій стійкості першого етапу може бути отриманий за допомогою першого диференційного наближення [8]. Стосовно до рівнянь (14) перше диференційне наближення має вигляд:

$$\begin{cases} \frac{\partial V_y}{\partial t} + \frac{\partial V_y^2}{\partial x} + \frac{\partial V_y V_x}{\partial y} = \left(\nu - \frac{\tau}{2} V_y^2 \right) \frac{\partial^2 V_y}{\partial x^2} + \left(\nu - \frac{\tau}{2} V_x^2 - \frac{h_2^2}{4} \frac{\partial V_x}{\partial y} \right) \frac{\partial^2 V_y}{\partial y^2}; \\ \frac{\partial V_x}{\partial t} + \frac{\partial V_y V_x}{\partial x} + \frac{\partial V_y^2}{\partial y} = \left(\nu - \frac{\tau}{2} V_y^2 - \frac{h_1^2}{4} \frac{\partial V_y}{\partial x} \right) \frac{\partial^2 V_x}{\partial x^2} + \left(\nu - \frac{\tau}{2} V_x^2 \right) \frac{\partial^2 V_x}{\partial y^2}. \end{cases} \quad (26)$$

Із (26) випливає критерій стійкості, який використовує різницеву схему ($h_1=h_2$):

$$\tau = \frac{4\nu}{V_x^2 + V_y^2}. \quad (27)$$

Виключивши p із (16) і (17), за допомогою методу Фур'є [12] легко показати безумовну стійкість другого і третього етапів.

За допомогою описаного метода в CFD-програмі FlowVision [11], на потужностях КС Інститута кібернетики ім. В. М. Глушкова НАН України, були отримані розв'язки цілого ряду задач зовнішньої гідродинаміки [2, 13]. Розглянемо деякі результати розв'язку задачі для поперечного обтікання кругового циліндра радіуса $a=1$ м, вісь якого перпендикулярна вектору швидкості набігаючого потоку U_∞ на на 250000 розрахункових комірках. Картини течії для різних чисел Рейнольдса ($Re=2aU_\infty/\nu$) представлені на рисунку 3.

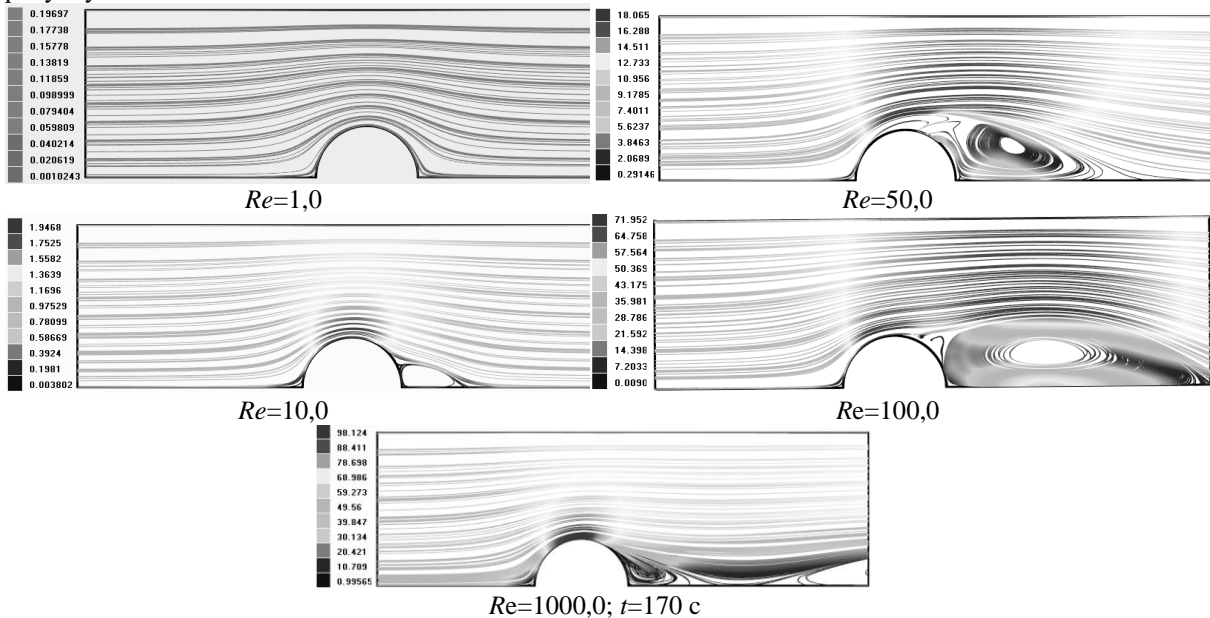


Рисунок 3 – Схема обтікання циліндру (лінії току) при різних числах Рейнольдса

Також на рисунку 3 представлені числові дані швидкості (м/с) набігаючого потоку рідини. В останньому випадку ($Re=1000,0; t=170$ с) (див. рис. 3) спостерігається нестационарна картина течії (має місце визначений ріст застійної зони і в деякий момент часу відбувається).

На рисунку 4 представлені результати розрахунку даним методом (криві 1) в порівнянні із результатами, отриманими за допомогою методу спільної блочної релаксації [5] (криві 2).

