ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.4 + 004.9

Р. Н. Квєтний, Н. Ф. Кузьміна

РОЗПОДІЛЕНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ ГРУПОВИХ РІШЕНЬ

Вінницький національний технічний університет, Вінниця

Анотація. Процес прийняття рішень є невід'ємною частиною сучасного суспільства. Дослідження показують що за останні десятиріччя використання груп в організаціях різко зросла і кожна організація функціонує на основі рішень прийнятих групами осіб всередині організації. Майже кожен аспект суспільного, політичного, законодавчого та економічного життя функціонує за рахунок прийняття рішень групами осіб. Теорія систем розглядає прийняття групових рішень як взаємозалежні сили здатні бути проаналізованими з точки зору інших сил. Поведінка індивідів у групах зумовлена багатьма причинами а системний методі підкреслює множинні причинно-наслідкові зв'язки та складний взаємозв'язок сил. Ефективне прийняття рішень розглядається як природний наслідок здатності осіб що приймають рішення аналізувати та розуміти процес прийняття групових рішень, але ніхто не може набути такої здатності без активної участі у процесі прийняття групових рішень.

Групове рішення, у загальному випадку являється вибором членів групи з числа доступних їм альтернатив. Дуже рідко група осіб приймає рішення ізольовано від решти групи. На сьогоднішній день не існує простих засобів та систем, що забезпечать прийняття найкращих рішень, що породжує необхідність досліджень у даній галузі.

Системи підтримки прийняття групових рішень – це інтерактивні комп'ютеризовані системи, які допомагають групі користувачів, що приймають рішення, використовувати дані та моделі для ідентифікації та розв'язання задач.

У даній статті як підхід до реалізації розподіленої системи підтримки прийняття групових рішень та розв'язання конфліктних ситуацій, що породжуються у процесі прийняття рішень пропонується використання аналітичного апарату Баєсових мереж. Для цього було розроблено інформаційну технологію розподіленої системи підтримки прийняття групових рішень, запропоновано інформаційну модель та динамічні структури даних та розроблено програмну реалізацію розподіленої системи підтримки прийняття групових рішень. Експериментальні дослідження розробленої системи показали, що за рахунок використання Баєсових мереж можна уникнути конфліктних ситуацій обумовлених використанням принципу більшості та його різноманітних модифікацій.

Ключові слова: Розподілена система, підтримка групових рішень, Баєсова мережа.

Аннотация. Процесс принятия решений является неотъемлемой частью современного общества. Исследования показывают, что за последние десятилетия использование групп в организациях резко возросло и каждая организация функционируют на основе решений, принятых группами лиц внутри организации. Почти каждый аспект общественной, политической, законодательной и экономической жизни функционирует за счет принятия решений группами лиц. Теория систем рассматривает принятие групповых решений как взаимосвязанные силы, которые могут быть проанализированы с точки зрения других сил. Поведение индивидов в группах обусловлено многими причинами, а системный метод подчеркивает причинно-следственные связи и сложную взаимосвязь сил. Эффективное принятие решений рассматривается как естественное следствие способности лиц принимающих решения анализировать и понимать процесс принятия групповых решений, но никто не может приобрести эту способность без активного участия в процессе принятия групповых решений.

Групповое решение, в общем случае является выбором членов группы из числа доступных им альтернатив. Очень редко группа индивидов принимает решение изолировано от остальной группы. На сегодняшний день не существует простых средств и систем обеспечивающих принятие лучших решений, что порождает необходимость исследований в данной области.

Системы поддержки принятия групповых решений – это интерактивные компьютеризированные системы, которые помогают группе пользователей, принимающих решения, использовать данные и модели для идентификации и решения задач.

В данной статье как подход к реализации распределенной системы принятия групповых решений и разрешения конфликтных ситуаций, порождаемых в процессе принятия решений, предлагается использование аналитического аппарата Байесовских сетей. Для этого разработана информационная технология распределенной системы поддержки принятия групповых решений, предложена информационная модель и динамические структуры данных и разработана программная реализация распределенной системы поддержки принятия групповых решений.

Экспериментальные исследования разработанной системы показали, что за счет использования Байесовских сетей можно избежать конфликтные ситуации, обусловленные использованием принципа большинства и его различных модификаций.

Ключевые слова. Распределенная система, поддержка групповых решений, Байесовская сеть.

Abstract. The decision-making process is an integral part of modern society. Research shows that over the last decades, the use of groups within organizations has increased dramatically, and each organization operates based on decisions made by groups of individuals within the organization. Almost every aspect of social, political, legislative and economic life functions through the decision making of groups of individuals. Systems theory views group decision making as interdependent forces capable of being analyzed from the perspective of other forces. The behavior of individuals in groups is due to many reasons, and the systematic method emphasizes multiple cause and effect relationships and the complex interplay of forces. Effective decision-making is seen as a natural consequence of the ability of decision-makers to analyze and understand the group decision-making process, but no one can acquire this ability without actively participating in the group decision-making process.

A group decision, in general, is the choice of group members from among the alternatives available to them. Very rarely does a group of individuals make decision in isolation from the rest of the group.

There are currently no simple tools and systems available to make the best decisions, which raises the need for research in this field.

Group decision support systems are interactive computerized systems that help a group of decision-makers use data and models to identify and solve tasks.

In this article, the use of Bayesian network analytics is proposed as an approach to implement a distributed group decision support system and resolving conflict situations in the decision-making process. For this purpose, the information technology of the distributed group decision support system was developed, the information model and dynamic data structures were proposed, and the software implementation of the group decision support system was developed.

Experimental studies of the developed system have shown that by using Bayesian networks one can avoid conflict situations caused by the use of majority principle and its various modifications.
Key words: Distributed system, group decision support, Bayesian network.
DOI: https://doi.org/10.31649/1999-9941-2020-47-1-4-13.

Вступ

Широке використання наукових методів прийняття групових рішень та їх реалізація за допомогою комп'ютерних засобів, обумовлені тим, що процес прийняття рішень групою користувачів потребує збереження та обробки великої кількості інформації. Дана особливість породжує пошук та дослідження різноманітних засобів та методів, що дозволять підвищити ефективність таких систем. Особливого поширення в останні роки набуло використання методу Баєса, що дає можливість отримання реалістичної моделі дійсності та орієнтації в найбільш ймовірному напрямку розвитку подій досліджуваної системи [1].

Актуальність

До цього часу найбільш поширеними та відомими методами підтримки прийняття групових рішень є методи визначення кінцевого рішення за допомогою принципу більшості та їх різноманітні модифікації. Основним недоліком принципу більшості є виникнення великої кількості конфліктних ситуацій та неврахування переваг осіб, що не ввійшли у більшість [2, 3]. У даній статті пропонується новий підхід для зменшення конфліктних ситуацій, врахування переваг кожної особи, що бере участь у процесі прийняття групових рішень та паралельного процесу навчання та оцінювання дій, що особливо важливо під час використання даної системи у навчальному процесі. Для зменшення конфліктних ситуацій пропонується використання аналітичного апарату Баєсових мереж, а саме ймовірнісних висновків, шляхом обчислення апостеріорного розподілення альтернатив вибору рішення через альтернативи-свідоцтва. Дана властивість дозволяє отримати нове знання про стан підмножини альтернатив спостерігаючи за іншими альтернативами, що в свою чергу є однією з основних причин широкого використання Баєсових мереж у системах підтримки прийняття рішень. Складність реалізації Баєсових мереж для великих систем вирішується за рахунок використання наближених методів обчислення [4].

Мета

Метою статті є підвищення ефективності систем підтримки прийняття групових рішень шляхом зменшення кількості конфліктних ситуацій за допомогою використання Баєсових мереж.

Задачі

1. Формалізувати параметри розподіленої системи підтримки прийняття групових рішень та сформувати інформаційну модель такої системи.
2. Розробити алгоритмічні та аналітичні засоби розподіленої системи підтримки прийняття групових рішень.
3. Розробити програмну реалізацію системи підтримки прийняття групових рішень.

Розв'язання задач

Застосування систем підтримки прийняття групових рішень дозволяє сформувати множину альтернатив для прийняття рішень та прогнозувати розвиток подій, що в свою чергу дозволяє зменшити негативні наслідки від прийнятих рішень і таким чином підвищити ефективність процесу прийняття рішень [5]. Враховуючи проведений аналіз [6, 7] у системі, що розглядається, основна увага буде приділятися методам прийняття рішень за принципом більшості та за допомогою використання Баєсової мережі. Метою використання принципу більшості у системах підтримки прийняття групових рішень є спостереження за поведінкою групи для досягнення спільної мети, а також перевірка знань користувачів. Метою використання Баєсових мереж у системах підтримки прийняття групових рішень є зменшення або уникнення конфліктних ситуацій, можливість враховувати рішення кожної особи із групи та здійснення навчання. Розподілені системи підтримки прийняття групових рішень забезпечують процес спільного прийняття рішень особами, що територіально розподілені та надають їм можливість взаємодіяти між собою у реальному часі [7]. Процес підтримки прийняття групових рішень містить велику кількість елементів, які необхідно врахувати при розробці комп'ютерних систем, особливо якщо ці системи дозволяють з'єднувати користувачів, що територіально розподілені.

Інформаційна модель розподіленої системи підтримки прийняття групових рішень

Розглянемо розроблену інформаційну модель розподіленої системи підтримки прийняття групових рішень M_S та її основні параметри [8]: $M_S = \{A_0, C, Z, U, V, A, L, T_G, M, D_G, H, \Psi\}$, де

A_0 – мета роботи розподіленої системи підтримки прийняття групових рішень для прийняття оптимального рішення у конкретний момент часу;

$C = \{c_1, c_2, \dots, c_n\}, n = \overline{1, N_C}$ – комп'ютери користувачів;

$Z = \{z_1, z_2, \dots, z_n\}, n = \overline{1, N_Z}$ – кількість активних з'єднань;

$U = \{u_1, u_2, \dots, u_n\}, n = \overline{1, N_u}$– користувачі;

$V = \{v_1, v_2\}$ – методи групового вибору користувачів, де

v_1 – принцип більшості,

v_2 – Баєсова мережа;

$A = \{a_1, a_2, \dots, a_n\}, n = \overline{1, N_a}$ – доступні альтернативи;

$L = \{l_1, l_2, \dots, l_n\}, n = \overline{1, N_l}$ – причинно-наслідкові зв'язки між альтернативами;

$T_G = \sum_{i=1}^{M} \sum_{j=1}^{N_u} t_{uij} + \sum_{k=1}^{M} t_{sk} + \sum_{k=1}^{M} t_{dk}$ – загальний час роботи системи у процесі прийняття комплексного рішення, де

$T_u = \{t_{1u}, t_{1u}, \dots, t_{nu}\}, n = \overline{1, N_{tu}}$ – час прийняття рішень користувачами;

$T_S = \{t_{1s}, t_{2s}, \dots, t_{ns}\}, n = \overline{1, M_{ts}}$ – час прийняття рішень системою;

$T_d = \{t_{1d}, t_{2d}, \dots, t_{nd}\}, n = \overline{1, N_d}$ – час затримки відповіді системи на дії користувача;

M– кількість ітерацій прийняття рішень для прийняття кінцевого комплексного рішення;

$D_G = \{d_1, d_2, \dots, d_n\}, n = \overline{1, N_d}$– комплексне рішення користувачів.

$H: U \times A \times L \to D$ – відношення множини альтернатив до множини зв'язків.

Оператор оцінки показника ефективності Ψ співвідносить множину комплексного рішення користувачів до множини значень коефіцієнта відповідності обраних альтернатив прийнятому рішенню системи [8].

$$\Psi = \left\{ \begin{array}{c} \sigma = \sqrt{\frac{1}{N_u} \sum_{i=1}^{N_u} \left(k_i - \bar{k}\right)^2} \to max, \\ \hline T_G = \sum_{i=1}^{M} \sum_{j=1}^{N_u} t_{uij} + \sum_{k=1}^{M} t_{sk} + \sum_{k=1}^{M} t_{dk} \to min \end{array} \right\}$$

де σ– коефіцієнт відповідності обраних альтернатив, що розраховується за допомогою проміжних коефіцієнтів k_i:

$k_i = \frac{N_V}{N_A}, n = \overline{0,1}$, де

N_V– кількість прийнятих рішень, які відповідають найбільш ймовірним альтернативам;

N_A– загальна кількість альтернатив.

Коефіцієнт $\bar{k}$ є середнім арифметичним значень проміжних коефіцієнтів k_i: $\bar{k} = \frac{1}{N_u} \sum_{i=1}^{N_u} k_i$.

Розробка алгоритмічних та аналітичних засобів розподіленої системи підтримки прийняття групових рішень

Баєсова мережа забезпечує природній візуальний спосіб представлення ймовірнісних незалежностей та складається з двох компонентів: направленого ациклічного графу та ймовірнісного опису, який визначає розподіл ймовірностей кожної вершини та підпорядковується умові Маркова [3, 6, 9-11]. Умова Маркова базується на тому, що залежно від батьків, будь-яка вершина є ймовірнісно-незалежною від усіх інших вершин, окрім її нащадків [9, 12]. Для оновлення ймовірностей у Баєсових мережах використовується алгоритм зв'язного дерева. Даний алгоритм працює зі зв'язним деревом, що являє собою дерево із групою вершин. Групи вершин зберігають таблицю з конфігураціями їх вершин, а алгоритм зв'язного дерева полягає у проведенні серії операцій над цими таблицями [10]. Алгоритм зв'язного дерева використовується для створення систем підтримки прийняття групових рішень на основі моделей проблемної області та полягає у виконанні наступних кроків: трансформації, ініціалізації та оновлення ймовірностей. Алгоритм зв'язного дерева орієнтований на побудову моделей на основі теорії Баєсових мереж [13]. Для випадку використання у розробленій системі підтримки прийняття рішень даний алгоритм був модифікований. Реалізація розробленої розподіленої системи підтримки прийняття групових рішень базується на технології "Client-Server" та використовує .NET Framework для обміну даними між користувачами [14]. Дана система розроблена для забезпечення спільної роботи користувачів над побудовою програмного коду у правильній послідовності. На виконання кожної послідовності дій користувачам відводиться певний час, по закінченню якого результати прийнятих рішень фіксуються та відбувається аналіз дій кожного користувача. Система забезпечує функціонування двох режимів: за принципом більшості та з використанням Баєсової мережі, що дозволяє порівняти ефективність прийнятих рішень та кількість конфліктних ситуацій [8, 14]. Для подальшої реалізації та дослідження розподіленої системи підтримки прийняття групових рішень було розроблено алгоритми роботи такої системи. Детальну схему алгоритму роботи розподіленої системи підтримки прийняття групових рішень наведено у [15].

Основу системи підтримки прийняття групових рішень складають десять основних програмних об'єктів [16, 17]. Узагальнену модель програмних модулів системи підтримки прийняття групових рішень та їх опис подано на рис.1 та у табл. 1.

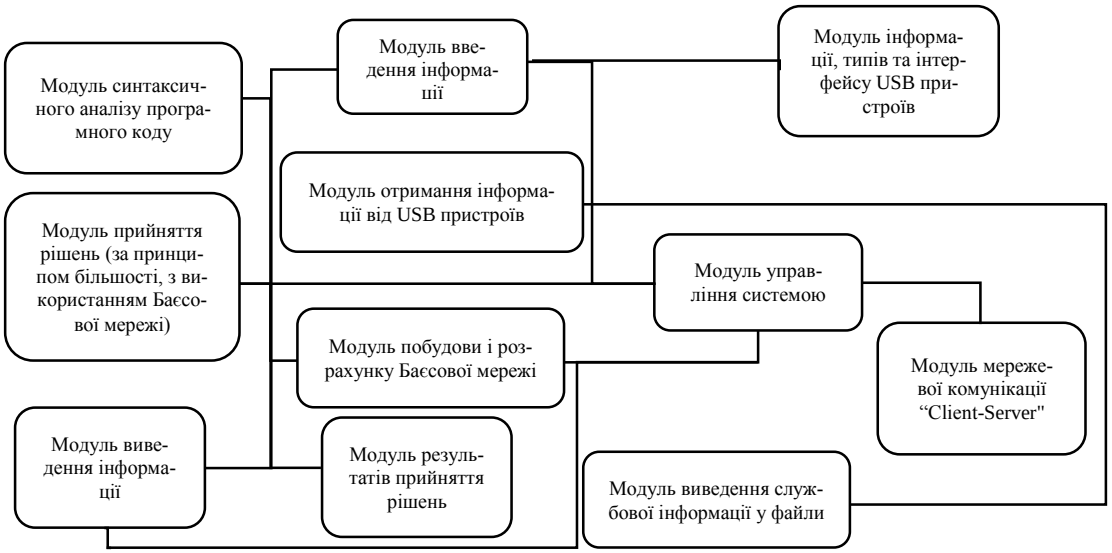

Рисунок 1 – Узагальнена модель програмних модулів розподіленої системи підтримки прийняття групових рішень

Основними програмними модулями є: модуль виведення інформації, модуль введення інформації, модуль прийняття рішень (за принципом більшості, з використанням Баєсової мережі), модуль результатів прийняття рішень, модуль управління системою, модуль отримання інформації від USB-пристроїв, модуль побудови і розрахунку Баєсової мережі, модуль синтаксичного аналізу програмного коду та модуль виведення службової інформації у файли. Обробка отриманих від пристроїв USB даних проводиться для знаходження комплексного рішення системи за отриманими від синтаксичного аналізатора і користувачів даними. Розглянемо детальніше основні програмні модулі, що забезпечують функціонування розробленої розподіленої системи підтримки прийняття групових рішень. Програмний модуль виведення інформації використовується для модифікації графічної інформації та виведення її на монітори користувачів. Під графічною інформацією розуміємо наповнення блоків прийняття рішень.