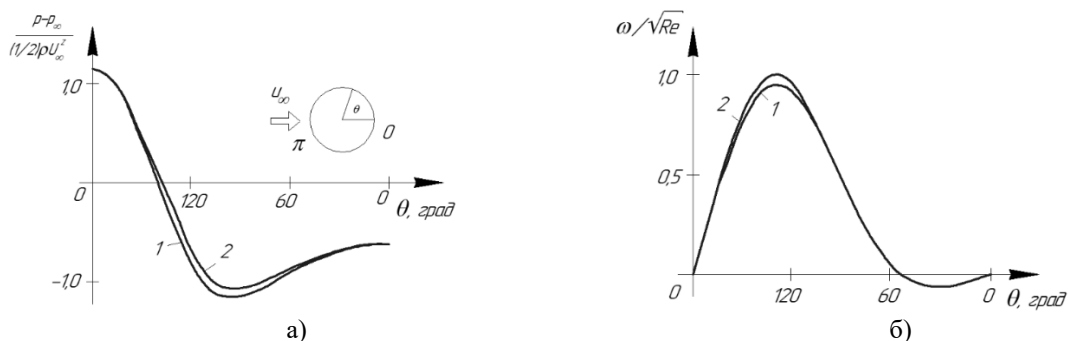


Рисунок 4 – Діаграма розподілу тиску (а) і вихору (б) по поверхні циліндру при $Re=50$: 1 – розрахунок вищевказаним методом; 2 – розрахунок методом [6]

Отримані результати показали високу збіжність результатів розрахунку на кутах до 60° і на кутах біля 180° для розподілу тиску (див. рис 4, а) і вихору (див. рис 4, б) течії рідини по поверхні циліндру при $Re=50$.

Висновки

1. Запропонований метод чисельного моделювання гідродинамічних процесів має певні сильні сторони в порівнянні із відомими чисельними методами [4-6], де різниці в представлення виконання умови прилипання приводить, із необхідністю, до визначення граничного значення вихору на твердій поверхні тіла, наслідком чого є відсутність балансу сил на твердій поверхні.

2. Різницева схема даного методу дозволяє розраховувати поле течії без використання значень вихору і тиску на твердій поверхні. Результати проведених розрахунків, а також пробні розрахунки тривимірних течій, виконані із використанням даного підходу, свідчать про його ефективність.

3. Також даний метод дозволяє проводити по єдиному алгоритму розрахунки обтікання плоских, осесиметричних і тривимірних тіл складної конфігурації потоком в'язкої слабостисненої рідини, а також внутрішніх течій в широкому діапазоні чисел Рейнольдса.

Список літератури

- [1] А. А. Яровий, *Методи та засоби організації високопродуктивних паралельно-ієрархічних обчислювальних систем із рекурсивною архітектурою*. Вінниця, Україна: ВНТУ, 2016.
- [2] Р. Д. Іскович–Лотоцький, Я. В. Іванчук, Я. П. Веселовський "Моделювання робочих процесів гідроімпульсного привода з однокаскадним клапаном пульсатором," *Вібрації в техніці та технологіях*, № 3(86), С.10–19, 2017.
- [3] Р. Д. Іскович–Лотоцький, Я. В. Іванчук, Я. П. Веселовський "Моделювання робочих процесів в піролізній установці для утилізації відходів," *Східно–європейський журнал передових технологій*. – Том 1, № 8(79), С.11–20, 2016. <https://doi.org/10.15587/1729-4061.2016.59419>.
- [4] F. H. Harlow, J. E. Welch, Numerical calculation of time-dependent viscous incompressible flow of fluid with free surface // *Phys. Fluids*, 1965. – V. 8, N. 12. – P. 2182 – 2189.
- [5] Amsden A. A., Harlow F. H. *The SMAC method*. – Los Alamos Scientific Lab., Rept. NLA-4370. Los Alamos, 1970.
- [6] C. R. Easton "Homogeneous boundary conditions for pressure in MAC method," *J.Comput. Phys*, V. 9, N. 2, P. 375-379, 1972.
- [7] Р. Д. Іскович–Лотоцький, О. В. Зелінська, Я. В. Іванчук, *Технологія моделювання оцінки параметрів формоутворення заготовок з порошкових матеріалів на вібропресовому обладнанні з гідроімпульсним приводом*. Вінниця, Україна: ВНТУ, 2018.
- [8] Р. Д. Іскович–Лотоцький, Н. Р. Веселовська, Я. В. Іванчук, Я. П. Веселовський, "Розрахунок температурних полів в робочих зонах піролізної установки," *Міжсвузівський збірник наукових праць "НАУКОВІ НОТАТКИ"*. Випуск 42, С. 113–120, 2013.
- [9] К. Флетчер, *Вычислительные методы в динамике жидкостей*: В 2-х томах: Т. 1: Пер. с англ. – М.: Мир, 1991. – 504 с.
- [10] Р. Д. Іскович–Лотоцький, Я. В. Іванчук, *Вібраційні та віброударні пристрої для розвантаження транспортних засобів*. Вінниця, Україна, 2012.
- [11] FlowVision – Made of access: World Wide Web – <https://fv-tech.com/en/>.
- [12] F. R. Menter, M. Kuntz, and R. Langtry (2003) "Ten years of Industrial Experience with the SST Turbulence Model", *Turbulence, Heat and Mass Transfer 4*, Begell House, Inc., 8 p.
- [13] Р. Д. Іскович–Лотоцький, Я. В. Іванчук, Я. П. Веселовський "Моделювання процесу спряженого теплообміну в установці для утилізації відходів" *Вісник Вінницького політехнічного інституту*, – №3(126), С. 51 – 57, 2016.

References

- [1] A. A. Yaroyvi, *Metody ta zasoby orhanizatsii vysokoproduktyvnykh paralelno-iierarhichnykh obchyslivalnykh system iz rekursyvnoiu arkhitekturoiu*. Vinnytsia, Ukraina: VNTU, 2016.
- [2] R. D. Iskovych–Lototskyi, Ya. V. Ivanchuk, Ya. P. Veselovskyi "Modeliuvannia robochykh protsesiv hidro-impulsnoho pryvoda z odnokaskadnym klapanom pulsatorom," *Vibratsii v tekhnitsi ta tekhnolohiiakh*, № 3(86), S.10–19, 2017.
- [3] R. D. Iskovych–Lototskyi, Ya. V. Ivanchuk, Ya. P. Veselovskyi "Modeliuvannia robochykh protsesiv v piroliznii ustanovtsi dlia utylizatsii vidkhodiv," *Skhidno–ievropeyskyi zhurnal peredovykh tekhnolohii*. – Tom 1, № 8(79), S.11–20, 2016. <https://doi.org/10.15587/1729-4061.2016.59419>.
- [4] F. H. Harlow, J. E. Welch, Numerical calculation of time-dependent viscous incompressible flow of fluid with free surface // *Phys. Fluids*, 1965. – V. 8, N. 12. – P. 2182 – 2189.
- [5] Amsden A. A., Harlow F. H. *The SMAC method*. – Los Alamos Scientific Lab., Rept. NLA-4370. Los Alamos, 1970.

- [6] C. R. Easton "Homogeneous boundary conditions for pressure in MAC method," J.Comput. Phys, V. 9, N. 2, P. 375-379, 1972.
- [7] R. D. Iskovych-Lototskyi, O. V. Zelinska, Ya. V. Ivanchuk, Tekhnolohiia modeliuvannia otsinky parametriv formoutvorennia zahotvok z poroshkovykh materialiv na vibropresovomu obladdanni z hidroiimpuls-nym pryvodom. Vinnytsia, Ukraina: VNTU, 2018.
- [8] R. D. Iskovych-Lototskyi, N. R. Veselovska, Ya. V. Ivanchuk, Ya. P. Veselovskyi, "Rozrakhunok temperaturnykh poliv v robochykh zonakh piroliznoi ustanovky," Mizhvuzivskyi zbirnyk naukovykh prats "NAUKOVI NOTATKY". Vypusk 42, S. 113-120, 2013.
- [9] K. Fletcher, Вычислительные методы в динамике жидкостей: V 2-х томakh: T. 1: Per. s anhl. – М.: Мир, 1991. – 504 s.
- [10] R. D. Iskovych-Lototskyi, Ya. V. Ivanchuk, Vibratsiini ta vibroudarni prystroi dlia rozvantazhennia transportnykh zasobiv. Vinnytsia, Ukraina, 2012.
- [11] FlowVision – Made of access: World Wide Web – <https://fv-tech.com/en/>.
- [12] F. R. Menter, M. Kuntz, and R. Langtry (2003) "Ten years of Industrial Experience with the SST Turbulence Model", Turbulence, Heat and Mass Transfer 4, Begell House, Inc., 8 p.
- [13] R. D. Iskovych-Lototskyi, Ya.V. Ivanchuk, Ya.P. Veselovskyi "Modeliuvannia protsesu spriazhenoho teploobminu v ustanovtsi dlia utylizatsii vidkhodiv" Visnyk Vinnytskoho politekhnichnoho instytutu, – №3(126), S. 51 – 57, 2016.

Відомості про авторів

Іванчук Ярослав Володимирович – к.т.н., доцент, доцент кафедри галузевого машинобудування Вінницького національного технічного університету, м.Вінниця, Хмельницьке шосе, 95.

Яровий Андрій Анатолійович – д.т.н., проф., завідувач кафедри компютерних наук Вінницького національного технічного університету, м.Вінниця, Хмельницьке шосе, 95.

Коваль Костянтин Олегович – к.т.н., доцент, завідувач кафедри інтеграції навчання з виробництвом Вінницького національного технічного університету, м. Вінниця, Хмельницьке шосе, 95.