Табл. 1 – Опис програмних модулів розподіленої системи підтримки прийняття групових рішень

Програмний модуль	**Параметри модуля**	**Опис**
Виведення інформації	Initialize	Підготовка модуля до роботи
	UpdateDecisionPanel	Оновлення зображення панелі прийняття рішень та коригування графічної інформації з урахуванням отриманих системою даних
	UpdateResultPanel	Оновлення панелі виведення результатів процесу прийняття рішень
	SetCoords	Встановлення координат зони відображення інформації
Введення інформації	m_listDevs	Список пристроїв, які підключені до системи та допоміжної інформації
	m_refOutput	Посилання на модуль виведення даних
	m_refDecisionPanel	Посилання на модуль прийняття рішень
	Initialize	Підготовка модуля до роботи
	ReadCallback	Викликається кожен раз, коли з'являються нові дані від пристроїв введення інформації
Прийняття рішень (за принципом більшості, з використанням Баєсової мережі)	m_refOutput	Відображення результатів прийнятих рішень
	m_refDecisionPanel	Посилання на модуль прийняття рішень
	m_refBayesNet	Посилання на модуль побудови і розрахунку Баєсової мережі
	Initialize	Підготовка модуля до роботи
	SetSelection	Встановлення поточної обраної альтернативи
	GetSelection	Визначення поточної обраної альтернативи
Інформації, типів та інтерфейсу USB пристроїв	Usbd_mouse	Тип пристрою: USB миша
	Usbd_keyboard	Тип пристрою: Клавіатура
	Usbd_both	Обидва типи пристроїв (USB миша та клавіатура)
	Type	Інформація про вид пристрою
	Device	Тип пристрою USB миша або клавіатура
	Buttons	Інформація про стан клавіш
	LastX	Останнє зміщення курсору по горизонталі (в пікселях)
	LastY	Останнє зміщення курсору по вертикалі (в пікселях)
	VirtKey	Інформація про код віртуальної клавіші (тільки для клавіатури)

	EnumDevices	Визначення наявних пристроїв введення інформації, що підключені до системи
	InitDevices	Визначення видів пристроїв та підготовка їх до початку роботи
	StopDevices	Завершення роботи усіх задіяних пристроїв та звільнення ресурсів системи
Результатів прийняття рішень	Initialize	Підготовка модуля до роботи
	m_refOutput	Посилання на модуль виведення інформації
	SetObject	Встановлення об'єкта
	SaveResult	Збереження файлів з результатами рішень
Управління системою	m_refDecisionPanel	Посилання на модуль панелі прийняття рішень
	m_refBayesNet	Посилання на модуль побудови і розрахунку Баєсової мережі
	m_refOutput	Посилання на модуль виведення інформації
	m_refInput	Посилання на об'єкт введення інформації
	Initialize	Підготовка модуля до роботи
Отримання інформації від USB пристроїв	m_listSTDDevices	Список пристроїв введення інформації
	m_lpReadCallback	Покажчик на функцію оберненого виклику
	Initialize	Підготовка модуля до роботи
	Enumerate	Визначення кількості наявних USB мишей та клавіатур.
	StartDevices	Запуск пристроїв введення та реалізації їх взаємодії
	RegisterDevices	Реєстрація певного виду пристроїв для подальшої роботи
	InitMsgWindow	Ініціалізація прихованого вікна повідомлень для отримання повідомлень від пристроїв введення
	MessageThreadProc	Реалізація потоку повідомлень призначеного для отримання інформації від пристроїв введення незалежно від головного потоку, що викликається
	WndProc	Реалізація обробки отриманих повідомлень прихованим вікном обробки повідомлень
Побудови і розрахунку Баєсової мережі	Initialize	Підготовка модуля до роботи
	Evaluate	Розрахунок мережі і визначення ймовірності появи альтернативи у будь-якому вершині
	GetChoices	Визначення найбільш ймовірних альтернатив
	Learn	Навчання мережі з використанням оперативних даних файлів, які містять програмний код
Виведення службової інформації у файли	m_hFile	Дескриптор файлу, в який виводиться службова інформація
	Open	Відкриття та підготовка певного файлу для виведення службової інформації
	Close	Закриття файлу виведення службової інформації
	WriteDate	Виведення у файл інформації, яка починається з поточної дати
	WriteTime	Виведення у файл інформації, яка починається з поточного часу
	Format	Форматування службової інформації, використовуючи текстовий рядок форматування
Синтаксичного аналізу програмного коду	m_refBayesNet	Посилання на об'єкт побудови і розрахунку Баєсової мережі
	Initialize	Підготовка модуля до роботи
	Open	Відкриття файлу для аналізу
	Close	Закриття файлу
	Learn	Навчання мережі в результаті синтаксичного аналізу файлу
	FindProbabilities	Розрахунок ймовірностей появи елементів програмного коду

Програмний модуль введення інформації призначений для отримання інформації від пристроїв введення, таких як миша і клавіатура. Даний модуль здійснює постійну обробку даних, та дозволяє підключати і обслуговувати нові пристрої у реальному часі. Програмний модуль прийняття рішень призначений для управління процесом прийняття рішень у системі. Модуль прийняття рішень може працювати в одному з двох режимів роботи: за принципом більшості та з використанням Баєсової мережі. У режимі роботи за принципом більшості модуль не взаємодіє з модулем побудови і розрахунку Баєсової мережі та приймає рішення самостійно. Програмний модуль результатів прийнятих рішень дозволяє подати результати у зручному для користувачів вигляді. Модуль управління системою запускає систему, готує її до роботи та запускає функції ініціалізації інших модулів у визначені моменти часу. Модуль інформації, типів та інтерфейсу USB пристроїв містить множину типів пристроїв, з якими може взаємодіяти система підтримки прийняття рішень, допоміжну інформацію про кожен пристрій та інтерфейс для взаємодії з модулем отримання інформації від USB-пристроїв. Програмний модуль отримання інформації від USB пристроїв використовується для визначення кількості наявних USB пристроїв (мишей та клавіатур), їх реєстрації та обробки отриманої від USB пристроїв інформації. Модуль побудови і розрахунку Баєсової мережі дозволяє будувати Баєсову мережу необхідної конфігурації та обчислювати її параметри. Модуль синтаксичного аналізу програмного коду виділяє основні структурні блоки тестової програми, формує з них альтернативи для прийняття рішень та визначає ймовірність використання елементів програми з метою навчання Баєсової мережі. Програмний модуль мережевої

комунікації “Client-Server” взаємодіє з модулем управління системою та забезпечує зв'язок комп’ютера адміністратора системи з комп’ютерами користувачів. Модуль виведення службової інформації у файли реєструє усі події, які відбуваються під час роботи системи. Усі програмні модулі системи підтримки прийняття групових рішень реалізовано за допомогою мови програмування C#.

Для реалізації програмних модулів системи підтримки прийняття групових рішень було розроблено ряд інтерфейсних елементів, що забезпечують простоту використання системи користувачами що територіально розподілені [18]. Головні інтерфейсні елементи системи представлено на рис. 2.

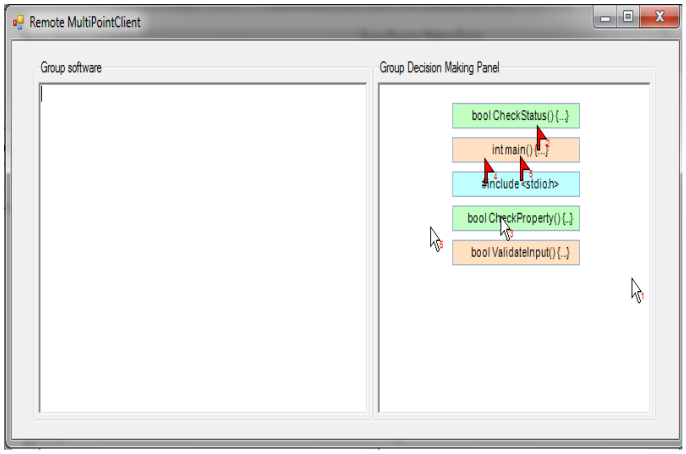

Рисунок 2 – Головні інтерфейсні елементи системи підтримки прийняття групових рішень

Розроблена розподілена система підтримки прийняття групових рішень візуально складається з двох основних частин: панелі групового програмного забезпечення та панелі групового прийняття рішень.

Панель групового прийняття рішень відображає наявні альтернатив на кожному етапі прийняття рішень. Алгоритм відображення інформації різниться в залежності від обраного режиму прийняття рішень: при використанні режиму за принципом більшості панель групового прийняття рішень відображає альтернативи, що базуються на синтаксичному аналізі програмного тестового коду, при використанні режиму з використанням Баєсової мережі панель групового прийняття рішень відображає альтернативи, ймовірності появи яких найбільші. Панель групового програмного забезпечення відображає обрані користувачами альтернативи та дозволяє будувати тестовий програмний код у правильній послідовності.

Розподілена система підтримки прийняття групових рішень являє собою програмний комплекс, що базується на розробленій інформаційній технології та моделях та включає систему прийняття групових рішень за принципом більшості та прийняття групових рішень з використанням Баєсової мережі [19]. Розроблена розподілена система забезпечує технічну та інформаційну підтримку користувачів під час прийняття рішень, при цьому враховує рівень знань користувачів у галузі, що розглядається. Система адаптована до навчання та тестування студентів які вивчають дисципліни пов’язані з розробкою та аналізом якості програмного коду.

Для перевірки працездатності розподіленої системи та її ефективності було проведено серію дослідів [7]. На рис. 3 подано графік часу прийняття рішень кожним користувачем системи при використанні режиму за принципом більшості (у мілісекундах).

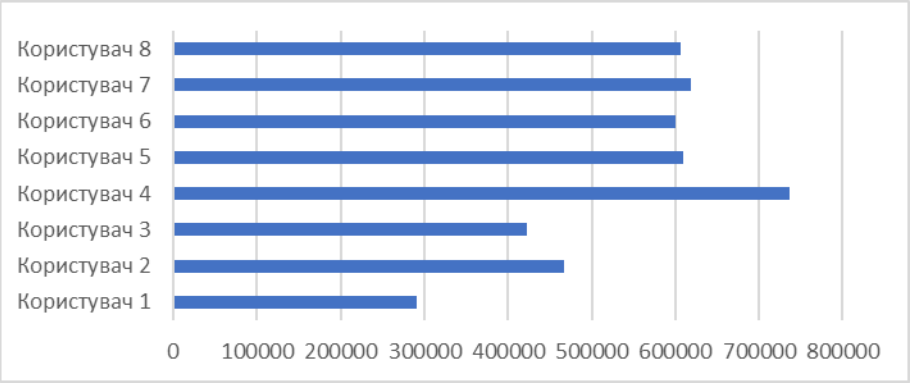

Рисунок 3 – Загальний час прийняття рішень кожним користувачем при використанні режиму за принципом більшості

Узагальнимо результати даних по часу прийняття рішень системою для кожного користувача при використанні режиму за принципом більшості (у мілісекундах) (рис.4):

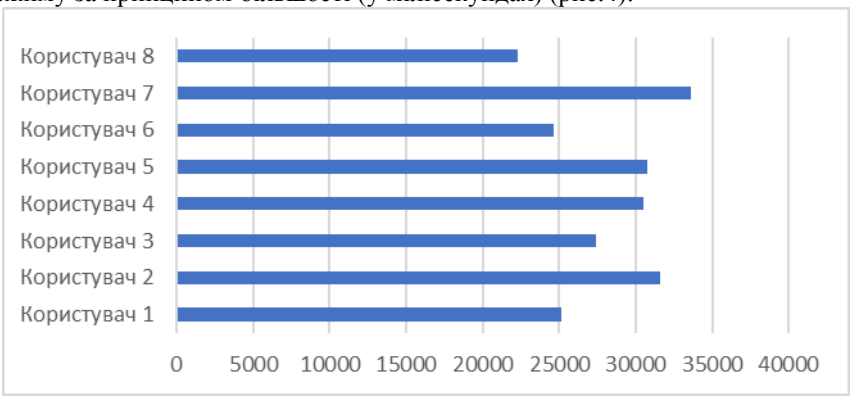

Рисунок 4 – Час прийняття рішень системою для кожного користувача при використанні режиму за принципом більшості

Загальний час прийняття рішень кожним користувачем при використанні режиму Баєсових мереж (у мілісекундах) подано на рис. 5:

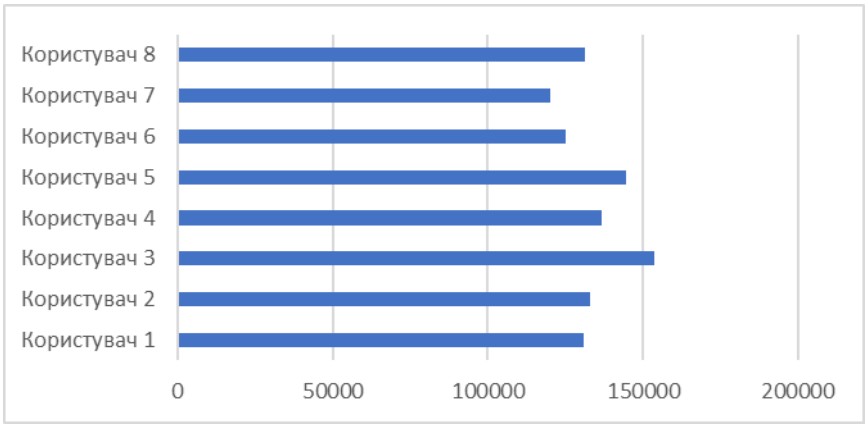

Рисунок 5 – Загальний час прийняття рішень кожним користувачем при використанні режиму Баєсових мереж

Визначимо загальний час прийняття рішень системою на кожному етапі вибору альтернатив при використанні Баєсових мереж (у мілісекундах) (рис. 6):

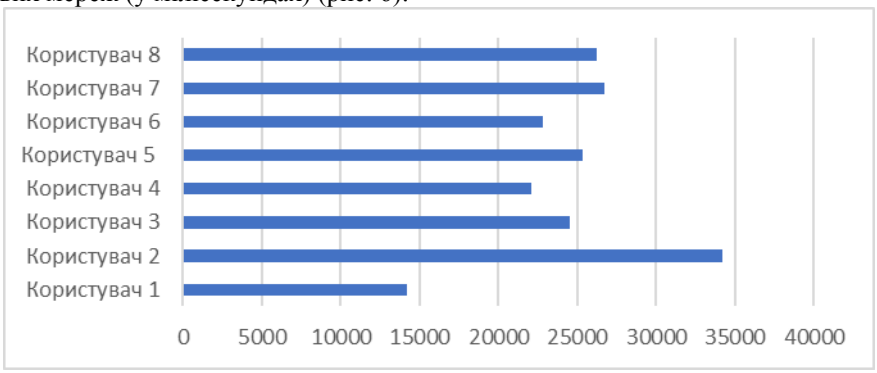

Рисунок 6 – Загальний час прийняття рішень системою на кожному етапі вибору альтернатив при використанні режиму Баєсових мереж

Проведення експериментальних досліджень дозволило сформувати графік залежностей (рис. 7-8) кількості конфліктних ситуацій від часу виконання завдань.

Рисунок 7– Графік залежності кількості конфліктних ситуацій від часу виконання завдання при використанні принципу більшості

Рисунок 8 – Графік залежності кількості конфліктних ситуацій від часу виконання завдання при використанні Баєсової мережі

Експериментальне дослідження розробленої розподіленої системи підтримки прийняття групових рішень дозволило підтвердити ефективність системи під час з'єднання групи користувачів, що територіально розподілені. У результаті проведених тестових досліджень також було виявлено, що використання Баєсових мереж для підтримки групового вибору у розподіленій системі підтримки прийняття групових рішень дозволяє значно підвищити ефективність прийняття рішень, за рахунок значного зменшення кількості конфліктних ситуацій.

Висновки

У статті запропоновано інформаційну технологію розподіленої системи підтримки прийняття групових рішень, яка на відміну від існуючих технологій реалізує два режими роботи користувачів: за принципом більшості та з використанням Баєсової мережі, що дозволяє, одночасно враховувати рішення багатьох користувачів, формувати на їх основі єдине рішення групи користувачів, та разом з процесом формування комплексного рішення проводити тестування, навчання та закріплення знань користувачів. Запропоновано також інформаційну модель розподіленої системи підтримки прийняття групових рішень, яка дозволяє органічно поєднувати усі елементи розподіленої системи та визначає їх взаємодію між собою. Основними характеристиками інформаційної моделі є можливість взаємодії знань користувачів, шляхом введення нових свідоцтв у мережу для прийняття рішень та знань мережі, що формуються під час синтаксичного аналізу елементів програмного коду і визначення ймовірності їх появи у тексті програмного коду. Запропоновано динамічні структури даних для формування альтернатив, які на відміну від існуючих дозволяють враховувати апріорну ймовірність обрання кожної конкретної альтернативи та динамічно оновлюються під час кожного етапу прийняття рішень користувачами. Розроблену систему пропонується використовувати для навчання та оцінювання знань студентів комп'ютерних наук.

Список літератури

[1] Пєтух А. М. Методи прийняття рішень і прогнозування подій в інтерактивних системах / А. М. Пєтух, Н. Ф. Кузьміна, Є. В. Кузьмін, В. В. Войтко // Збірник матеріалів третьої науково-практичної конференції «Матеріали електронної техніки та сучасні інформаційні технології (МЕТІТ-3)» / Кременчук. – 2008. – С. 228.

[2] Турунтаев Л. П. Теория принятия решений: Учебное пособие / Турунтаев Л. П.; Томский межвузовский центр дистанционного образования. — Томск: 2007. — 197 с.

[3] Пєтух А. М. Методи групового вибору в інтерактивних системах колективної взаємодії / А. М. Пєтух, В. В. Войтко, Є. В. Кузьмін, Н. Ф. Кополовець, С. М. Бурбело // Збірник матеріалів міжвузівської науково-практичної конференції «Прогресивні інформаційні технології в науці та освіті» / Вінниця. – 2007. – С. 188–195.

[4] Кузьміна Н. Ф. Огляд методів обчислення Байєсових мереж / Н. Ф. Кузьміна, А. М. Пєтух // Вісник Сумського державного університету. Сер.: Технічні науки. – 2012. – №1. – С. 112-117.

[5] Turban E. Decision support and expert systems: management support systems / E. Turban. – Englewood Cliffs, N.J.: Prentice Hall, 1995 – 887 p.
[6] Пєтух А. М. Принципи реалізації групового вибору в інтерактивних системах колективної взаємодії / А. М. Пєтух, В. В. Войтко, Є. В. Кузьмін, Н. Ф. Кузьміна // Нові технології. Науковий вісник Кременчуцького університету економіки, інформаційних технологій і управління. – 2008. – №1 (19). – С. 160–166.
[7] Кузьміна Н. Ф. Аналіз основних характеристик розподіленої системи підтримки прийняття групових рішень / Н. Ф. Кузьміна // Сборник научных трудов SWorld. – Иваново: МАРКОВА АД. – 2013. – Выпуск 3. – Том 6. – С. 84–87.
[8] Пєтух А. М. Автоматизована система підтримки групових рішень / А. М. Пєтух, В. В. Войтко, Є. В. Кузьмін, Н. Ф. Кузьміна // Вісник Вінницького політехнічного інституту. – 2009. – №1. – С. 76-79.
[9] Williamson J. Bayesian Nets and Causality. Philosophical and Computational Foundations / J. Williamson. – Oxford University Press Inc, New York, 2005 – 239 p.
[10] N. Kuzmina, "The informational model of Bayesian networks clustering methods in group decision making support systems", Norwegian journal of development of the international science, №39, Vol. 1, 2020. – p. 22-25.
[11] Чорна О.В. Модифікований метод автоматизації прийняття управлінських рішень для створення команди управління проектами / О.В. Чорна, Л.А. Люшенко, Н.А. Рибачок. – УсиМ, №2, 2019. – с. 32-39.
[12] «Комп'ютерна програма групового прийняття рішень щодо виконання послідовності дій з використанням принципу медіани Кемені в системах колективної взаємодії» / Н. Ф Кузьміна., Є. В. Кузьмін. – Свідоцтво про реєстрацію авторського права на твір №23007 від 3.12.2007 р.
[13] Тулупьев А. Л. Байесовские сети: Логико–вероятностный подход / А. Л. Тулупьев, С. И. Николенко, А. В. Сироткин – СПб. : Наука, 2006. – 607 с.
[14] «Комп'ютерна програма підтримки прийняття групових рішень на основі Байєсової мережі» / Є. В. Кузьмін, Н. Ф Кузьміна. – Свідоцтво про реєстрацію авторського права на твір №25844 від 25.09.2008 р.
[15] А. Пєтух, В. Войтко, Є. Кузьмін, Н. Кузьміна, Модель процесу підтримки прийняття рішень з використанням Байєсових мереж, Наукові праці Вінницького національного технічного університету,
№ 3, 1.
[16] Пєтух А. М. Моделі режимів групового вибору користувачів в інтерактивній системі колективної взаємодії / А. М. Пєтух, В. В. Войтко, Є. В. Кузьмін, Н. Ф. Кополовець, С. В. Бевз // Оптико-електронні інформаційно-енергетичні технології. – Вінниця: УНІВЕРСУМ. – 2007. – №1(13). – С. 80–86.
[17] Пєтух А. М. Модель системи підтримки прийняття групових рішень / А. М. Пєтух, В. В. Войтко, Є. В. Кузьмін, Н. Ф. Кузьміна // Збірник матеріалів шостої міжнародної конференції ІОН – 2008 / Вінниця: УНІВЕРСУМ-Вінниця. – 2008. – Том 2. – С. 514–517.
[18] Пєтух А. М. Інтерфейсні елементи системи колективного тестуючого навчання / А. М. Пєтух, В. В. Войтко, Д. І. Катєльніков, Н. Ф. Кополовець // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2007. – №1. – С. 98–106.
[19] «Розподілена система підтримки прийняття групових рішень» / Н. Ф Кузьміна, Є. В. Кузьмін. – Свідоцтво про реєстрацію авторського права на твір №50446 від 26.07.2013 р.