Y. V. Ivanchuk, A. A. Yarovyi, K. O. Koval

NUMERICAL SIMULATION METHOD OF HYDRODYNAMIC PROCESSES

Vinnytsia National Technical University, Vinnytsia

Я. В. Иванчук, А. А. Яровой, К. О. Коваль

МЕТОД ЧИСЛЕННОГО МОДЕЛИРОВАНИЯ ГИДРОДИНАМИЧЕСКИХ ПРОЦЕССОВ

Винницкий национальный технический университет, г. Винница

УДК 519.688: 004.75:004.421

І. О. Процько¹, О. В. Грищук²

РОЗПАРАЛЕЛЕННЯ ОБЧИСЛЕННЯ КАНОНІЧНОГО РОЗКЛАДУ ЧИСЛА НА МНОЖНИКИ

¹Національний університет "Львівська політехніка", ²ТзОВ "Логіка"

Анотація. В статті розглянуто обчислення канонічного розкладу числа на множники з використанням модифікованого методу пробних ділень. Виконання операцій ділення числа розкладу на прості числа для перевірки на кратність вимагає відповідних часових затрат в сучасних комп'ютерних системах. Для їх зменшення використовується бінарне подання числа розкладу в процесі його аналізу на кратність. Для кожного розряду бінарного числа розкладу, що дорівнює одиниці, визначаються залишки його вагового коефіцієнта за модулем відповідного простого числа. Отримані значення залишків акумулюються і потім виконується перевірка накопленого значення на рівність з відповідним значенням з множини простих чисел. У випадку рівності отримуємо елемент канонічного розкладу і знову перевіряємо степені цього елемента розкладу на кратність. В протилежному випадку переходимо на наступне більше просте число для подальшої перевірки на кратність, обмежуючись значенням кореня квадратного числа розкладу. Незалежність підзавдань виконання перевірки бінарного подання числа на подільність простими числами дає можливість розпаралелювати виконання розкладу числа в багатоядерних мікропроцесорах комп'ютерних систем. Серед рівнів паралельності можна послідовно виділити: визначення залишків вагових коефіцієнтів, акумулювання залишків для одиничних розрядів бінарного подання числа розкладу, перевірки на кратність сукупністю простих чисел. Паралельне обчислення розкладу числа досягається виконання алгоритму в багатьох потоках. Програмна реалізація на мові C++, відповідно алгоритму, розподіляє обчислення між потоками, використовуючи пул потоків. В алгоритмі розпаралелення обчислень канонічного розкладу, в залежності від введеного значення числа розкладу, визначається відповідне значення кількості простих чисел та їхніх степенів і рівномірно розподіляється між потоками для виконання аналізу на подільність. В результаті визначено залежність часу обчислення канонічного розкладу числа від кількості потоків в багатоядерних мікропроцесорах лінійки Intel Core i3/i5/i7. Для кожної комп'ютерної системи, що має певну кількість обчислювальних ядер в мікропроцесорах, існує оптимальна кількість потоків, яка забезпечує мінімальний час канонічного розкладу числа на множники.

Ключові слова: канонічний розклад, прості множники, залишки, вагові коефіцієнти, потоки, паралельне обчислення.

Аннотация. В статье рассмотрено вычисление канонического разложения числа на множители с использованием модифицированного метода пробных делений. Выполнение операций деления числа разложения на простые числа для проверки на кратность требует соответствующих временных потерь в современных компьютерных системах. Для их уменьшения используется бинарное представление числа разложения в процессе его анализа на кратность. Для каждого разряда бинарного числа разложения, что равняется единице, определяются остатки его весового коэффициента по модулю соответствующего простого числа. Полученные значения остатков аккумулируются и потом выполняется проверка накопленного значения на равенство с соответствующим значением из множества простых чисел. В случае равенства получаем элемент канонического разложения и снова проверяем степени этого элемента разложения на кратность. В противном случае переходим на следующее большее простое число для дальнейшей проверки на кратность, ограничиваясь значением квадратного корня числа разложения. Независимость подзадач выполнения проверки бинарного представления числа на делимость простыми числами дает возможность распараллеливать выполнение разложения числа в многоядерных микропроцессорах компьютерных систем. Среди уровней параллельности можно последовательно выделить: определение остатков весовых коэффициентов, аккумулирование остатков для единичных разрядов бинарного представления числа разложения, проверки на кратность наборам из простых чисел. Программная реализация на C++, соответственно алгоритму, распределяет вычисления во многих потоках, используя пул потоков. В алгоритме распараллеливания вычислений канонического разложения, в зависимости от введеного значения числа разложения, определяется соответствующее значение количества простых чисел с их степенями и равномерно распределяется между потоками для выполнения анализа на делимость. В результате определена зависимость времени вычисления канонического разложения числа от количества потоков в многоядерных микропроцессорах линейки Intel Core i3/i5/i7. Для каждой компьютерной системы, которая имеет определенное количество вычислительных ядер в микропроцессорах, существует оптимальное количество потоков, которое обеспечивает минимальное время канонического разложения числа на множители.

Ключевые слова: каноническое разложение, простые множители, остатки, весовой коэффициент, потоки, параллельное вычисление.