Стаття надійшла: 17.02.20.

References

[1] Pietukh A. M. Metody pryiniattia rishen i prohnozuvannia podii v interaktyvnykh systemakh / A. M. Pietukh, N. F. Kuzmina, Ye. V. Kuzmin, V. V. Voitko // Zbirnyk materialiv tretoi naukovo-praktychnoi konferentsii «Materialy elektronnoi tekhniky ta suchasni informatsiini tekhnolohii (METIT-3)» / Kremenchuk. – 2008. – C. 228.
[2] Turuntaev L. P. Teoryia pryniatyia reshenyi: Uchebnoe posobye / Turuntaev L. P.; Tomskyi mezhvuzovskyi tsentr dystantsyonnoho obrazovanyia. — Tomsk: 2007. — 197 s.
[3] Pietukh A. M. Metody hrupovoho vyboru v interaktyvnykh systemakh kolektyvnoi vzaiemodii / A. M. Pietukh, V. V. Voitko, Ye. V. Kuzmin, N. F. Kopolovets, S. M. Burbelo // Zbirnyk materialiv mizhvuzivskoi naukovo-praktychnoi konferentsii «Prohresyvni informatsiini tekhnolohii v nautsi ta osviti» / Vinnytsia. – 2007. – S. 188–195.
[4] Kuzmina N. F. Ohliad metodiv obchyslennia Baiiesovykh merezh / N. F. Kuzmina, A. M. Pietukh // Visnyk Sumskoho derzhavnoho universytetu. Ser.: Tekhnichni nauky. – 2012. – №1. – S. 112-117.
[5] Turban E. Decision support and expert systems: management support systems / E. Turban. – Englewood Cliffs, N.J.: Prentice Hall, 1995 – 887 p.

[6] Pietukh A. M. Pryntsypy realizatsii hrupovoho vyboru v interaktyvnykh systemakh kolektyvnoi vzaiemodii / A. M. Pietukh, V. V. Voitko, Ye. V. Kuzmin, N. F. Kuzmina // Novi tekhnolohii. Naukovyi visnyk Kremenchutskoho universytetu ekonomiky, informatsiinykh tekhnolohii i upravlinnia. – 2008. – №1 (19). – С. 160–166.
[7] Kuzmina N. F. Analiz osnovnykh kharakterystyk rozpodilenoi systemy pidtrymky pryiniattia hrupovykh rishen / N. F. Kuzmina // Sbornyk nauchnыkh trudov SWorld. – Yvanovo: MARKOVA AD. – 2013. – Vыpusk 3. – Tom 6. – S. 84–87.
[8] Pietukh A. M. Avtomatyzovana systema pidtrymky hrupovykh rishen / A. M. Pietukh, V. V. Voitko, Ye. V. Kuzmin, N. F. Kuzmina // Visnyk Vinnytskoho politekhnichnoho instytutu. – 2009. – №1. – S. 76-79.
[9] Williamson J. Bayesian Nets and Causality. Philosophical and Computational Foundations / J. Williamson. – Oxford University Press Inc, New York, 2005 – 239 p.
[10] N. Kuzmina, "The informational model of Bayesian networks clustering methods in group decision making support systems", Norwegian journal of development of the international science, №39, Vol. 1, 2020. – p. 22-25.
[11] Chorna O.V. Modyfikovanyi metod avtomatyzatsii pryiniattia upravlinskykh rishen dlia stvorennia komandy upravlinnia proektamy / O.V. Chorna, L.A. Liushenko, N.A. Rybachok. – UsyM, №2, 2019. – s. 32-39.
[12] «Kompiuterna prohrama hrupovoho pryiniattia rishen shchodo vykonannia poslidovnosti dii z vykorystanniam pryntsypu mediany Kemeni v systemakh kolektyvnoi vzaiemodii» / N. F Kuzmina., Ye. V. Kuzmin. – Svidotstvo pro reiestratsiiu avtorskoho prava na tvir №23007 vid 3.12.2007 r.
[13] Tulupev A. L. Baiesovskye sety: Lohyko–veroiatnostnыi podkhod / A. L. Tulupev, S. Y. Nykolenko, A. V. Syrotkyn – SPb. : Nauka, 2006. – 607 s.
[14] «Kompiuterna prohrama pidtrymky pryiniattia hrupovykh rishen na osnovi Baiiesovoi merezhi» / Ye. V. Kuzmin, N. F Kuzmina. – Svidotstvo pro reiestratsiiu avtorskoho prava na tvir №25844 vid 25.09.2008 r.
[15] A. Pietukh, V. Voitko, Ye. Kuzmin, N. Kuzmina, Model protsesu pidtrymky pryiniattia rishen z vykorystanniam Baiiesovykh merezh, Naukovi pratsi Vinnytskoho natsionalnoho tekhnichnoho universytetu, № 3, 1.
[16] Pietukh A. M. Modeli rezhymiv hrupovoho vyboru korystuvachiv v interaktyvnii systemi kolektyvnoi vzaiemodii / A. M. Pietukh, V. V. Voitko, Ye. V. Kuzmin, N. F. Kopolovets, S. V. Bevz // Optykoelektronni informatsiino-enerhetychni tekhnolohii. – Vinnytsia: UNIVERSUM. – 2007. –№1(13). – С. 80–86.
[17] Pietukh A. M. Model systemy pidtrymky pryiniattia hrupovykh rishen / A. M. Pietukh, V. V. Voitko, Ye. V. Kuzmin, N. F. Kuzmina // Zbirnyk materialiv shostoi mizhnarodnoi konferentsii ION – 2008 / Vinnytsia: UNIVERSUM-Vinnytsia. – 2008. – Tom 2. – С. 514–517.
[18] Pietukh A. M. Interfeisni elementy systemy kolektyvnoho testuiuchoho navchannia / A. M. Pietukh, V. V. Voitko, D. I. Katielnikov, N. F. Kopolovets // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – 2007. – №1. – С. 98–106.
[19] «Rozpodilena systema pidtrymky pryiniattia hrupovykh rishen» / N. F Kuzmina, Ye. V. Kuzmin. – Svidotstvo pro reiestratsiiu avtorskoho prava na tvir №50446 vid 26.07.2013.

Відомості про авторів

Квєтний Роман Наумович – д. т. н., професор, завідувач кафедрою автоматизації та інтелектуальних інформаційних технологій ВНТУ, член-кореспондент Національної академії педагогічних наук України Хмельницьке шосе 95, м. Вінниця 21021.

Кузьміна Наталя Федорівна – здобувач кафедри автоматизації та інтелектуальних інформаційних технологій ВНТУ

Р. Н. Кветный, Н. Ф. Кузьмина

РАСПРЕДЕЛЕННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ ГРУППОВЫХ РЕШЕНИЙ

Винницкий национальный технический университет, Винница

R. N. Kvyetnyy, N. F. Kuzmina

DISTRIBUTED GROUP DECISION SUPPORT SYSTEM

Vinnitsa National Technical University, Vinnitsa

УДК 004.63

Л. А. Савицька, Т. І. Коробейнікова, П. В. Чирва

МЕТОД ТА КРОСПЛАТФОРМЕНИЙ ЗАСІБ АРХІВАЦІЇ ОДНОТИПНИХ ФАЙЛІВ

Вінницький національний технічний університет, Вінниця

Анотація. Дана робота присвячена розробці методу та кросплатформеній реалізації засобу архівації однотипних файлів. Цей програмний засіб дозволить ефективно виконувати архівацію великої кількості однотипних файлів.

Високий рівень вирішення поставленої задачі досягнуто за рахунок використання сучасної мови програмування Java.

В даній роботі виконано дослідження і аналіз сучасних методів та засобів архівації даних в галузі інформаційних технологій, аналіз підходів, методів та моделей архівації даних. Розглянуті методи стиснення та архівації даних та їх порівняльна характеристика. Виконано огляд сучасних засобів архівації даних, а саме, процеси архівації за кросплатформеною технологією Java. Дослідження, виконані під час дослідження, ґрунтуються на теоретико-множинних підходах і принципах кросплатформеного підходу для виконання процесів архівації за кросплатформеною технологією Java; структурному проектуванні програмного забезпечення – для реалізації кросплатформеного програмного забезпечення архівації однотипних файлів; методах об'єктно-орієнтованого програмування – для реалізації алгоритмів і процесів методу архівації однотипних файлів та розробки відповідного програмного забезпечення.

Зокрема, у роботі розроблено метод архівації однотипних файлів, вдосконалено процес формування основного словника, вдосконалено процес архівації файлів.

Ключові слова: метод та кросплатформена реалізація засобу архівації однотипних файлів, методи стиснення та архівації даних, кросплатформена технологія Java, ключовий файл, початковий словник, однотипні файли, стиснення з втратами, стиснення без втрат.

Abstract. This work is devoted to the development of a method and cross-platform implementation of a file archiving tool of the same type. This software tool will allow you to efficiently archive a large number of files of the same type.

The high level of the solution to this task was achieved through the use of modern Java programming language.

In this thesis research and analysis of modern methods and means of archiving of data in the field of information technologies, analysis of approaches, methods and models of data archiving have been performed. The methods of compression and archiving of data and their comparative characteristics are considered. An overview of modern data archiving tools is performed, namely, processes of archiving on a cross-platform Java technology. The research performed during the research is based on multiple-theoretical and cross-platform approaches for performing cross-platform archiving of Java technology; structural software design - for implementation of cross-platform archiving of the same files; object-oriented programming methods - to implement algorithms and processes of the method of archiving of the same files and development of the corresponding software.

In particular, the method of archiving of the same type files has been developed, the process of formation of the main vocabulary has been improved, the file archiving process has been improved.

Keywords: method and cross-platform implementation of the same file archiving tool, data compression and archiving methods, cross-platform Java technology, key file, source dictionary, single file, lossy compression, lossless compression.

Аннотация. Данная работа посвящена разработке метода и кроссплатформенных реализации средства архивации однотипных файлов. Этот про- программно средство позволит эффективно выполнять архивацию большого количества однотипных файлов.

Высокий уровень решения поставленной задачи достигнуто за счет использования современного языка программирования Java.

В данной работе выполнено исследование и анализ современных методов и средств архивации данных в области информационных технологий, анализ подходов, методов и моделей архивации данных. Рассмотрены методы сжатия и архивации данных и их сравнительная характеристика. Выполнен обзор современных средств архивации данных, а именно, процессы архивации по кросплатформеною технологии Java. Исследования, выполненные в ходе исследования, основанные на теоретико-множественных подходах и принципах кроссплатформенных подхода для выполнения процессов архивации по кросплатформеною технологии Java; структурном проектировании программного обеспечения - для реализации кроссплатформенных программного обеспечения архивации однотипных файлов; методах объектно-ориентированного программирования - для реализации алгоритмов и процессов метода архивации однотипных файлов и разработки соответствующего программного обеспечения.

В частности, в работе разработан метод архивации однотипных файлов, усовершенствован процесс формирования основного словаря, усовершенствован процесс архивации файлов.

Ключевые слова: метод и кроссплатформенных реализация средства архивации однотипных файлов, методы сжатия и архивации данных, кросплатформена технология Java, ключевой файл, начальный словарь, однотипные файлы, сжатие с потерями, сжатие без потерь.

DOI: https://doi.org/10.31649/1999-9941-2020-47-1-14-21.

Вступ

Задача компактного зберігання, перетворення та передавання інформаційних даних завжди була актуальною в галузі інформаційних технологій.

Інформаційні ресурси нині є продуктом інтелектуальної діяльності дійсно найбільш кваліфікованої й творчо активної частини молоді та працездатного населення світу. В останній чверті XX століття набуті інформаційні ресурси досягли (і продовжують досягати) настільки рекордних обсягів, що цілком повсякденним стали поняття «інформаційного вибуху», «інформаційної революції». В якості доказу є об'єктивне збільшення інформаційного потоку з початку цього сторіччя більш ніж в 30 разів! [1].

Актуальність

Отже, **актуальною** є наукова задача розробки та застосування принципово нових методів і засобів сприйняття, передачі, обробки, зберігання і розповсюдження інформаційних даних, таких, що здатних оперувати великими масивами інформації, причому, у реальному часі.

З метою забезпечити надійне збереження інформації створюють резервні копії даних. Задача збереження резервних копій у компактному вигляді є основою для процесів архівації та стиснення даних. В загальному випадку, основний зміст архівації полягає у створенні таких резервних копій, які потребували би значно меншого обсягу на інформаційних ресурсах, ніж та сама інформація у вихідному стані. Таким чином, в контексті під архівацією слід розуміти процес перекодування деякої сукупності файлів з метою зменшення загального об'єму пам'яті, який вони займають. Часто архівацією ще називають процес стиснення даних [3].

Нині відомо досить багато різних підходів до процесу архівації. Усі підходи мають в своїй основі різні підходи та різні методи, проте подібні вони в одному – це те, що вони сповідують принцип заміни рівномірного двійкового коду на нерівномірний. З метою архівації файлів та папок використовують спеціальні програмні засоби, які називають архіваторами. Стиснуті файли поміщають у файли, який називають архівами [2].

Перші прототипи архіваторів з'явилися у 80-х роках минулого сторіччя. Основними можливостями сучасних архіваторів є такі:

- занесення груп файлів та (або) підкаталогів в архів;
- можливість поновлення архіву;
- перегляд файлів з меж архіву;
- вилучення окремих файлів з архіву;
- захист файлів від несанкціонованого доступу (НСД);
- перевірка архіву на цілісність;
- створення багатотомних архівів;
- можливість створення архівів, що автоматично відкриваються.

Можливості сучасних програм-архіваторів дозволяють зекономити від 20 до 90 відсотків дискового простору. Файлом, що знаходиться в архіві, можна скористатися після того, як він буде відновлений у початковому вигляді, тобто розархівований (розпакований). Розархівування виконують або ті ж самі програми-архіватори в зворотному напрямку, або окремі програми, які називають розраховаторами, серед яких найбільш відомими є: ZIP, JAR, RAR. Під час вибору конкретного засобу для архівування (розархівування) користувачі керуються багатьма критеріями, як то швидкістю роботи, коефіцієнти стискування даних, інтерфейс, сумісність тощо. Важливим є те, що для одного типу файлів кращим може бути один архіватор, а для іншого – інший [5].

Мета

Метою дослідження є збільшення середнього значення процесу архівації для великої кількості однотипних файлів.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз сучасних методів та засобів архівації даних в галузі інформаційних технологій, виконати їх порівняльну характеристику та сформувати вимоги та обрати й обґрунтувати вибір методу, що задовольняв би меті даного дослідження;
- розглянути існуючі способи архівації за кросплатформеною технологією Java;
- запропонувати метод архівації однотипних файлів згідно мети магістерської кваліфікаційної роботи, розробити ключові процеси роботи методу архівації однотипних файлів та виконати програмну реалізацію запропонованого методу архівації однотипних файлів;
- провести тестування програмного продукту та виконати аналіз отриманих результатів.

Сучасні методи архівації даних в галузі інформаційних технологій

Характерною особливістю усіх наявних типів інформаційних даних є їх надлишковість. Для людини, як для суб'єкта, надлишковість цих даних часто пов'язана із якістю отриманої даних, оскільки така надлишковість покращує нам зрозумілість та сприйняття цієї даних. Проте, коли ми говоримо про зберігання та передавання даних засобами обчислювальної техніки, то наявність надлишковості відіграє дуже негативну роль, оскільки вона призводить до зростання вартості зберігання та передавання даних [4].

Особливо актуальною є ця задача у випадках необхідності оброблення величезних обсягів даних при незначних чи недостатніх об'ємах носіїв даних. У зв'язку із цим постійно виникає задача відійти від надлишковості або процесу стиснення та архівації даних.

Базовий принцип, що є основою для процесу стиснення та архівації даних, полягає в економічному описанні повідомлення, згідно якого можливе відновлення його початкового значення із похибкою, яка контролюється [4].

Аналіз підходів, методів та моделей архівації даних

Методи стиснення та архівації даних можна розділити на два типи:

1) без спотворення (loseless) – методи стиснення та архівації гарантують, що декодовані дані будуть в збігатися із вихідними;
2) із втратами (lossy) – методи процесу стиснення та архівації можуть спотворювати вихідні дані, за рахунок видалення несуттєвих частин даних, після чого повне відновлення неможливе .

Методи стиснення та архівації даних без втрат засновані на усуненні надлишковості подання даних. Ефективність кодування досягається за рахунок подання малоймовірних подій більш довгими словами, ніж подій із вищою ймовірністю настання.

Якщо ймовірність настання події є деяке значення P, то, відповідно теоремі Шеннона, цю подію варто кодувати словом завдовжки -log2P біт. Методи стиснення та архівації даних явно або неявно мають в основі саме це [4].

У результаті процесів ефективного кодування «1» вихідних даних ставиться у відповідність КС (КС). КС складається із послідовності двійкових цифр. Сукупність кодових слів утворює сам код. У випадку, коли довжини всіх кодових слів сталі, то застосовується код має фіксовану (постійну) довжину, інакше – змінну. Якщо вихідні дані можуть бути відновлені по масиву кодових слів, то кодування не призводить до втрат даних.

Ефективність процесів стиснення та архівації визначається ступінню стиснення. Ступінь самого стиснення становить значення, яке дорівнює відношенню обсягу вихідних даних до об'єму відповідних їм стиснутих даних і вимірюється в кількості разів.

Всі методи стиснення та архівації прийнято розділяти на 2 класи:

1) статистичного кодування
2) словникового стиснення та архівації [2].

У схемах процесів стиснення та архівації часто застосовуються допоміжні перетворення, що забезпечують та сприяють виконанню ефективного кодування.

Метод та кросплатформений засіб архівації однотипних файлів

Розроблений метод призначений для процесів оптимізованої архівації великих кількостей маленьких однотипних файлів. В основі роботи запропонованого методу архівації однотипних файлів є ідея заміни повторного входження цілого блока даних посиланням на попередню позицію його входження.

Загальна схема складових та процесів методу архівації однотипних файлів зображена на рис. 1.

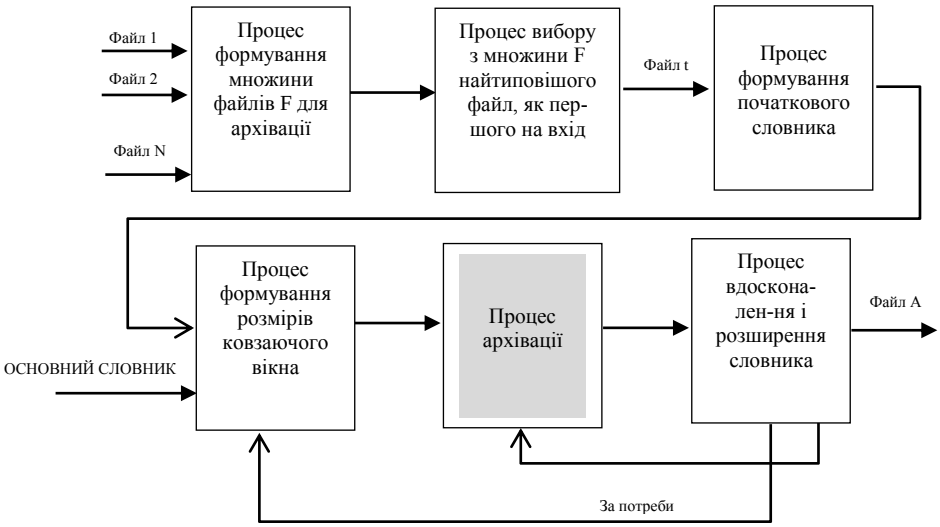

Рисунок 1 – Загальна схема методу архівації однотипних файлів

Метод архівації однотипних файлів передбачає забезпечення та виконання таких процесів:

1) Прийом на вхід множини файлів;
2) Процес формування множини файлів F для архівації;
3) Процес вибору з множини F найтиповішого файл, як першого на вхід;

4) Виокремлення такого ключового файлу;
5) Процес формування початкового словника;
6) Процес формування розмірів ковзаючого вікна. «Ковзаюче вікно» в даному випадку є динамічною структурою даних, що організована таким чином, аби містити в собі введену раніше інформацію та надавати до неї доступ;
7) Процес архівації. Передбачає звертання до елементів «ковзаючого вікна» і замість значень послідовності, що архівується, вставлення посилань на ці значення своєрідному «словнику»;
8) За потреби – перехід до процесу формування розмірів ковзаючого вікна.
9) Процес вдосконалення і розширення словника. Перехід на процес архівації знову;
10) Архівний файл А.

3.1 Розробка процесу формування початкового словника

Процес формування словника у стандартному використанні алгоритму LZ77 це формування комбінації, що повторюється і кодуються парою:

– довжина збігу (match length)
– зсув (offset) або дистанція (distance).

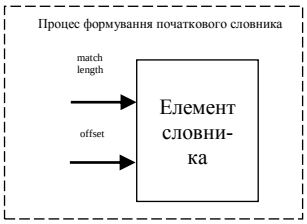

Рисунок 2 – Процес формування словника

Під час процесу формування початкового словника кожна така комбінація «довжина збігу + зсув» трактується як команда копіювання символів із певної позиції «ковзаючого вікна», або дослівно звучить так: «Повернутися назад в словнику на значення «зсуву» символів і скопіювати значення «довжини збігу» символів, починаючи із поточної позиції».

3.2 Розробка процесу архівації

Особливість розглянутого в даному методі архівації однотипних файлів є сам процесу архівації, який полягає в тому, що використання комбінації кодової пари «довжина-зміщення» є не тільки прийнятним, але й ефективним у тих випадках, коли значення довжини збігу *match length* перевищує значення зсуву *offset*.

В кінцевому підсумку, ступінь ефективності процесу та архівації в даному методі архівації однотипних файлів залежить від того, наскільки багато в файлі повторюваних комбінацій, і наскільки вони великі.

Це приводить нас до такої запропонованої ідеї: з метою збільшити кількість таких блоків, необхідно «об’єднати» всі файли, які планується архівувати, в один великий файл, і вже після цього його, цей великий файл, стискати. Звісно, такий підхід буде дуже ефективним для однотипних файлів (і виправдовує мету даної роботи), і вкрай неефективним для різних типів файлів, іншими словами, із різним профілем даних. Тому застосування запропонованого методу архівації однотипних файлів може давати високі результати роботи процесу архівації.

Оскільки запропонований метод тісно пов’язаний із змістом даних, що архівуються, можна говорити про ентропію.

В загальному випадку, дані, що отримуються приймачем несуть корисну інформацію, якщо має місце невизначеність відносно стану джерела даних. Величина, що визначає невизначеність окремого і-го повідомлення називають частковою ентропією (1).

$$M(x_i) = \frac{log_2 y}{p(x_i)} \quad (1)$$

І тоді кількість інформації і невизначеність для цієї множини випадкових повідомлень можна отримати шляхом усереднення по всіх елементам даних (2)-(3).

$$\mathrm{I}(x) = -\sum p(x_i) * \frac{log_a 1}{p(x_i)}; \tag{2}$$

$$H(x_i) = -\sum P(x_i) log_a p(x_i) \tag{3}$$

де $H(x_i)$ – ентропія.

Не дивлячись на те, що є співпадіння залежностей, все ж ентропія і кількість інформації є принципово різними. Сама ентропія, що виражає «середню невизначеність джерела» даних є характеристикою джерела даинх і, якщо нам доступна статистика повідомлень, яка може бути визначена заздалегідь. $I(x)$ є попередньою характеристикою і визначає кількість даних, що отримуються із вхідного повідомлення. $H(x)$ – це, так звана, міра нестачі інформації про стан окремої частини якоїсь системи чи системи. Пропорційно надходженню даних про стан системи, ентропія останньої стає меншою. Співпадіння виразів (2) і (3) говорить про те, що кількість отриманих даних в числововму еквіваленті дорівнює ентропії, що існує залежно від джерела даних на розглянутій частині каналу зв'язку тією кількості інформації з ентропією, що чітко проявляється діалектичний закон.

Середнє значення ентропії даних при однаковій кількості елементів може відрізнятися залежно від статистики і характеристик самих даних. Під час наявності зв'язків залежності між елементами даних, ентропія стає меншою. У випадках, коли зв'язки залежності охоплюють 2 або 3 елементи, тоді формула для обчислення ентропії стане (4) для 2 елементів і (5) для 3 елементів.

$$H(x) = -\sum\sum p(x_i, x_j) log_a p(x_i, x_j), \tag{4}$$

$$H(x) = -\sum\sum\sum p(x_i, x_j, x_k) log_a p(x_i, x_j, x_k) \tag{5}$$

Ті початкові дані є кращими, у яких показники ентропії є оптимальними. Виміром наскільки дані за своєю ентропією відрізняється оптимальних даних, покаже коефіцієнт архівації (6):

$$\mu = \frac{H(x)}{H(x)_{max}} \tag{6}$$

де $H(x)$ – реальне; $H(x)_{max}$ – ентропія відповідному йому оптимального повідомлення.

Якщо дані, що не є оптимальними і оптимальні деякі дані характеризуються однаковим значенням ентропієї, тоді справедлива така рівність (7)

$$n * H(x) = n' * H(x)\max, \tag{7}$$

де n – число елементів не оптимального повідомлення даних; n' – число елементів відносно оптимального повідомлення даних.

Оскільки ентропія для оптимальних даних є максимальною, тоді число елементів неоптимальних даних n завжди буде більшою від кількості елементів відповідних оптимальних даних n'. І тоді коефіцієнт ахівування можна виразити через кількість елементів повідомлення (8)

$$\mu = \frac{n'}{n}. \tag{8}$$

Так, реальні дані тоді при однаковій ступені інформативності володіють визначеною надлишковістю в своїх елементах у порівнянні з оптимальними даними. Дійсним коефіцієнтом архівування вважатимемо (9)

$$K_A = \frac{N_{in}}{N_{out}}. \tag{9}$$

де N_{in} – кількість двійкових розрядів на вході методу архівації. N_{out} – кількість двійкових розрядів на виході методу архівації.

В рамках даної роботи це було експериментально досліджено автором, і виявлено, що текстові файли були заархівовані гірше за файли реляційної бази даних. Саме цей факт пояснює тим, що в текстових (чи інших складних форматів) файлах, наявне досить незначне число повторюваних блоків в цих файлах.

В таблиці 1 наведено експериментальні дані архівації однотипних файлів по одному та однотипних файлів у кількості 10 шт. та 100 шт.

Середнє значення процесу архівації для різних типів файлів Arh_m розраховане для процесу архівації для різних типів файлів, кількість – 1 файл, процесу архівації для однотипних файлів, кількість – 10 файлів та процесу архівації для однотипних файлів, кількість – 100 файлів.

Таблиця 1 – Середнє значення процесу архівації

Тип файлів	Arh_m – 1 файл, %	Arh_m – 10 файлів, %	Arh_m – 100 файлів, %
Документ (*.docx)	62,875	40,33	47,4
Документ (*.doc)	37,7825	32, 567	35,7
Текстовий (*.txt)	55,305	47, 376	56,78
Бази даних (*.accdb)	18,89	83,02	85,189
Графічні файли (*.jpg)	27,31	28,5	30,01
Звукові файли (*.mp3)	76,4	77,08	78,5
HTML (*.html)	14,74	24,129	35,67
Усереднене значення показника архівування	41,9003571	50,612	52,75

На рис. 3 наведено графічне представлення результатів дослідження процесів архівації і виявлено, що розроблений метод архівації однотипних файлів гарно працює в умовах наявності не менше 10 файлів на вході методу, а при наявності більшої кількості (100 і більше) однотипних файлів значення Arh_m росте.

а)

Рисунок 3 – Діаграма процесу архівації

Запропонований метод архівації однотипних файлів дає приріст середнього значення процесу архівації на 10,85%. А зі збільшенням кількості однотипних файлів для процесу архівації цей показник може все більше зростати.

Висновки

Підсумком виконання даного дослідження роботи стала розробка методу та кросплатформеного засобу архівації однотипних файлів. Високий рівень виконання поставленої прикладної задачі вирішено засобами мови програмування Java.

Розроблений метод призначений для процесів оптимізованої архівації великих кількостей маленьких однотипних файлів. В основі запропонованого роботи методу архівації однотипних файлів є ідея заміни повторного входження цілого блока даних посиланням на попередню позицію його входження.

Зокрема, у роботі отримані такі наукові результати:

- вперше запропоновано метод архівації однотипних файлів, який дозволяє збільшити середнє значення процесу архівації однотипних файлів на 10, 85%;
- вдосконалено процес формування основного словника за рахунок застосування методу «ковзного вікна» до його формування;
- вдосконалено процес архівації за рахунок застосування вдосконаленого процесу формування основного словника.

Практичне значення одержаних результатів полягає у такому: розроблено новий метод архівації однотипних файлів, вдосконалено процес формування основного словника за рахунок застосування до його формування методу «ковзного вікна»; розроблено алгоритм роботи формування основного словника однотипних файлів, який дозволяє ефективніше стискати велику кількість однотипних файлів; розроблено програмний засіб для архівації однотипних файлів.

В рамках даної роботи виявлено, що розроблений метод архівації однотипних файлів гарно працює в умовах наявності не менше 10 файлів на вході методу, а при наявності більшої кількості (100 і більше) однотипних файлів значення Arh_m росте. Запропонований метод дає приріст середнього значення процесу архівації на 10,85%, а зі збільшенням кількості однотипних файлів для процесу архівації цей показник може все більше зростати.

Список літератури

[1] Семѐнов Ю. Телекоммуникационные технологи / Семенов Ю. – М.: Бином. Лаборатория знаний, 2007. – 640с.
[2] Luzhetsky, V.A., Savytska, L.A., Troianovska, T.I. Adaptive compression methods of data based on Fibonacci linear forms. G.2017 Proceedings of SPIE - The International Society for Optical Engineering.
[3] Сергеенко В. Сжатие данных, речи, звука и изображений в телекоммуникационных системах / Сергеенко В., Баринов В. – М.: КудицОбраз, 2009. – 360с.
[4] Молдовян А. Криптография / Молдовян А., Советов Б. – М.: Лань, 2000. – 224с.
[5] Макконнелл С. Совершенный код / Макконнелл С. – СПб.: Питер, 2007. – 896с.
[6] Azarov, O.D., Troianovska, T.I., Savytska, L.A., Kozbekova, A., Sagymbekova, A. Quality of content delivery in computer specialists training system. G.2017 Proceedings of SPIE - The International Society for Optical Engineering.

Стаття надійшла: 12.12.19.

References

[1] Semènov Yu. Telekommunykatsyonnыe tekhnolohy / Semenov Yu. – M.: Bynom. Laboratoryia znanyi, 2007. – 640s.
[2] Luzhetsky, V.A., Savytska, L.A., Troianovska, T.I. Adaptive compression methods of data based on Fibonacci linear forms. G.2017 Proceedings of SPIE - The International Society for Optical Engineering.
[3] Serheenko V. Szhatye dannыkh, rechy, zvuka y yzobrazhenyi v telekommunykatsyonnыkh systemakh / Serheenko V., Barynov V. – M.: KudytsObraz, 2009. – 360s.
[4] Moldovian A. Kryptohrafyia / Moldovian A., Sovetov B. – M.: Lan, 2000. – 224s.
[5] Makkonnell S. Sovershennыi kod / Makkonnell S. – SPb.: Pyter, 2007. – 896s.
[6] Azarov, O.D., Troianovska, T.I., Savytska, L.A., Kozbekova, A., Sagymbekova, A. Quality of content delivery in computer specialists training system. G.2017 Proceedings of SPIE - The International Society for Optical Engineering.

Відомості про авторів

Савицька Людмила Анатоліївна, к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця, Хмельницьке шосе, 95

Коробейнікова Тетяна Іванівна, к.т.н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця, Хмельницьке шосе, 95

Чирва Павло Васильович, магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця, Хмельницьке шосе, 95

Л. А. Савицька, Т. И. Коробейникова, П. В. Чирва

МЕТОД ТА КРОСПЛАТФОРМЕНИЙ ЗАСІБ АРХІВАЦІЇ ОДНОТИПНИХ ФАЙЛІВ

Вінницький національний технічний університет, м. Вінниця

L.A. Savytska, T.I. Korobeinikova, P. V. Chyrva

METHOD AND CROSS-PLATFORM FILE ARCHIVING TOOL

Vinnytsia National Technical University, Vinnitsa

КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 621.316

О.Д. Азаров, Є.С. Генеральницький

ВИСОКОЛІНІЙНІ БАЛАНСНІ ДВОТАКТНІ ПІДСИЛЮВАЧІ ПОСТІЙНОГО СТРУМУ ІЗ НИЗКОЮ ПОХИБКОЮ ЗСУВУ НУЛЯ

Вінницький національний технічний університет, Вінниця

Анотація. Відомо, що двотактні підсилювачі постійного струму (ДППС), як правило мають високу лінійність передатної характеристики, широку смугу пропускання (сотні МГц та одиниці ГГц) на рівні одиничного підсилення та значну швидкість змінення вихідної наруги (не нижче тисяч вольт на мікросекунду). Серійні моделі таких інтегральних ДППС випускаються фірмами Analog Devices, Texas Instruments, Linear Technology, National Semiconductor та іншими. Завдяки наявності зазначених характеристик ДППС широко використовуються в перетворювачах струм-напруга, струм-струм, АЦП, ЦАП, системах прямого цифрового синтезу та багатоканальних цифрових системах опрацювання й реєстрування аналогових сигналів.

Незважаючи на високі вказані статичні й динамічні характеристики ДППС, побудовані на біполярних транзисторах, мають істотну адитивну похибку у вигляді вхідного струму зсуву нуля на рівні сотен нА й одиниць мкА. Часто - густо це може погіршити статичні параметри вказаних пристроїв і систем. При появі вхідного струму зсуву нуля $I_{СЗ.0}$ є базові струми біполярних транзисторів у вхідних каскадах підсилювачів. Для зменшення їх впливу в однотактних підсилювачах струму застосовують деякі спеціальні схемні методи. Які дозволяють на порядок зменшити вхідний струм зсуву нуля диференційного каскаду, не погіршуючи напругу зсуву або швидкодію.

Для зменшення вхідного струму зсуву нуля у ДППС було запропоновано застосовувати компенсацію базових струмів у вхідних каскадах, а також будувати вхідні каскади на складених транзисторах Шиклаї, що дасть змогу значно покращити точність роботи схеми загалом.

Ключові слова: Двотактний підсилювач постійного струму (ДППС), похибка лінійності передатної характеристики (ПЛПХ), струм зсуву нуля, відбивач струму, блок балансування підсилення струмів.

Аннотация. Известно, что двухтактные усилители постоянного тока (ДУПТ), как правило, имеют высокую линейность передаточной характеристики, широкую полосу пропускания (сотни МГц и единицы ГГц) на уровне единичного усиления и значительную скорость изменение выходного напряжения (не ниже тысяч вольт на микросекунду). Серийные модели таких интегральных ДУПТ выпускаются фирмами Analog Devices, Texas Instruments, Linear Technology, National Semiconductor и другими. Благодаря наличию указанных характеристик ДУПТ широко используются в преобразователях ток-напряжение, ток-ток, АЦП, ЦАП, системах прямого цифрового синтеза и многоканальных цифровых системах обработки и регистрации аналоговых сигналов.

Несмотря на высокие указаные статические и динамические характеристики ДУПТ, построенные на биполярных транзисторах, имеющих существенное аддитивную погрешность в виде входного тока смещения нуля на уровне сотен нА и единиц мкА. Часто это может ухудшить статические параметры указанных устройств и систем. При появлении входного тока смещения нуля IС3.0 есть базовые токи биполярных транзисторов во входных каскадах усилителей. Для уменьшения их влияния в однотактным усилителях тока применяют некоторые специальные схемные методы. Которые позволяют на порядок уменьшить входной ток смещения нуля дифференциального каскада, не ухудшая напряжение смещения или быстродействие.

Для уменьшения входного тока смещения нуля в ДППС было предложено применять компенсацию базовых токов во входных каскадах, а также строить входные каскады на составных транзисторах Шиклаи, что позволит значительно улучшить точность работы схемы в целом.

Ключевые слова: Двухтактный усилитель постоянного тока (ДУПТ), погрешность линейности передаточной характеристики (ПЛПХ), ток смещения нуля, отражатель тока, блок балансировки усиления токов.