Abstract. The computation of the canonical factorization of a number using the modified trial divisions method has been considered. The performing operations of the division a number of factorization into prime numbers for the testing on a repetition factor demands a respective loss of the execute time in modern computer systems. To reduce them, the presentation of the number of factorization in the binary form is used for the process of analysis on repetition factors. The residuals of weighting coefficient are defined for each digit of the binary representation the number of factorization, which is equal to one. The obtained values of the residuals are accumulated and then the accumulated value is checked for the equality with the corresponding value from the set of prime numbers. In case of equality, we obtain an element of canonical factorization and again check the degrees of this element for a repetition factor. Otherwise, we proceed to the next larger prime number for further checking for a repetition factor. The independence of the subtasks to perform the check of the binary representation of a number on divisibility by prime numbers makes it possible to parallelize the execution of the factorization of a number in multi-core microprocessors of computer systems. Among the levels of the parallelism can be consistently identified: the definition of residual weighting coefficients, the accumulation of residuals for bits equal to one of the binary representation of the number of factorization, the checking for a repetition factor from the sets of primes. Software implementation in C++, according to the algorithm, schedules the computations in multi-threads, using a pool of threads. In the algorithm for parallelizing the computations of the canonical factorization, depending on the entered value of the expansion number, the corresponding value of the number of primes with their powers is determined and is evenly distributed between the streams to perform an analysis of divisibility. As a result, the dependence of the run time the computation of the factorization of a number from the number of threads is defined in multi-core processors of Intel Core i3/i5/i7. For the each computer system exist the optimal number of the threads, which supports the minimal time of the canonical factorization of a number on the prime numbers.

Key words: canonical factorization, prime factors, residual, weighting factor, threads, parallel computation.

DOI: <https://doi.org/10.31649/1999-9941-2019-44-1-46-51>.

І. О. Процько, О. В. Грищук, 2019

Вступ

Сучасні багатоядерні системи обчислювальної техніки нарощують свою продуктивність завдяки виконанню паралельних обчислень. Особливо, якщо така можливість закладена в алгоритмі та реалізована новітніми технологіями паралельного програмування.

Канонічний розклад числа, як фундаментальна теорема арифметики про однозначне представлення цілого числа [1], турбував вчених ще до нашої ери і пов'язаний з іменами Евкліда, Ератосфена Киренського. Канонічний розклад числа N на прості множники подано у вигляді

$$N = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}, \quad (1)$$

де $p_1^{s_1}, p_2^{s_2}, \dots, p_k^{s_k}$ прості множники ($p_1^{s_1} < p_2^{s_2} < \dots < p_k^{s_k}$) та s_1, s_2, \dots, s_k степінь їх повторюваності. В наш час задача підвищення методів та алгоритмів пошуку розкладу числа на прості множники або перевірки простоти цілих чисел вийшла на кардинально новий рівень. Це зумовлено потребою побудови високостійких криптосистем, в яких використовуються "випадкові" прості числа з великого числа цифр [2].

Починаючи з 1977 року, коли було опубліковано в журналі «Scientific American» новий алгоритм шифрування [3] і було дано список з 42 тестових чисел різної розрядності й за розклад кожного з цих чисел була призначена премія, розроблено класичні алгоритми канонічного розкладу. До яких відносять p – метод, $(p-1)$ – метод Полларда, метод еліптичних кривих, метод квадратичного решета, метод решета числового поля й інші [4]. На основі цих методів розробляються програмні модулі та модифікації класичних алгоритмів для рішення різноманітних прикладних завдань. Дослідження методів канонічного розкладу в напрямку розпаралелювання виконання обчислень показує, що основна ідея полягає у виборі випадкового значення для кожного окремого паралельного процесу, кождний з яких буде виконувати алгоритм відповідно методу. Однак одночасне виконання алгоритму декількома значними за складністю потоками для знаходження множників числа розкладу на завжди дає очікуваний результат [5].

Найпростішим рішенням канонічного розкладу є метод пробних ділень. Для розкладу числа на множники метод використовує елементарної перевірки на ділення без залишку даного обсягу N на послідовний вибір дільників з множини простих чисел 2,3,5,7,9,11,13,17,... Однак послідовне виконання операцій ділення для перевірки на кратність в сучасних комп'ютерних моделях виконується за допомогою мікропрограми або спеціалізованих арифметичних вузлів, що збільшує тривалість обчислення канонічного розкладу. Адже операція ділення реалізується з послідовного набору арифметичних операцій додавання/віднімання, незалежно від того, який з алгоритмів використовується. Для перевірки простоти числа з великою кількістю цифр метод пробних ділень з обчислювальної точки зору є достатньо емкий.

Актуальність

Забезпечення високої швидкодії обчислення комп'ютерними системами класичної задачі факторизації цілочисельного значення на прості множники вимагає розробки ефективних алгоритмічних методів з використанням новітніх інформаційних технологій. Швидке обчислення факторизації чисел для забезпечення високої криптостійкості інформаційних даних, для переходу до багатовимірних подання одновимірних послідовностей інформаційних даних та інших застосувань є достатньо затребуваним в багатьох практичних завданнях.

Мета

Метою роботи є підвищення швидкодії обчислення канонічного розкладу числа на множники на основі вдосконаленого методу пробних ділень та розпаралелення виконання розкладу багатоядерними процесорами сучасних комп'ютерних систем. Виконання канонічного розкладу в обчислювальному середовищі на програмному або апаратному рівнях елементарної операції накопичення значень залишків значно ефективніше з точки зору їхніх величин і в порівнянні з виконанням операції ділення. Можливість подальшого підвищення швидкодії обчислення розкладу числа полягає в паралельному апаратному виконанні методу пробних ділень в аспекті перевірки накоплених значень залишків на рівність простим числам та їхнім степеням.