Annotation. It is known that push-pull DC amplifiers (PPDA), as a rule, have a high linearity of the transfer characteristic, a wide passband (hundreds of MHz and GHz units) at the level of unity gain, and a significant rate of change in the output voltage (at least thousands of volts per microsecond). Serial models of such integrated PPDA are produced by Analog Devices, Texas Instruments, Linear Technology, National Semiconductor and others. Due to the presence of these characteristics, PPDA are widely used in current-voltage, current-current, ADC, DAC, direct digital synthesis systems and multi-channel digital systems for processing and recording analog signals.

Despite the high indicated static and dynamic characteristics of the PPDAs built on bipolar transistors, which have a significant additive error in the form of an input zero bias current of hundreds of nA and μA units. Often this can degrade the static parameters of these devices and systems. When the input zero bias current appears, there are basic currents of bipolar transistors in the input stages of the amplifiers. To reduce their influence in single-cycle current amplifiers, some special circuit methods are used. Which allow an order of magnitude to reduce the input zero bias current of the differential stage without affecting the bias voltage or speed.

To reduce the input zero bias current in the PPDA, it was proposed to apply basic current compensation in the input stages, as well as to build the input stages on Shiklai composite transistors, which will significantly improve the accuracy of the circuit as a whole.

Keywords: Two-stroke DC amplifier (PPDA), linearity error of the transfer characteristic (LETC), zero bias current, current reflector, current amplification balancing unit.

DOI: https://doi.org/10.31649/1999-9941-2020-47-1-22-31.

Вступ

Двотактні підсилювачі постійного струму (ДППС), як правило мають високу лінійність передатної характеристики, широку смугу пропускання (сотні МГц та одиниці ГГц) на рівні одиничного підсилення та значну швидкість змінення вихідної наруги (не нижче тисяч вольт на мікросекунду). Серійні моделі

таких інтегральних ДППС випускаються фірмами Analog Devices, Texas Instruments, Linear Technology, National Semiconductor та іншими [1, 2, 3, 4]. Завдяки наявності зазначених характеристик ДППС широко використовуються в перетворювачах струм-напруга, струм-струм, АЦП, ЦАП, системах прямого цифрового синтезу та багатоканальних цифрових системах опрацювання й реєстрування аналогових сигналів.

Актуальність

Незважаючи на високі вказані статичні й динамічні характеристики ДППС, побудовані на біполярних транзисторах, мають істотну адитивну похибку у вигляді вхідного струму зсуву нуля на рівні сотен нА й одиниць мкА. Часто - густо це може погіршити статичні параметри вказаних пристроїв і систем. При появі вхідного струму зсуву нуля $I_{С3.0}$ є базові струми біполярних транзисторів у вхідних каскадах підсилювачів. Для зменшення їх впливу в однотактних підсилювачах струму застосовують деякі спеціальні схемні методи [5]. Які дозволяють на порядок зменшити вхідний струм зсуву нуля диференційного каскаду, не погіршуючи напругу зсуву або швидкодію. Водночас використовування таких методів у ДППС є недоцільним ,оскільки вони ускладнюють схему і як правило збільшують вхідний опір, що в підсилювачах струму зменшує глибину зворотного зв'язку і дещо погіршує як статичні так і динамічні характеристики.

Автори пропонують для зменшення вхідного струму зсуву нуля у ДППС застосовувати компенсацію базових струмів у вхідних каскадах, а також будувати вхідні каскади на складених транзисторах Шиклаї. Проте вказані підходи є новими й оригінальними. Вони недостатньо розглянуті в науково технічній літературі, тому публікація цієї статті є актуальною

Мета досліджень-підвищення точності функціонування балансного двотактного підсилювача постійного струму за рахунок зменшення вхідного струму зсуву нуля.

Задачі досліджень:

запропонувати й проаналізувати два підходи щодо зменшення вхідного струму зсуву нуля $I_{ЗС.0}$:

а) шляхом автокомпенсації базових струмів транзисторів вхідного каскаду ДППС струмами протилежних напрямків, сформованими внутрішніми генераторами;

б) розглянути побудову вхідних каскадів на складених транзисторах Шиклаї;

скласти математичні моделі $I_{ЗС.0}$ для вказаних двох підходів;

здійснити комп'ютерне моделювання підсумкових значень $I_{ЗС.0}$, отриманих із застосуванням вказаних підходів;

порівняти отриманні результати й надати практичні рекомендації щодо застосування розглянутих ДППС у перетворювачах струм-напруга, струм – струм та інших.

Розв'язання задач досліджень

Вхідним сигналом підсилювача струму є струм, при чому у всіх каскадах схеми (за винятком вихідного) всі операції здійснюються саме над струмами. Це дає можливість схематично мінімізувати прирости напруг на паразитних ємностях і досягти високої швидкодії, зокрема, широкої смуги пропускання на рівні одиничного підсилення. Побудова підсилювача за двотактною структурою дозволяє до того ж забезпечити максимальну лінійність передатної характеристики. Функціональну схему ДППС зображень на рисунку 1.

Вона містить: вхідний двотактний каскад (Вх. ДК), $I_{Р1}$, $I_{Р2}$ - генератори робочих струмів, відбивачі струму (ВС1, ВС2), блок балансування - підсилення струмів (ББПС), відбивачі струму (ВС3, ВС4), а також вихідний каскад (Вих. ДК).

Схема реалізує режим перетворення струм-напруга у вигляді $U_{ВИХ}=I_{ВХ}\cdot R_М$, де: $I_{ВХ}$ - вхідний струм; $R_М$ - масштабний резистор, який задає діапазон змінення вихідної напруги; $R_Н$ - резистор навантаження; $I_Н$ - струм навантаження ; $I_{ЗЗ}$ - струм зворотнього зв'язку.

Працює ДППС таким чином. Вхідний струм $I_{ВХ}$ розщіплюється на складові I', $\overline{I'}$ та I'', $\overline{I''}$. Далі I' і I'', що крім робочих містять і сигнальні складові $\Delta I'$ і $\Delta I''$ через відбивачі ВС1 і ВС2 подаються на робочі входи ББПС.

На сигнальні входи цього блока поступають також інверсні струми $\overline{I'}$ і $\overline{I''}$. Із виходів ББПС підсилені і збалансовані струми складові $I'_{БЛ}$, $\overline{I'}_{БЛ}$ та $I''_{БЛ}$, $\overline{I''}_{БЛ}$ подаються на прямі й інверсні входи ВС3 і ВС4. Вихідні струми цих відбивачів далі поступають на входи Вих. ДК, підсилюються і формують складові $I_{ВИХ}$, як розчіплюються на $I_{ЗЗ}$ і протікає в контур зворотнього зв'язку ,а також на $I_Н$, що подається на опір навантаження $R_Н$.

Розглянемо окремо вхідні каскади ДППС, оскільки саме від них залежить значення $I_{ЗС.0}$. На рисунку 2 наведено схеми Вх. ДК зі зменшеним $I_{ЗС.0}$. Причому, перший підхід, що реалізує автокомпенсацію базових струмів n-p-n і p-n-p транзисторів продемонстровано на рисунку 2а).

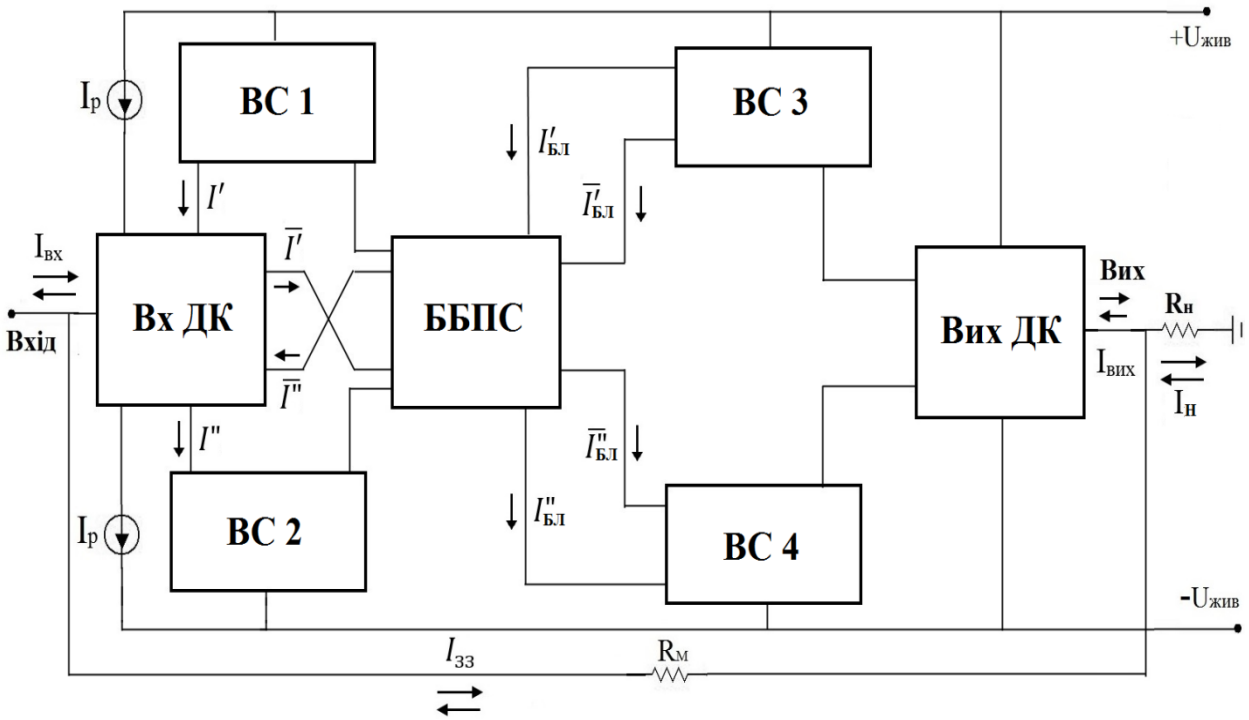

Рисунок 1. Функціональна схема двотактного балансного підсилювача постійного струму

Цю схему побудовано у вигляді двотактної комплементарної структури відбивачів струму Вілсона, відповідно на транзисторах Т1-Т4, транзисторах регуляторах Т11,Т16, транзисторах давачах Т12, Т15. Саме остання пара підсилює вхідний струм $I_{ВХ}$ і формує вхідний різницевий базовий струм, а саме $\Delta I_Б = I_{БР} \cdot I_{БП}$.

Для заданого рівня $I_Р$ маємо:

$$\Delta I_Б = I_P \cdot \left(\frac{1}{\beta_{p-n-p}} - \frac{1}{\beta_{n-p-n}}\right),$$

де β_{p-n-p} і β_{n-p-n} - базовий струми, відповідно, p-n-p і n-p-n транзисторів.

У випадку застосування інтегральних малопотужних транзисторів типу npn — NUHFARRY, pnp — PUHFARRY при $I_Р$ = 1мА маємо $\beta_{p-n-p} \approx 60$, $\beta_{n-p-n} \approx 100$. Таким чином $\Delta I_Б \approx 40$мкА, що дає істотну похибку зсуву нуля. $I_{ЗС.0}$ може бути зменшено шляхом його компенсації, якщо згенерувати струм $\Delta I_{БК}$ близький за значенням $\Delta I_Б$, але протилежного напрямку і підключити його до входу ДППС. Для цього колектори транзисторів Т2 і Т3 підключено до емітерів Т5 і Т6. При цьому базові струми цих транзисторів мають значення близькі до базових струмів Т13 і Т14.

Оскільки бази Т5 і Т6 під'єднано до відбивачів струму на транзисторах Т7, Т9 і Т8, Т10, відповідно, то різниця $\Delta I_К = I_{К9} - I_{К10} \approx I_{Б13} - I_{14}$. Точність цієї рівності істотно залежить від припасування параметрів інтегральних транзисторів в інтегральній схемі [6]. Орієнтуючись на дані наведені в [7, 8, 9] можна стверджувати, що $I_{ЗС.0}$ буде зменшено, як мінімум у 20 разів. Треба також додати, що робочі точки Т2, Т3 і Т13, Т14 особливо по колекторному струму повинні бути максимально наближенні, що забезпечується конфігурацією ДППС. Комп’ютерне моделювання характеристик цього вхідного каскаду за допомогою інтегрованого пакету Micro-CAP 12 показало, що вхідний струм зсуву нуля за умов компенсації дорівнює $I_{ЗС.0}$=111.6нА.

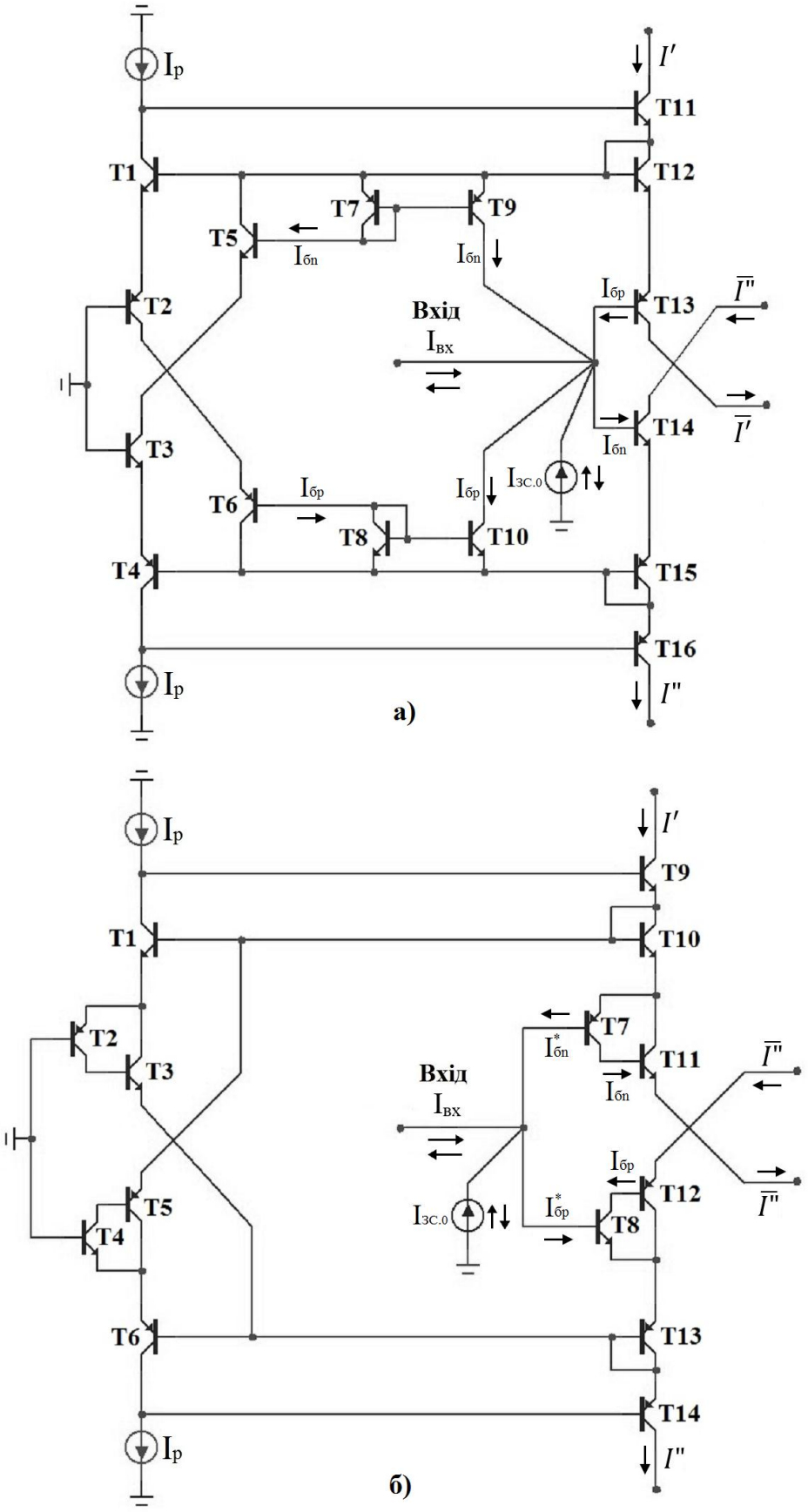

Рисунок 2 - Вхідні каскади ДППС із низькими струмами $I_{ЗС.0}$: а) на генераторах компенсуючих струмів; б) на складених транзисторах Шиклаї.

Оцінимо вхідний малосигнальний опір схеми $R_{ВХ}$ Вх. ДК. Якщо компенсацію відключено ,то $R_{ВХ}$ дорівнює паралельному з'єднанню вхідних опорів Т13 і Т14. $R_{вх} = R_{вх}(\text{T13}) \| R_{вх}(\text{T14})$, Відомо, що для інтегральної зарядової моделі Гумеля - Пуна вхідний опір гібридної схеми загальний емітер дорівнює [4]:

$$R_{вх.\text{зе}} = R_б + \beta R_e + R_e(1+\beta),$$

де: $R_Б$, $R_Е$ - малосигнальні опори бази й емітера; β – коефіцієнт передачі струму; $R_Е$ - опір зовнішнього емітерного резистора. Слід зазначити, що в ролі емітерного навантаження виступають діоди на базі транзисторів Т12 і Т15. Опір цих діодів дорівнює:

$$R_Д = \frac{\varphi_T}{I_Д},$$

де φ_T - термопотенціал, $I_Д$ - струм через діод. Таким чином для n-p-n і p-n-p транзистора маємо:

$$R_{вх.\text{n–p–n}} = R_{б\ n-p-n} + \beta_{n-p-n} \cdot R_e + R_Д(1+\beta_{n-p-n}),$$

$$R_{вх.\text{p–n–p}} = R_{б\ p-n-p} + \beta_{p-n-p} \cdot R_e + R_Д(1+\beta_{p-n-p}),$$

За умови об'єднання баз Т13 іТ14 вхідний опір дорівнює:

$$R_{вх} = \frac{\left[R_{б\ n-p-n} + \beta_{n-p-n} \cdot R_e + R_Д(1+\beta_{n-p-n})\right] \cdot \left[R_{б\ p-n-p} + \beta_{p-n-p} \cdot R_e + R_Д(1+\beta_{p-n-p})\right]}{R_{б\ n-p-n} + \beta_{n-p-n} \cdot R_e + R_Д(1+\beta_{n-p-n}) + R_{б\ p-n-p} + \beta_{p-n-p} \cdot R_e + R_Д(1+\beta_{p-n-p})},$$

Беручи до уваги що $R_Е \approx R_Д$, а $\beta \approx (1+\beta)$ остаточно маємо:

$$R_{вх} = \frac{(R_{б\ n-p-n} + 2R_e \cdot \beta_{n-p-n}) \cdot (R_{б\ p-n-p} + 2R_e \cdot \beta_{p-n-p})}{R_{б\ n-p-n} + R_{б\ p-n-p} + 2R_e \cdot (\beta_{p-n-p} + \beta_{n-p-n})} \quad (1)$$

Для транзисторів, що використовуються у схемі при $I_Р$ = 1мА маємо $R_{б\ n-p-n}$= 35 Ом, $R_{б\ p-n-p}$ = 37 Ом, $\beta_{n-p-n} = 127$, β_{p-n-p} =63.

Підставляючи ці значення в (1) маємо $R_{ВХ}$=2251Ом, ккомп'ютерне моделювання дає $R_{ВХ}$=2273Ом то результати збігаються з похибкою не більше 1%.

Підключення генераторів компенсуючих струмів до входу схеми значення вхідного опору $R_{ВХ}$ змінює на досить мале значення, яким можна знехтувати.

Подальше зменшення $I_{ЗС.0}$ можна досягти, якщо побудувати вхідний каскад ДППС на складених транзисторах Шиклаї, як це показано на рисунку 2б). При цьому симетруючі транзистори Т2 - Т5 і вхідні транзистори Т7, Т11 і Т8, Т12 являють собою комбінації n-p-n і p-n-p транзисторів. Оцінимо значення $I_{ЗС.0}$ для цієї схеми. Відзначимо, що робочі струми, які протікають через діоди, побудовані на транзисторах Т10 і Т13 дорівнюють $I_Р$. Тому маємо:

$$I_{К11} \approx I_Р, \quad I_{Б11} = I_{К7} = \frac{I_p}{\beta_{11}}, \quad a \quad I_{Б7} = \frac{I_p}{\beta_{11} \cdot \beta_7}$$

Аналогічно отримаємо:

$$I_{К12} \approx I_Р, \quad I_{Б12} = I_{К8} = \frac{I_p}{\beta_{12}}, \quad a \quad I_{Б8} = \frac{I_p}{\beta_{12} \cdot \beta_8}$$

Таким чином $I_{ЗС.0}$ дорівнює різниці базових струмів Т7 і Т8, тобто

$$I_{ЗС.0} = I_{Б7} - I_{Б8} = I_p \cdot \left(\frac{1}{\beta_{11} \cdot \beta_7} - \frac{1}{\beta_{12} \cdot \beta_8}\right) = I_p \cdot \frac{\beta_{12} \cdot \beta_8 - \beta_{11} \cdot \beta_7}{\beta_{11} \cdot \beta_7 \cdot \beta_{12} \cdot \beta_8} \quad (2)$$

Теоретично $I_{ЗС.0}$ на основі рівності (2) може наближатися до нуля. На практиці це значення визначається технологічними похибками припасування значень β пар n-p-n і p-n-p транзисторів. Комп'ютерне моделювання надає результат $I_{ЗС.0} \approx 1.92$ нА.

Водночас для першої схеми $I_{ЗС.0} \approx 111.6$ нА. Таким чином рівень $I_{ЗС.0}$ для другого варіанта вхідного каскада струм зсуву є на порядок меншим.

Визначимо вхідний опір $R_{ВХ}$ для другої схеми Вх. ДК. Для цього скористуємося виразом (1) із [4].

$$R_{BX} = R_Б + \beta \cdot R_E + R_E(1+\beta),$$

при цьому в ролі RE у цьому випадку будуть виступати вхідні опори Т11 і Т12. Так зі входу схеми з боку бази маємо:

$$R_{BX7} = R_{б\ n-p-n} + \beta_{n-p-n} \cdot R_E + R_{BX11} \cdot (1+\beta_{n-p-n}) \approx R_{BX11} \cdot (1+\beta_{n-p-n}),$$

Підставляючи в останній вираз RBX11 і спрощуючи, маємо:

$$R_{BX7} = \left[R_{б\ n-p-n} + \beta_{n-p-n} \cdot R_E + R_Д \cdot (1+\beta_{n-p-n})\right] \cdot (1+\beta_{n-p-n})$$

$$\approx 2 \cdot R_E \cdot \beta_{n-p-n} \cdot (1+\beta_{n-p-n}) \approx 2 \cdot R_E \cdot \beta^2_{n-p-n}.$$

Аналогічно для Т8 отримаємо:

$$R_{BX7} = 2 \cdot R_E \cdot \beta^2_{p-n-p}$$

Таким чином загальний вхідний опір має значення:

$$R^*_{BX} = R_{BX7} \| R_{BX8} = \frac{2 \cdot R_E \cdot \beta^2_{n-p-n} \cdot \beta^2_{p-n-p}}{\beta^2_{n-p-n} + \beta^2_{p-n-p}} \quad (3)$$

Підставляючи у (3) значення RE, βp-n-p, βn-p-n, маємо $R^*_{BX} \approx 211 кОм.$ У результаті комп'ютерного моделювання отримаємо $R^*_{BX} \approx 212 кОм.$

Отже вхідний опір R^*_{BX} другої схеми вхідного каскаду є набагато більшим ніж $R_{ВХ}$ першої схеми.

Для оцінювання значень коефіцієнта передачі струму, а також похибок лінійності потрібно розглянути підсилювачі у цілому. Варіант схеми ДППС із компенсацією $I_{ЗС.0}$ зображено на рисунку 3. Вона крім вхідного двотактного каскаду містить ВС1 і ВС2 на транзисторах Т17-Т19 і Т20, Т23, Т24 відповідно; блок балансування підсилення струмів (ББПС) на транзисторах Т21, Т22 і Т25-Т28; вихідний двотактний каскад Вих. ДК із відбивачами струмів на транзисторах Т29, Т31, Т33, Т34 і Т30, Т32, Т37, Т38 та безпосередньо вихідний каскад на транзисторах Т35, Т36 і Т39, Т40.

Визначимо малосигнальний коефіцієнт передачі струму при розірваній петлі зворотного зв'язку (відключено резистор масштабу RM) в режимі балансу, тобто коли вихідний струм $I_Н$, що протікає через опір навантаження RH, зведено до мінімуму шляхом компенсації $I_{ЗС.0}$.

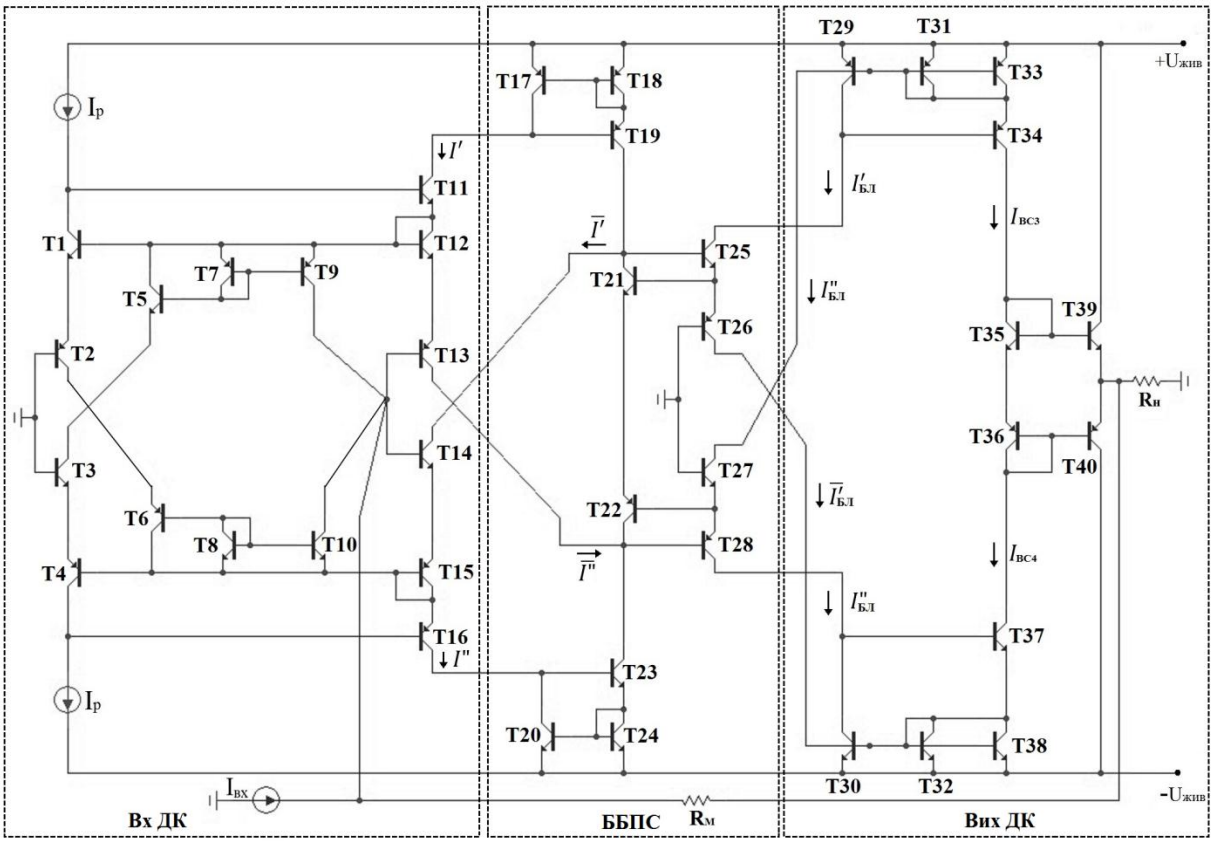

Рисунок 3. Схема ДППС із компенсацією зсуву нуля $I_{ЗС.0}$:

Використовуючи аналітичні вирази, наведені в [5] нескладно довести, що:

$$\left|\frac{I^{'}}{I_{BX}}\right| \approx \left|\frac{I^{''}}{I_{BX}}\right| \approx \left|\frac{\overline{I^{'}}}{I_{BX}}\right| \approx \left|\frac{\overline{I^{''}}}{I_{BX}}\right| = \frac{\beta_n \cdot \beta_p}{\beta_n + \beta_p} \quad ,$$

де β_n, β_P - малосигнальні коефіцієнти підсилення струму n-n-n і p-n-n транзисторів відповідно. На входах ББПС ці струми підсумовуються і на його виходах маємо:

$$\left|\frac{I^{'}_{БЛ}}{I_{BX}}\right| \approx \left|\frac{I^{''}_{БЛ}}{I_{BX}}\right| \approx \left|\frac{\overline{I^{'}_{БЛ}}}{I_{BX}}\right| \approx \left|\frac{\overline{I^{''}_{БЛ}}}{I_{BX}}\right| = \left(\frac{\beta_n \cdot \beta_p}{\beta_n + \beta_p}\right)^2 .$$

На прямих й інверсних входах відбивачів струмів ВС3 і ВС4 ці складові алгебраїчно підсумовуються, забезпечуючи коефіцієнт передачі Кі ВС ≈ 2,5 тому:

$$\left|\frac{I_{BC3}}{I_{BX}}\right| = \left|\frac{I_{BC4}}{I_{BX}}\right| = 2{,}5 \cdot \left(\frac{\beta_n \cdot \beta_p}{\beta_n + \beta_p}\right)^2 .$$

Оскільки схема ДППС має двотактну структуру, то на входах вихідного каскаду струми $I_{ВС3}$ і $I_{ВС}$ складаються, подвоюючи підсумковий коефіцієнт підсилення. З урахуванням коефіцієнта передачі Вих. ДК, остаточно маємо:

$$K_i = 5 \cdot \left(\frac{\beta_n \cdot \beta_p}{\beta_n + \beta_p}\right)^3 . \qquad (4)$$

Підставляючи в (4) значення βn і βP отримаємо $K_i \approx 2.56 \cdot 10^6$. На рисунку 4 зображені АЧХ і ФЧХ ДППС із двома типами Вх. ДК, отриманні шляхом комп'ютерного моделювання. У випадку за-

стосування першої схеми (графік 1) Вх. ДК маємо $K_i \approx 2.56 \cdot 10^6$ на низьких частотах, а смугу пропускання на рівні 0дБ – 1000МГц. Таким чином результати визначення коефіцієнтів підсилення за допомогою (4) і комп'ютерним моделюванням практично збігаються.

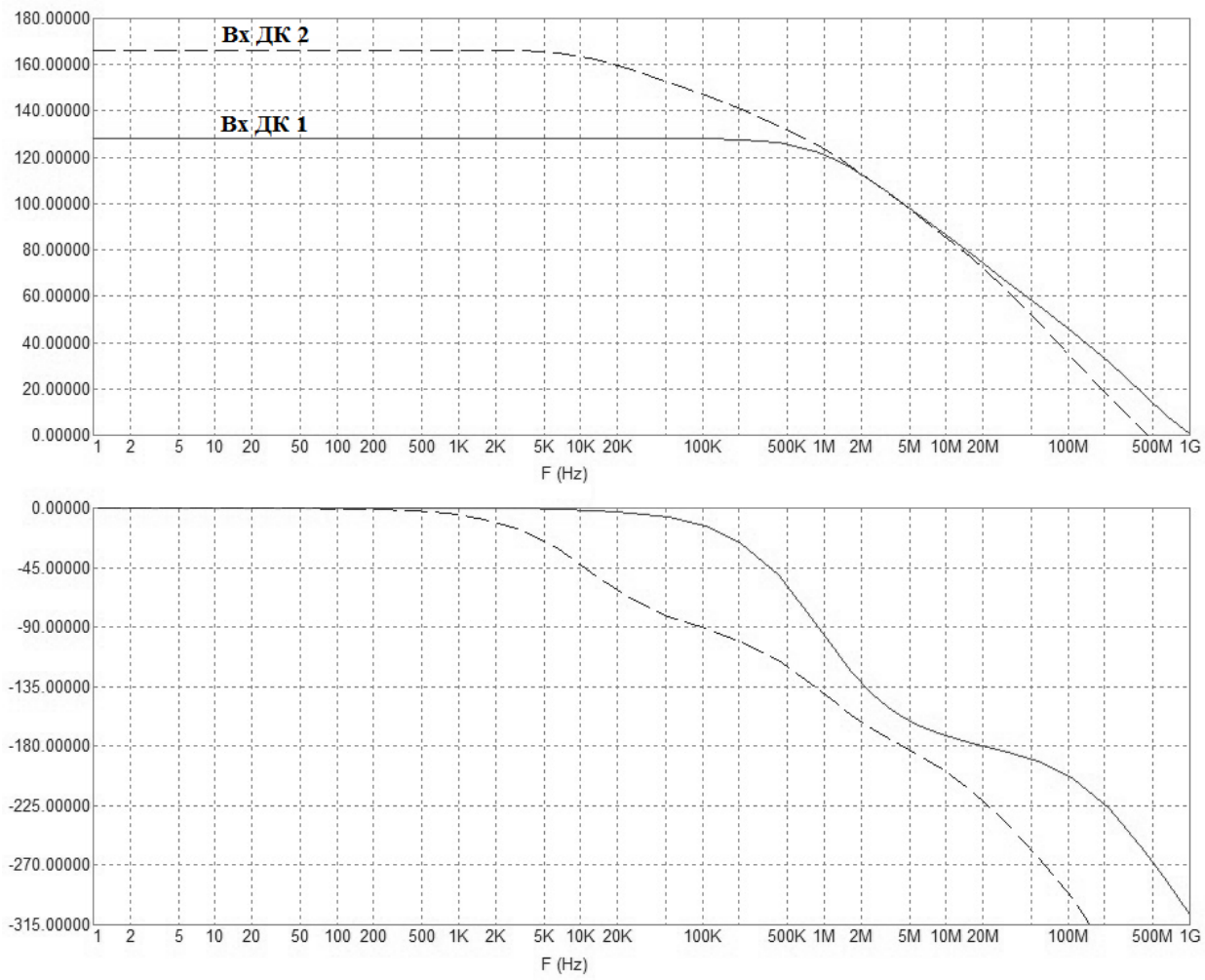

Рисунок 4. Графіки АЧХ і ФЧХ ДППС із Вх ДК першого і другого типів

Застосування Вх. ДК другого типу дає більший коефіцієнт підсилення за рахунок побудови каскаду на складених транзисторах Шиклаї. Реалізуючи процедури подібні для Вх. ДК першого типу, неважко показати, що у випадку використання вхідного каскаду другого типу отримаємо вираз:

$$K_i = 5 \cdot \left(2 \cdot \frac{\beta_n \cdot \beta_p}{\beta_n + \beta_p} \right)^4 . \qquad (5)$$

Підставляючи в (5) βn і βP маємо $K_i \approx 2.56 \cdot 10^6$. Орієнтуючись на графік 2, одержуємо $K_i \approx 208 \cdot 10^6$. Вказані значення Кі і RBX ДППС треба використовувати у практичних рекомендаціях під час проектування перетворювачів струм - напруга або напруга - напруга. При цьому слід зазначити, що похибки лінійності таких перетворювачів істотно залежать, як відзначень Кі при розірваній петлі зворотнього зв'язку, так і від глибини цього зв'язку. У свою чергу глибина ЗЗ визначається співвідношенням R_M і R_{BX}. Чим більше це співвідношення, тим більша частина вихідного сигналу (струму) повертається на вхід ДППС, тому бажано, щоб на практиці виконувалася умова $R_M \geq R_{BX}$ або принаймні, щоб R_M було співвимірним із R_{BX}. Похибка лінійності $\Delta I_Л$ у значній мірі також залежить від діапазону змінення $R_{ВИХ}$, що протікає, через навантаження.

Досліджувати $\Delta I_Л$ доцільно шляхом комп'ютерного моделювання у вигляді функції: $\Delta I_Л = f(K_{ПІ})$ при заданому $I_Н$, де $K_{ПІ} = \frac{R_M}{R_H}$.

Множину абсолютних значень $\Delta I_Л$ і відносних $\delta I_Л$ значень похибок лінійності при $R_Н$ = 1 кОм для Вх. ДК першого типу наведено в таблиці 1, а для Вх. ДК другого типу наведено в таблиці 2.

Таблиця 1

$K_{ПІ}$	2	5	10	20	50	100
$\Delta I_Л$ (нА)	0.006	0.044	0.235	1.5	18.5	91
$\delta I_Л$ (%)	$6 \cdot 10^{-5}$	$44 \cdot 10^{-5}$	$0.235 \cdot 10^{-4}$	$1.5 \cdot 10^{-4}$	$18.5 \cdot 10^{-4}$	$91 \cdot 10^{-4}$

Таблиця 2

$K_{ПІ}$	2	5	10	20	50	100
$\Delta I_Л$ (нА)	0.0029	0.013	0.046	0.171	1.02	2.97
$\delta I_Л$ (%)	$2.9 \cdot 10^{-5}$	$13 \cdot 10^{-5}$	$46 \cdot 10^{-5}$	$0.17 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$2.9 \cdot 10^{-4}$

Отриманні результати свідчать, що похибки лінійності у другій схемі є нижче, ніж у першій у 2-10 разів і навіть більше залежно від $K_{ПІ}$. Разом із тим в обох випадках розглянуті схеми ДППС можна використовувати в багаторозрядних високолінійних ЦАП і АЦП із роздільною здатністю 20 і більше двійкових розрядів.

Висновки

1. Запропоновано й проаналізовано два підходи зменшення вхідного струму зсуву нуля у ДППС на біполярних транзисторах, а саме:

а) шляхом компенсації базових струмів вхідного каскаду струмами протилежних напрямків, сформованих внутрішніми генераторами;

б) побудовою вхідних каскадах на складених транзисторах Шиклаї.