Задачі

1. Формулювання аналітичної моделі канонічного розкладу на основі вагових залишків бінарного числа.
2. Аналіз обчислювальної складності $O(f(n))$ визначення канонічного розкладу числа на основі вагових залишків.
3. Розробка програмної реалізації шляхом розподілення обчислення канонічного розкладу числа в багатьох потоках.
4. Тестування залежності часу виконання обчислення канонічного розкладу числа на множники від кількості потоків.

Підхід канонічного розкладу на основі вагових залишків бінарного числа

Розглянемо підхід пробних ділень з використанням залишків для кожного вагового коефіцієнта бінарного представлення числа, що визначаються операцією за модулем від простих чисел p_i та їх можливих повторень s_i [6]. Визначення подільності десяткового числа N , коли залишок дорівнює нулю, у випадку представлення в двійковій системі числення матиме вигляд:

$$N \bmod i = (a_n 2^n + a_{n-1} 2^{n-1} + a_{n-2} 2^{n-2} + \dots + a_1 2 + a_0) \bmod i = (a_n (2^n \bmod i) + a_{n-1} (2^{n-1} \bmod i) + a_{n-2} (2^{n-2} \bmod i) + \dots + a_1 (2 \bmod i) + a_0 \bmod i), \quad (2)$$

де a_i – двійкові розряди числа, i – просте число.

Розклад числа N за формулою (2) базується на використанні залишків кожного вагового коефіцієнта ($2^k \bmod i$), де $k=0,1,\dots,n$ кількість двійкових розрядів числа. Ці залишки, що відображені в таблиці 1, значно ефективніше в порівнянні з арифметичною операцією ділення, запам'ятовується або визначаються [6] в обчислювальному середовищі. Пробна перевірка подільності числа виконується для послідовності простих чисел та їх степенів $P = \{2,3,5,7,9,11,13,17,\dots,i\}$ загальною кількістю m .

Виконавши накопичення значень залишків за вибраними вагами, порівнюємо накопичену суму з простим числом i або його степенем i^s . У випадку порівняння, коли накопичене значення залишків більше – знову проводиться за формулою (2) накопичення залишків від попереднього одержаного накопиченого числа, а у випадку рівності – виводиться елемент канонічного розкладу i та виконується перехід до наступного значення з послідовності простих чисел $P\{i\}$. Отже, в результаті отримуємо набір простих множників канонічного розкладу (1) числа N .

Обчислювальна складність $O(f(n))$ визначення канонічного розкладу на основі вагових залишків бінарного числа в загальному випадку визначається кількістю операцій, які необхідно виконати. Наближену оцінку обчислювальної складності (3) для найскладнішого випадку N можна визначити, взявши на основі таблиці значень залишки для всіх n вагових коефіцієнтів з послідовності $m = N/2$ простих чисел та їх степенів.

Таблиця 1 – Значення залишків двійкового розряду числа за модулями простих чисел та їх степенів

m/n	n	...	7	6	5	4	3	2	1	0	$P\{i\}$
1	$2^n \bmod 3$...	2	1	2	1	2	1	2	1	$\bmod 3$
2	$2^n \bmod 5$...	3	4	2	1	3	4	2	1	$\bmod 5$
3	$2^n \bmod 7$...	2	1	4	2	1	4	2	1	$\bmod 7$
4	$2^n \bmod 9$...	2	1	5	7	8	4	2	1	$\bmod 9$
5	$2^n \bmod 11$...	7	9	10	5	8	4	2	1	$\bmod 11$
6	$2^n \bmod 13$...	11	12	6	3	8	4	2	1	$\bmod 13$
...
m	$2^n \bmod i$...	$2^7 \bmod i$	$2^1 \bmod i$	$2^0 \bmod i$	$\bmod i$

У цьому випадку будемо мати $(n \cdot N/2)$ – максимальну кількість додавань та $(N/2)$ – мінімальну кількість порівнянь одержаної суми накопичення з простим числом i або його степенем i^s . Для накопичення залишків з мінімальною кількістю порівнянь врахуємо множник їх можливого повторення в межах $k = (1,5 \div 3)$.

$$O(k(n \cdot N/2 * N/2)) = O(N^2 * n * k) = O((p_1^{s_1} p_2^{s_2} \dots p_k^{s_k})^2 n k). \quad (3)$$

Отже, обчислювальна складність канонічного розкладу на основі вагових залишків бінарного числа має квадратичну залежність від значення числа розкладу $N = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ та лінійну від кількості його двійкових розрядів n . Тому розклад великих чисел на основі даного підходу ефективно може бути реалізований з використанням паралельного аналізу на подільність в багатоядерних комп'ютерних системах.

Виконання паралельного алгоритму канонічного розкладу

На сьогодні розпаралелення обчислювальних процесів вийшло на кардинально новий рівень з точки зору підвищення продуктивності. Ефективність розробки паралельних програм багато в чому залежить не тільки від паралельності алгоритму, але від наявності відповідного програмного та апаратного інструментарію.

Практично всі сучасні ОС підтримують керування потоками. Прикладна програма реалізує керування потоками за допомогою спеціальних бібліотек, що дозволяють досягнути апаратного прискорення канонічного розкладу числа. Обчислення канонічного розкладу числа на множники з використанням залишків для кожного вагового коефіцієнта в бінарному представленні числа розроблена в IDE Visual C++ 2017, але може бути скомпільована для іншого середовища.

Програма виконує наступні дії:

1. Введення числа для розкладу на множники та введення кількості потоків для паралельного обчислення.
2. Побудова таблиці залишків від ділення на прості числа.
3. Вивід на екран канонічних множників розкладу для введеного числа.
4. Тестування швидкодії виконання розкладу чисел на прості множники з виводом часу обчислення.

Паралельне обчислення розкладу числа досягається шляхом розподілення алгоритму роботи в багатьох потоках (threads). В залежності від кількості потоків визначається час виконання канонічного розкладу числа. Блок-схема (рис.1) алгоритму розподілення обчислень канонічного розкладу на множники в залежності від введеного числа розкладу N визначає відповідну кількість простих чисел та їх степенів (табл. 1) і розподіляє на потоки для аналізу на подільність. Завдяки високій степені розпаралелення задачі розкладу числа на множники з використанням залишків для кожного вагового коефіцієнта в бінарному представленні числа в плані функціональної декомпозиції і відповідної незалежності даних розподілення обчислень підзадач між потоками здійснюється пропорційно. Наприклад, розглянемо як будуть обчислюватись множники числа 262143 при використанні двох потоків. Для даного числа Таблиця 1 значення залишків двійкового розряду числа за модулями простих чисел та їх степенів буде складатись з 23000 рядків. Потоки поділять для опрацювання таблиці порівну, отже кожен потік опрацює по 11500 рядків таблиці. Після завершення обчислень, результат роботи для першого потоку буде: 3 3 3 7 19 73. В другому потоці не буде знайдено жодного простого множника.



Рисунок 1 – Блок-схема алгоритму розподілення обчислень канонічного розкладу числа

В програмі написаній на мові C++ використовуються функції:

find_prime_factors() розподіляє роботу між заданою кількістю потоків;

create_mod_prime_table() створює таблицю простих чисел і залишків від ділення на кожне просте число;

is_next_prime() визначає чи є число наступним простим числом, використовуючи відомі попередні прості числа;

is_divider() виконує за формулою (2) операції накопичення значень залишків та їх перевірку на рівність зі значенням з множини простих чисел та їх степенів. Накопичення значень залишків проводиться, коли двійкові розряди числа $a_i = 1$;

pool() для організації використання пулу потоків і взаємодії між ними використовується функція бібліотеки STPL [7], що є надбудовою над стандартою бібліотекою STL, яка має можливість працювати з системними потоками.

Реалізація розробленої паралельної програми здійснюється комп'ютерними системами з багатоядерними процесорами лінійки Intel Core i3/i5/i7, що можуть використовувати підтримку технологій (Intel Turbo Boost Technology 2.0, Intel Hyper-Threading Technology, Intel Smart Cache, Intel HD Graphics 3000). Створені паралельні потоки з можливістю застосування гіперпотокості (HT) та без реалізуються повноцінними обчислювальними ядрами, що однаково суттєво впливають на продуктивність виконання.

Результати обчислення отримані в 32-бітному режимі на багатоядерних процесорах з тактовою частотою 3.7ГГц:

- Intel Core i3-6100, який має два фізичних ядра і кожне фізичне ядро складається з двох віртуальних (HT);
- Intel Core i5-9600, який має шість фізичних ядер і не

підтримує технології HT;

– Intel Core i7-2600 який має *чотири* фізичних ядра і кожне фізичне ядро складається з двох віртуальних (HT).

Наступна таблиця 2 показує залежність часу (мілісекунди) витраченого комп'ютерними системами з багатоядерними процесорами на обчислення канонічного розкладу числа на множники від введеного значення кількості потоків.

Таким чином, швидше виконується розроблена паралельна програма обчислення канонічного розкладу числа на множники на процесорах з найбільшою кількістю ядер. Подвоєння продуктивності в процесорі Intel Core i7-2600 з підтримкою гіперпотоковості (HT) у кількості 8 потоків не показало меншого часу в порівнянні з процесором Intel Core i5-9600, який має шість фізичних ядер і не підтримує технології HT. Для процесора Intel Core i3-6100 найкраща швидкодія досягається при використанні 4 потоків, при цьому найбільший приріст спостерігається при задіянні 2-х фізичних ядер процесора.

Таблиця 2 – Залежності часу обчислення канонічного розкладу числа на множники від кількості потоків

К-ть потоків	1	2	3	4	5	6	7	8	9	10	11	12
i3-6100 (HT)	3468	2817	2146	2041	2064	2099	2087	2211				
i5-9600	2355	1738	1307	1112	943	826	773	721	701	1076	2244	2564
i7-2600 (HT)	2630	2076	1522	1323	1216	1150	1069	1012	970	937	944	903

Висновки

1. Вдосконалено метод пробних ділень канонічного розкладу числа на множники з використанням залишків для кожного вагового коефіцієнта у бінарному представленні числа. При цьому виконання канонічного розкладу в обчислювальному середовищі на апаратному або програмному рівнях елементарної операції накопичення значень залишків значно ефективніше з точки зору їхніх менших величин і в порівнянні з виконанням операції ділення.