2. Отримано аналітичні співвідношення для оцінювання рівня $I_{ЗС.0}$ для розглянутих двох схем вхідних каскадів ДППС. Доведено, що у другій схемі значення струму зсуву нуля є істотно нижче 2-10 разів і навіть більше залежно від $K_{ПІ}$.

3. Шляхом комп'ютерного моделювання доведено, що коефіцієнт передачі струму є більшим (принаймні у 6 разів) у другій схемі, а похибка лінійності істотно меншою.

4. Надано практичні рекомендації щодо застосування розглянутих ДППС у високолінійних перетворювачах струм – струм, струм - напруга із низьким струмом зсуву нуля.

Список використаної літератури

[1] О.Д. Азаров, та С.В. Богомолов, «Основи теорії високолінійних аналогових пристроїв на базі двотактних підсилювальних схем» : монографія /.УНІВЕРСУМ-Вінниця, 2013.- 142 с.

[2] О. Д. Азаров, М. Ю. Теплицький, та В. А. Гарнага, «Двотактні підсилювачі постійного струму на базі двонаправлених відбивачів струму» Проблеми інформатизації та управління, № 2 (34), с. 15-22, 2011.

[3] О. Д. Азаров, М. Ю. Теплицький, та Н. О. Біліченко, «Швидкодійні двотактні підсилювачі постійного струму з балансним зворотним зв'язком»,. Вінниця, Україна,ВНТУ, 2016, 136 с.

[4] О.Д. Азаров, та В.А. Гарнага, «Двотактні підсилювачі постійного струму для багаторозрядних перетворювачів форми інформації, що самокалібруються», Вінниця, Україна УНІВЕРСУМ - Вінниця, 2011, 156 с.

[5] Дж. Коннели «Аналоговые интегральные схемы» Ред. Москва: изд-во «Мир» 1977.- 107-112 с

[6] И. П. Степаненко, «Основы теории транзисторов и транзисторных схем», изд. 4-е, перераб. и доп. Москва: Энергия, 1977

[7] А. Б. Гребен, Проектирование аналоговых интегральных схем. Москва: Энергия, 1976, 256с.

[8] Г. В. Зевеке, П. А. Ионкин, А. В. Нетушил, и С. В. Страхов, «Основы теории цепей» Москва: Энергия, 1975. 752 с

[9] Дж. Грэм, Дж. Тоби, и Л. Хьюлсман «Проектирование и применение операционных усилителей,» В. Л. Левин, и И. М. Хейфец, пер. с англ., И. Н. Теплюк, Ред. Москва: изд-во «Мир». Редакция литературы по новой технике, 1974.

Стаття надійшла: 24.03.2020.

References

[1] O.D. Azarov, ta S.V. Bohomolov, «Osnovy teorii vysokoliniinykh analohovykh prystroiv na bazi dvotaktnykh pidsyliuvalnykh skhem» : monohrafiia /.UNIVERSUM-Vinnytsia, 2013.- 142 s.

[2] O. D. Azarov, M. Y. Teplytskyi, ta V. A. Harnaha, «Dvotaktni pidsyliuvachi postiinoho strumu na bazi dvonapravlenykh vidbyvachiv strumu» Problemy informatyzatsii ta upravlinnia, № 2 (34), s. 15-22, 2011.

[3] O. D. Azarov, M. Y. Teplytskyi, ta N. O. Bilichenko, «Shvydkodiini dvotaktni pidsyliuvachi postiinoho strumu z balansnym zvorotnym zviazkom»,. Vinnytsia, Ukraina,VNTU, 2016, 136 s.

[4] O.D. Azarov, ta V.A. Harnaha, «Dvotaktni pidsyliuvachi postiinoho strumu dlia bahatorozriadnykh peret-voriuvachiv formy informatsii, shcho samokalibruiutsia», Vinnytsia, Ukraina UNIVERSUM - Vinnytsia, 2011, 156 s.

[5] Dzh. Konneli «Analogovye integralnye skhemy» Red. Moskva: izd-vo «Mir» 1977. 107-112 s.

[6] I. P. Stepanenko, «Osnovy teorii tranzistorov i tranzistornykh skhem», izd. 4-ye, pererab. i dop. Moskva: Energiya, 1977

[7] A. B. Greben «Proektirovanie analogovykh integralnykh skhem». Moskva: Energiia, 1976, 256s.

[8] G. V. Zeveke, P. A. Ionkin, A. V. Netushil, i S. V. Strakhov, «Osnovy teorii tsepey». Moskva: Energiya, 1975. 752 s

[9] Dzh. Grem, Dzh. Tobi, i L. KH'yulsman «Proyektirovaniye i primeneniye operatsionnykh usiliteley,» V. L. Levin, i I. M. Kheyfets, per. s angl., I. N. Teplyuk, Red. Moskva: izd-vo «Mir». Redaktsiya literatury po novoy tekhnike, 1974.

Відомості про авторів

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

Генеральницький Євгеній Сергійович — аспірант кафедри обчислювальної техніки.

А. Д. Азаров, Е. С. Генеральницкий

ВЫСОКОЛИНЕЙНЫЙ БАЛАНСНЫЙ ДВУХТАКТНЫЙ УСИЛИТЕЛЬ ПОСТОЯННОГО ТОКА С НИЗКОЙ ПОГРЕШНОСТЬЮ СМЕЩЕНИЯ НУЛЯ

Винницкий национальный технический университет, Винница

O.D. Azarov, Y.S. Heneralnytskyi

HIGH LINEARITY BALANCED PUSH-PULL DC AMPLIFIER WITH LOW ERROR OF ZERO OFFSET

Vinnytsia National Technical University, Vinnytsia

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 004.624

В. В. Войтко, С. В. Бевз, С. М. Бурбело, П. В. Ставицький

МОДЕЛІ СИСТЕМИ АНАЛІЗУ ТА РОЗПІЗНАВАННЯ МУЗИЧНИХ КОМПОЗИЦІЙ

Вінницький національний технічний університет, Вінниця

Анотація. У статті розглядаються моделі системи розпізнавання музичних композицій у системі синтезу та аналізу музичних звуків, спрямовані на підвищення ідентифікаційних можливостей автоматизованої системи. Модуль розпізнавання музичних композицій орієнтований на серверну частину системи, яка, незалежно від клієнта, містить базу даних з відбитками музичних композицій. За допомогою алгоритмів розпізнавання мелодій за заданим аргументом у вигляді відбитку сервер повертає список музичних композицій, які найбільше задовольняють умовам пошуку. Клієнтська частина взаємодіє з серверною за допомогою розробленого прикладного програмного інтерфейсу, який, крім відомого функціоналу підходу до архітектури мережевих протоколів REST, що базується на протоколі HTTP, де клієнт використовує запити лише в форматі, визначеному специфікацією серверної частини, також передбачає реалізацію можливостей підходу до архітектури мережевої взаємодії з використанням мови запитів GraphQL, що дозволяє будувати параметри запиту зі сторони клієнта. Локальна база даних містить набір відбитків та метаданих про музичні композиції для прискорення процесу розпізнавання, оскільки дозволяє покрити більшість сценаріїв використання додатку з найпопулярнішими музичними композиціями з можливістю швидкого повернення результату після локального співставлення даних без необхідності затримок клієнт-серверної взаємодії. Модуль синхронізації бази даних відповідає за своєчасне оновлення локальної бази новими відбитками з серверної частини та за загальну синхронізацію клієнтської і серверної частин системи. Планувальник синхронізації забезпечує формування розкладу синхронізації локальної та серверної баз даних, а також реалізує стратегії оптимізації використання акумулятора та забезпечує роботу з низьким рівнем інтернет-з'єднання. Розглянуто особливості зберігання бази відбитків композицій та стратегії роботи з пристроями на базі мобільних платформ, зокрема, під операційну систему Android з використанням режиму Doze, який забороняє фонову роботу пристрою у стані спокою, окрім коротких проміжків часу, так званих вікон підтримки, які визначаються операційною системою в процесі роботи та дозволяють виконувати короткочасні фонові операції. Проведено оптимізацію процесу використання енергії акумулятора мобільного пристрою при синхронізації метаданих музичних композицій між клієнтською та серверною складовими системи.

Ключові слова: мобільний додаток, розпізнавання музики, клієнт-серверна система, зберігання даних.

Аннотация. В статье рассматриваются модели системы распознавания музыкальных композиций в системе синтеза и анализа музыкальных звуков, направленные на повышение идентификационных возможностей автоматизированной системы. Модуль распознавания музыкальных композиций ориентирован на серверную часть системы, которая, независимо от клиента, содержит базу данных с отпечатками музыкальных композиций. С помощью алгоритмов распознавания мелодий с заданным аргументом в виде отпечатка сервер возвращает список музыкальных композиций, наиболее удовлетворяющих условиям поиска. Клиентская часть взаимодействует с серверной с помощью разработанного прикладного программного интерфейса, который, кроме известного функционала подхода к архитектуре сетевых протоколов REST, основанном на протоколе HTTP, где клиент использует запросы только в формате, определенном спецификацией серверной части, также предусматривает реализацию возможностей подхода к архитектуре сетевого взаимодействия с использованием языка запросов GraphQL, что позволяет строить параметры запроса со стороны клиента. Локальная база данных содержит набор отпечатков и метаданных о музыкальных композициях для ускорения процесса распознавания, поскольку позволяет покрыть большинство сценариев использования приложения с самыми популярными музыкальными композициями с возможностью быстрого возврата результата после локального сопоставления данных без необходимости задержек клиент-серверного взаимодействия. Модуль синхронизации базы данных отвечает за своевременное обновление локальной базы новыми отпечатками с серверной части и за общую синхронизацию клиентской и серверной частей системы. Планировщик синхронизации обеспечивает формирование расписания синхронизации локальной и серверной баз данных, а также реализует стратегии оптимизации использования аккумулятора и обеспечивает работу с низким уровнем интернет-соединения. Рассмотрены особенности хранения базы отпечатков композиций и стратегии работы с устройствами на базе мобильных платформ, в частности, под операционную систему Android в режиме Doze, запрещающем фоновую работу устройства в состоянии покоя, кроме коротких промежутков времени, так называемых окон поддержки, которые определяются операционной системой в процессе работы и позволяют выполнять кратковременные фоновые операции. Проведена оптимизация процесса использования энергии аккумулятора мобильного устройства при синхронизации метаданных музыкальных композиций между клиентской и серверной составляющими системы.

Ключевые слова: мобильное приложение, распознавание музыки, клиент-серверная система, хранение данных.

Abstract. The article discusses the models of the recognition system for musical compositions in the system of synthesis and analysis of musical sounds, aimed at increasing the identification capabilities of an automated system. The recognition module for musical compositions is oriented to the server part of the system, which, regardless of the client, contains a database with fingerprints of musical compositions. With the help of melody recognition algorithms with a given argument in the form of a fingerprint, the server returns a list of musical compositions that most satisfy the search conditions. The client part interacts with the server part using the developed application programming interface, which, in addition to the well-known functional approach to the REST network protocol architecture based on the HTTP protocol, where the client uses requests only in the format defined by the server part specification, also provides for the implementation of the capabilities of the network architecture approach interactions using the GraphQL query language, which allows to build query parameters on the client side. The local database contains a set of fingerprints and metadata about musical compositions to speed up the recognition process, since it allows to cover most application scenarios with the most popular musical compositions with the ability to quickly return results after local data matching without the need for client-server interaction delays. The database synchronization module is responsible for the timely updating of the local database with new fingerprints from the server side and for the general synchronization of the client and server parts of the system. The synchronization scheduler provides a synchronization schedule for the local and server databases, as well as implements strategies for optimizing battery usage and ensures work with a low level of Internet connection. The features of storing the fingerprint database of compositions and strategies for working with devices based on mobile platforms, in particular, for the Android operating system in Doze mode, which prohibits the background operation of the device at rest, except for short periods of time, the so-called support windows, which are determined by the operating system work process and allow to perform short-term background operations. Performed the optimi-

zation of the process of using the battery energy of a mobile device while synchronizing the metadata of musical compositions between the client and server components of the system.
Keywords: mobile application, music recognition, client-server system, data persistence.
DOI: https://doi.org/10.31649/1999-9941-2020-47-1-32-38.

Вступ

Мобільні пристрої швидко набувають популярності і поширення серед пересічних користувачів, а тому можуть слугувати інструментом для розв'язання великої кількості повсякденних задач. Більше того, такі пристрої не є прив'язаними до конкретної фізичної локації, тому додатки на базі їхніх платформ мають широкий спектр сценаріїв застосування. Одним з таких сценаріїв є функціонал обробки аудіо контенту, синтезу та розпізнавання музичних композицій [1-2].

З іншого боку ключовою особливістю професійного програмного забезпечення на базі мобільних платформ є обмеженість ресурсів мобільних пристроїв у порівнянні з настільними або веб-рішеннями. Зокрема, енергія акумулятора є вичерпною і потребує додаткових стратегій економії, об'єм оперативної та фізичної пам'яті є досить обмеженим [2-3]. Крім того, зв'язок клієнтських мобільних додатків з серверною частиною є не завжди можливим, а його якість не є ідеальною і залежить від сили сигналу стільникового зв'язку. Враховуючи наведені особливості функціонування програмного забезпечення на базі мобільних платформ, необхідним є використання додаткових стратегій та алгоритмів для оптимізації розроблюваної системи синтезу та аналізу музичних звуків.

Актуальність теми

Автоматизація процесу обробки аудіо контенту набуває популярності в процесі розвитку і поширення як професійних, так і любительських мобільних програм, орієнтованих на розпізнавання музичних композицій та синтез звукових сигналів у процесі створення власних мелодій. Це обумовлює актуальність розробки та дослідження сучасних засобів обробки аудіо сигналів з використанням мобільних платформ та технологій у процесі аналізу й розпізнавання аудіо контенту, що, в свою чергу, відкриває новий спектр сценаріїв використання розроблюваної системи.

Мета

Метою дослідження є підвищення ідентифікаційних можливостей процесу аналізу музичних звуків з використанням сучасних програмних технологій, які, в тому числі, базуються на мобільних платформах, що дозволяє автоматизувати процес обробки аудіо контенту.

Задачі

1. Провести аналіз сучасних технологій і підходів у реалізації швидкої синхронізації клієнтської складової мобільної системи з серверною.
2. Розробити структуру та архітектуру процесу розпізнавання музичних звуків та модель взаємодії клієнтської та серверної складових.
3. Проаналізувати особливості використання мобільних платформ, зокрема, оптимізацію ресурсів для ефективного енергозбереження, а також обмеженість об'єму доступної пам'яті.
4. Дослідити процес і послідовність розпізнавання музичних композицій.

Розробка моделей автоматизованої системи розпізнавання музичних композицій

Однією з базових компонентів розроблюваної системи обробки аудіо контенту є модуль розпізнавання музичних композицій. Для його реалізації необхідна наявність серверної частини, яка, незалежно від клієнта, міститиме базу даних з відбитками музичних композицій [1, 2, 3]. За допомогою алгоритмів розпізнавання мелодій за заданим аргументом у вигляді відбитку сервер повертатиме список музичних композицій, які найбільше задовольняють умовам пошуку. Клієнтська частина матиме змогу взаємодіяти з серверною за допомогою розробленого прикладного програмного інтерфейсу (англ. API). Існує декілька шляхів для реалізації такого інтерфейсу. Одним з них є підхід REST, що базується на протоколі HTTP [4]. Іншим підходом є використання мови запитів GraphQL, що дозволяє будувати параметри запиту зі сторони клієнта [5, 6], на відміну від REST, де клієнт використовує запити лише в форматі, визначеному специфікацією серверної частини.

Узагальнену модель автоматизованої системи розпізнавання музичних звуків можна подати у формалізованому вигляді виразу 1:

$$M = \{I, N, D\}, \quad (1)$$

де I – вхідний аудіо потік, що записується користувачем;
N – рівень шумів у вхідному аудіо записі;
D – обсяг даних у базі відбитків існуючих композицій.

Модель клієнт-серверної мобільної системи розпізнавання музичних композицій, що презентує структуру автоматизованої системи, наведена на рис. 1.

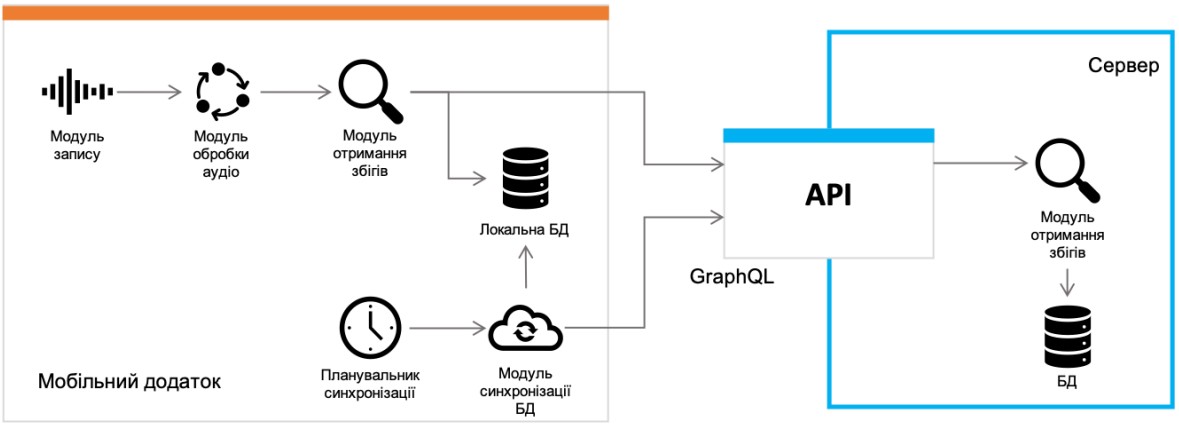

Рисунок 1 – Модель клієнт-серверної мобільної системи розпізнавання музичних композицій

Серед основних компонентів клієнтського мобільного додатку виділимо:

- Модуль запису – модуль запису вхідного аудіо потоку.
- Модуль обробки аудіо – компонента, що відповідає за дискретизацію вхідного аудіо потоку та створення його відбитку [1, 2, 3].
- Модуль отримання збігів – модуль, що реалізує логіку пошуку збігів у базах даних, а також оркеструє взаємодію локальної та серверної баз даних. В основу його реалізації покладено шаблон репозиторій (repository) [7].
- Локальна база даних (БД) містить набір відбитків та метаданих про музичні композиції для прискорення процесу розпізнавання. Наявність такої компоненти є важливою, оскільки вона дозволяє покрити більшість сценаріїв використання додатку з найпопулярнішими музичними композиціями з можливістю швидкого повернення результату після локального співставлення даних без необхідності затримок клієнт-серверної взаємодії.
- Модуль синхронізації БД – компонента, що відповідає за своєчасне оновлення локальної бази даних новими відбитками з серверної частини та за загальну синхронізацію клієнтської і серверної частин.
- Планувальник синхронізації – планувальник, що відповідає за розклад синхронізації локальної та серверної баз даних, а також реалізує стратегії оптимізації використання акумулятора та забезпечує роботу з низьким рівнем інтернет-з’єднання.