2. Програмне рішення канонічного розкладу числа на множники реалізовано в IDE Visual C++ 2017, яке може бути й скопійованим для іншого середовища. Завдяки високій степені розпаралелення задачі розкладу числа на множники з використанням залишків для кожного вагового коефіцієнта в бінарному представленні числа в плані функціональної декомпозиції і відповідної незалежності даних програмне рішення виконує розподілення обчислень підзадач між паралельними потоками пропорційно.

3. Виконання програмного коду канонічного розкладу числа комп'ютерними системами з багатоядерними процесорами лінійки Intel Core i3/i5/i7 показало залежність часу обчислення від кількості сформованих потоків, що відповідно пов'язані з кількістю фізичних та віртуальних (Hyper Threading) ядер процесора.

4. Подальші дослідження пов'язані з розширенням розрядної сітки, більш ніж 32-бітний режим, для бінарного представлення числа розкладу та використання продуктивнішого апаратного інструментарію.

Список літератури

- [1] И. М. Виноградов, *Основы теории чисел*, М.: Наука, 1981.
- [2] В. А. Орлов, Н. В. Медведев, Н. А. Шимко, А. Б. Домрачева, *Теория чисел в криптографии* : учеб. Пособие, М.: Изд-во МГТУ им. Н. Э. Баумана, 2011.
- [3] The Alternative History of Public-Key Cryptography [Електронний ресурс] – Режим доступу: <http://cryptome.org/ukpk-alt.htm>
- [4] Ш. Т. Ишмухаметов, *Методы факторизации натуральных чисел*: учебное пособие. – Казань: Казан. ун. 2011.
- [5] Параллельная реализация и сравнительный анализ алгоритмов факторизации с распределенной памятью / Макаренко А.В. Пыхтеев А.В. Ефимов С.С. [Електронний ресурс] – Режим доступу: <http://cyberleninka.ru/article/n/parallelnaya-realizatsiya-i-sravnitelnyu-analiz-algoritmov-faktorizatsii-v-sistemah-s-raspredelyonnoy-pamyatyu>
- [6] Патент 116912 Україна, G06F7/04(2006.01), G06F17/10(2006.01). Пристрій канонічного розкладу числа на множники / І.О. Процько, В.М. Теслюк; Опубл. 25.05.2018, Бюл. №10.
- [7] Бібліотека CTPL [Електронний ресурс] – Режим доступу: <https://github.com/vit-vit/CTPL>.

References

- [1] Y. M. Vynohradov, *Osnovy teoryy chysel, yzd. 9-e, pererab.* – М.: Nauka, 1981. – 167 s.

- [2] V. A. Orlov, N. V. Medvedev, N. A. Shymko, A. B. Domracheva, Teoriya chysel v kryptohrafiy : ucheb. posobyе. – M. : Yzd-vo MHTU ym. N. Eh. Baumana, 2011. – 223 s.
- [3] The Alternative History of Public-Key Cryptography [Elektronnyi resurs] – Rezhym dostupu: <http://cryptome.org/ukpk-alt.htm>
- [4] Sh. T. Yshmukhametov, Metody faktoryzatsyy naturalnykh chysel: uchebnoe posobyе. – Kazan: Ka-zan. un. 2011. – 190 s.
- [5] Parallelnaia realizatsiya y sravnitelnyi analiz alhorytmov faktoryzatsyy s raspredelennoi pamiatu / Makarenko A.V. Pykhteev A.V. Efymov S.S. [Elektronnyi resurs] – Rezhym dostupu: <http://cyberleninka.ru/article/n/parallelnaya-realizatsiya-i-sravnitelnyy-analiz-algoritmov-faktorizatsii-v-sistemah-s-raspredelyonnoy-pamyatyu>
- [6] Patent 116912 Ukraina, G06F7/04(2006.01), G06F17/10(2006.01). Prystrii kanonichnogo rozkladu chysla na mnozhnyky / I.O. Protsko, V.M. Tesliuk; Opubl. 25.05.2018, Biul. №10.
- [7] Biblioteka CTPL [Elektronnyi resurs] – Rezhym dostupu: <https://github.com/vit-vit/CTPL>.

Відомості про авторів

Процько Ігор Омелянович, к.т.н., доцент, НУ "Львівська політехніка", кафедра автоматизованих систем управління, м. Львів, Україна.

Грищук Олександр Васильович, розробник, ТзОВ "Логіка", м. Львів, Україна.

I.O. Prots'ko¹, O.V.Gryschuk²

**PARALLIZATION OF THE COMPUTATION
OF CANONICAL SPLIT A NUMBER ON THE FACTORS**

1 – Lviv National Polytechnic University , 2 – LtdC "Lohika", Lviv

И. Е. Процько¹, А. В. Грищук²

**РОСПАРАЛЛЕЛИВАНИЕ ВЫЧИСЛЕНИЯ
КАНОНИЧЕСКОГО РАЗЛОЖЕНИЯ ЧИСЛА НА
МНОЖИТЕЛИ**

1 – Национальный университет "Львівська політехніка", 2 – ТзОВ "Логіка", Львов

ДО ВІДОМА АВТОРІВ

Найновіші правила оформлення і подання статей знаходяться на сайті журналу
<http://itce.vntu.edu.ua/>