Основна задача планування оновлень – реалізація синхронізації локальної та серверної баз даних за мінімальних обчислювальних витрат і економії енергії акумулятора мобільного пристрою. Необхідно враховувати особливості виконання фонових задач на мобільних платформах, де є досить жорстке їх обмеження при роботи пристрою в стані спокою. Зокрема, операційна система Android використовує режим Doze, який забороняє фонову роботу пристрою у стані спокою, окрім коротких проміжків часу, так званих вікон підтримки, які визначаються операційною системою в процесі роботи та дозволяють виконувати короткочасні фонові операції [8].

Використання повної синхронізації в такому випадку є недоцільним, адже під час роботи в режимі Doze розроблювана система не має достатньо часу на завантаження оновлень у базу даних. Проте, такий підхід може використовуватися для коротких статусних оновлень. Крім того, необхідно враховувати силу сигналу інтернет-з’єднання і забороняти завантаження великого об’єму даних при слабкому рівні сигналу.

Таким чином, доцільно режим оновлення здійснювати шляхом отримання коротких статусних оновлень у фоновому режимі, що є можливим також при низькій якості інтернет-зв’язку. Повне оновлення та синхронізацію бази даних необхідно виконувати на старті додатку за наявним з’єднанням WiFi. Крім того, для зменшення об’єму даних, що необхідно завантажити мережею, виконуваний файл додатку міститиме встановлений початковий набір відбитків у базі даних.

Дослідження процесу розпізнавання звукового контенту

Після початкового запису вхідного аудіо сигналу, його дискретизації та створення відбитку [1,2,3] система надсилає запит до локальної бази даних на предмет пошуку збігів. При їх наявності відбувається

сортування за відсотковим показником збігу в порядку його спадання та обирається перший запис, що буде відображений користувачеві у вигляді метаданих бажаної музичної композиції.

Процес розпізнавання музичних композицій у вигляді блок-схеми алгоритму зображено на рис. 2.

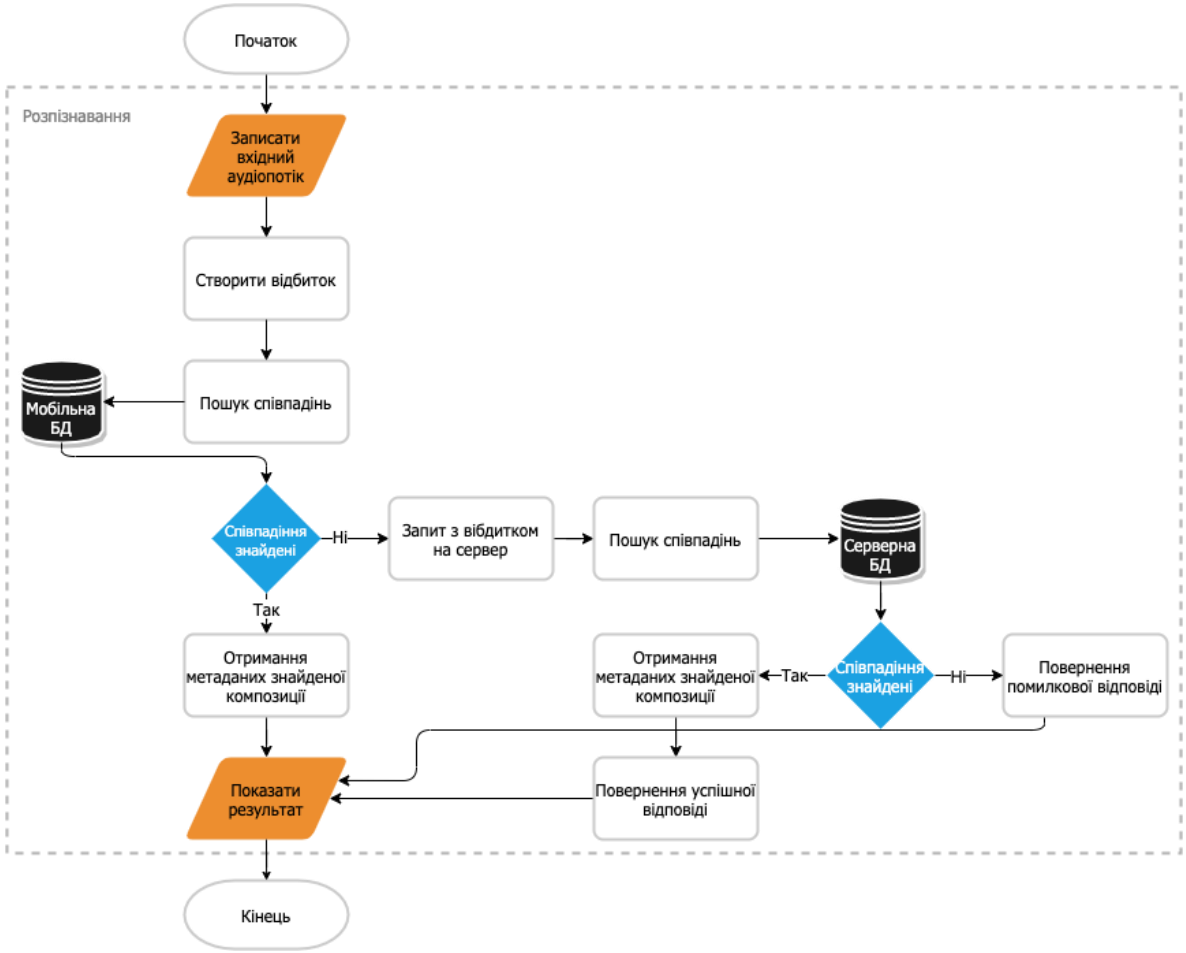

Рисунок 2 – Блок-схема алгоритму процесу розпізнавання музичних композицій

У разі відсутності локальних збігів, мобільний додаток створює запит до серверної компоненти і передає відбиток бажаної композиції у якості аргументу. Сервер, у свою чергу, робить запит до власної бази даних на предмет збігу відбитків. При позитивному результаті сервер формує успішну відповідь для клієнтського додатку з поверненням списку збігів. Мобільний додаток зберігає отримані дані у локальну базу, визначає найбільш релевантний елемент, що характеризує бажану музичну композицію, та відображає його користувачеві як результат.

У разі відсутності збігів з елементами серверної бази даних, клієнтський додаток отримуватиме відмову в шуканому результаті. Відповідне повідомлення про відмову буде відображене користувачеві.

Описаний процес розпізнавання аудіо контенту відображено на рис. 3 у вигляді діаграми послідовності з ідентифікацією архітектури процесу обробки звукових даних.

Описаний процес аналізу та розпізнавання музичних мелодій дозволяє оптимізувати ідентифікацію аудіо контенту за несприятливих комунікаційних умов клієнт-серверної взаємодії компонентів мобільної системи.

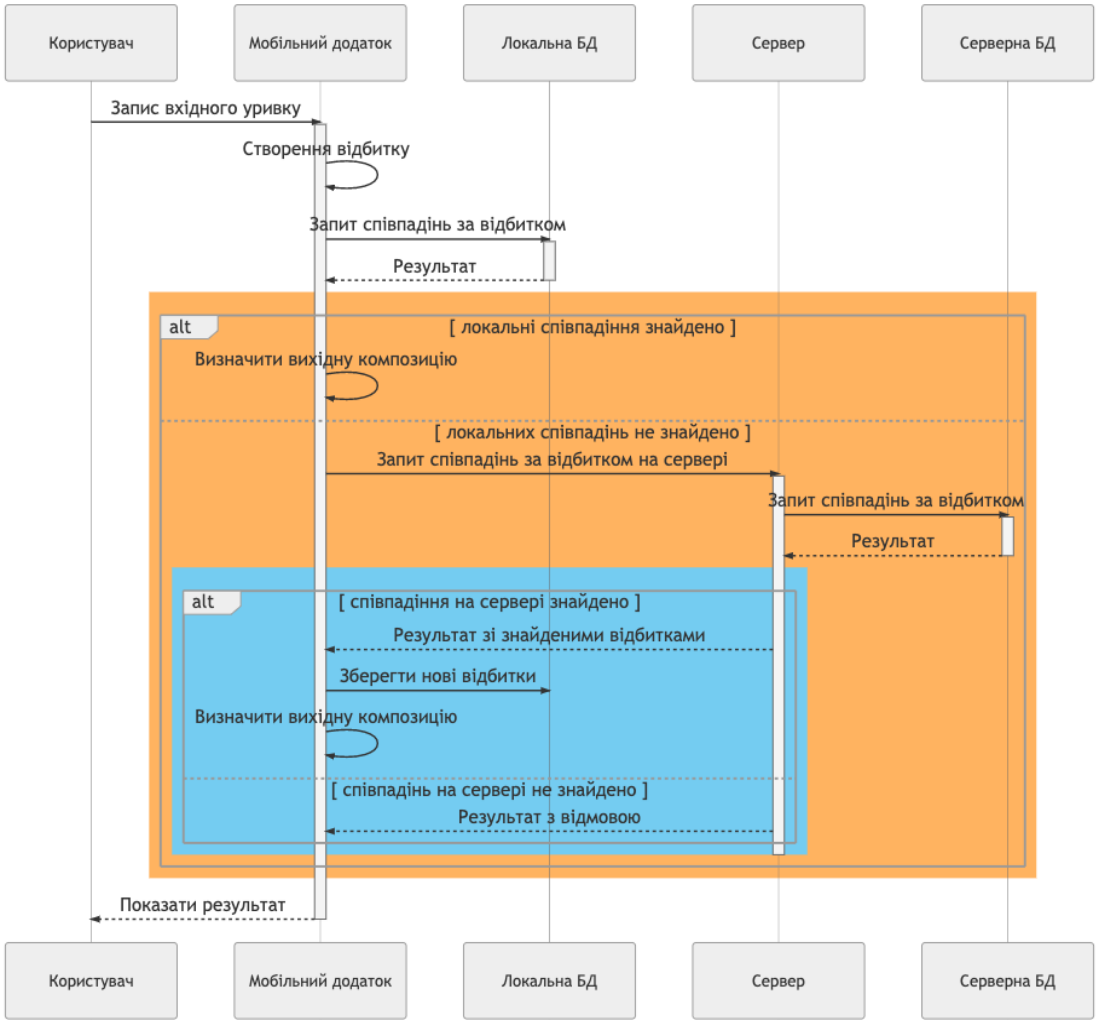

Рисунок 3 – Діаграма послідовності процесу розпізнавання музичних композицій

Висновки

Запропоновано моделі клієнт-серверної архітектури мобільної системи розпізнавання музичних композицій, орієнтовані на підвищення ідентифікаційних можливостей автоматизованої системи. Процес аналізу звукових потоків використовує закладені спеціалізовані особливості зберігання бази відбитків музичних композицій для прискорення процесу знаходження співпадань досліджуваного аудіо контенту. Проведено оптимізацію роботи мобільного додатку шляхом ефективного оновлення локальної бази музичних композицій з використанням режиму Doze на базі операційної системи Android, що дозоляє контролювати якість інтернет-зв’язку та враховувати можливість економії енергії акумулятора шляхом отримання коротких статусних оновлень бази даних у фоновому режимі.

Список літератури

[1] Ставицький П.В. Використання технологій аналізу та синтезу музичних звуків для розробки музичного синтезатора / П.В. Ставицький, А.В. Денисюк, В.В Войтко. НТКП ВНТУ. Факультет інформаційних технологій та комп'ютерної інженерії : XLVI Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії, 2017. С. 3 – URL: https://conferences. vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2793/2521

[2] Ставицький П.В. Розробка модуля розпізнавання музики для мобільного додатку / П.В.Ставицький, В.В Войтко. НТКП ВНТУ. Факультет інформаційних технологій та комп'ютерної інженерії : XLVII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії, 2018. – URL: https:// conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/view/ 5209/4571

[3] Voitko Viktoriia Automated system of audio components analysis and synthesis / Viktoriia V. Voitko, Svitlana V. Bevz, Sergii M. Burbelo, Pavlo V. Stavytskyi, Bogdan Pinaiev, Zbigniew Omiotek, Doszhon Baitussupov, Aigul Bazarbayeva. Proc. SPIE 11045, Optical Fibers and Their Applications, 2018, 110450V (15 March 2019); doi: 10.1117/12.2522313.
[4] Identify songs playing near you: веб-сайт. [Електронний ресурс] – Режим доступу: https://support.google.com/googleplaymusic/answer/2913276?hl=en
[5] GraphQL Specification Versions [Електронний ресурс] – Режим доступу: https://spec.graphql.org
[6] GraphQL: A data query language – Facebook Engineering [Електронний ресурс] – Режим доступу: https://engineering.fb .com/core-data/graphql-a-data-query-language/
[7] Fowler M. Patterns of Enterprise Application Architecture, Addison-Wesley Professional / M. Fowler, D.Rice, M. Foemmel, E. Hieatt, R. Mee, R. Stafford, 1 edition, 560, (November 15, 2002) – p. 322.
[8] Optimize for Doze and App Standby / Android Developers [Електронний ресурс] – Режим доступу: https://developer.android. com/training/monitoring-device-state/doze-standby

Стаття надійшла: 20.04.2020.

References

[1] Stavytskyi P.V. Vykorustannia tehnologiy analizy ta suntezy myzuchnuh zvukiv dlia rozrobku myzuchnogo suntezatora / P.V. Stavytskyi, A.V. Denusiuk, V.V. Voitko. NTKP VNTU. Facultet informatsijnuh tehnology ta kompjuternoj engenerii : XLVI Naukovo-tehnichna konferenzia facultety informatsijnuh tehnology ta kompjuternoj engenerii, 2017. P. 3 – URL: https://conferences. vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2793/2521
[2] Stavytskyi P.V. Rozrobka modulia rozpiznavannia myzuku dlia myzuchnogo dodatku / P.V. Stavytskyi, V.V. Voitko. NTKP VNTU. Facultet informatsijnuh tehnology ta kompjuternoj engenerii : XLVII Naukovo-tehnichna konferenzia facultety informatsijnuh tehnology ta kompjuternoj engenerii, 2018. – URL: https:// conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/view/ 5209/4571
[3] Voitko Viktoriia Automated system of audio components analysis and synthesis / Viktoriia V. Voitko, Svitlana V. Bevz, Sergii M. Burbelo, Pavlo V. Stavytskyi, Bogdan Pinaiev, Zbigniew Omiotek, Doszhon Baitussupov, Aigul Bazarbayeva. Proc. SPIE 11045, Optical Fibers and Their Applications, 2018, 110450V (15 March 2019); doi: 10.1117/12.2522313.
[4] Identify songs playing near you: web-sait. [Electronic resource] – Available: https://support.google.com/googleplaymusic/answer/2913276?hl=en
[5] GraphQL Specification Versions [Electronic resource] – Available: https://spec.graphql.org
[6] GraphQL: A data query language – Facebook Engineering [Electronic resource] – Available: https://engineering.fb .com/core-data/graphql-a-data-query-language/
[7] Fowler M. Patterns of Enterprise Application Architecture, Addison-Wesley Professional / M. Fowler, D.Rice, M. Foemmel, E. Hieatt, R. Mee, R. Stafford, 1 edition, 560, (November 15, 2002) – p. 322.
[8] Optimize for Doze and App Standby / Android Developers [Electronic resource] – Available: https://developer.android. com/training/monitoring-device-state/doze-standby

Відомості про авторів

Войтко Вікторія Володимирівна – канд. техн. наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет.
Бевз Світлана Володимирівна – канд. техн. наук, доцент кафедри електричних станцій і систем, Вінницький національний технічний університет.
Бурбело Сергій Михайлович – канд. техн. наук, старший викладач кафедри програмного забезпечення, Вінницький національний технічний університет.
Ставицький Павло Валерійович – аспірант кафедри програмного забезпечення, Вінницький національний технічний університет, Вінниця

В. В. Войтко, С. В. Бевз, С.М. Бурбело, П. В. Ставицкий

МОДЕЛИ СИСТЕМЫ АНАЛИЗА И РАСПОЗНАВАНИЯ МУЗЫКАЛЬНЫХ КОМПОЗИЦИЙ

Винницкий национальный технический университет, Винница

V.V. Voitko, S.V. Bevz, S.M. Burbelo, P.V. Stavytskyi

MODELS OF ANALYSIS AND RECOGNITION SYSTEM OF MUSICAL COMPOSITIONS

Vinnytsia National Technical University, Vinnytsia

УДК 638.235.231

О. В. Циганкова

НОВІ АЛГОРИТМИ ЗНАХОДЖЕННЯ БАЗОВОЇ ТОЧКИ НА ЕЛІПТИЧНИХ КРИВИХ У ФОРМІ ЕДВАРДСА

Національний технічний університет України «КПІ ім. Ігоря Сікорського», Фізико-технічний інститут, місто Київ

Анотація. Перетворення еліптичних кривих, що використовують у національному стандарті цифрового підпису ДСТУ 4145 2002, відповідають сучасним вимогам. Однак, бурхливий розвиток обчислювальної техніки та значне підвищення інтересу до криптології в усьому світі, залучення величезної кількості спеціалістів, у тому числі математиків, до роботи у даній галузі, призвели до зростання об'єму досліджень, постійного виникнення нових, все більш потужних методів криптоаналізу і, як наслідок, до можливого зменшення терміну життя існуючих та нових алгоритмів. У даній статті розв'язано актуальну науково-практичну задачу дослідження властивостей еліптичних кривих у формі Едвардса над простим полем F_p, де $p \neq 2$, придатних для використання в алгоритмах асиметричних криптосистем, зокрема, в алгоритмах цифрового підпису (ЦП). На підставі проведених досліджень було знайдено та описано нові способи знаходження базової точки на кривих у формі Едвардса. З застосуванням цих методів запропоновано три нових алгоритми визначення базової точки для побудови криптосистеми на повних та скручених кривих у формі Едвардса. Також у статті проведено порівняльний аналіз швидкодії розроблених алгоритмів знаходження базової точки для побудови криптосистеми на кривих у формі Едвардса та швидкодії криптоалгоритмів на несуперсингулярних еліптичних кривих у формі Вейєрштрасса над полями характеристики 2, перетворення яких використовуються в криптоалгоритмах ЦП ДСТУ 4145 2002. За результатами проведеного аналізу встановлено, що швидкодія трьох запропонованих алгоритмів вища, від стандартного алгоритму цифрового підпису на кривих у формі Вейєрштрасса, для першого алгоритму у 180 раз, другого - у 16log (n) (де $n \in \mathbb{P}$) раз та третього алгоритму у 32log (n) (де $n \in \mathbb{P}$) раз відповідно. На підставі проведених досліджень, у статті доведено, що використання еліптичних кривих у формі Едвардса над простими полями, замість кривих Вейєрштрасса, дозволяють підвищити швидкість експоненціювання точки в асиметричних криптосистемах. Результати роботи можуть бути використані в задачах аналізу існуючих та при розробці нових алгоритмів і стандартів асиметричної криптографії.

Ключові слова: скручені криві Едвардса, повні криві Едвардса, порядок кривої, порядок точки, базова точка, квадратичний лишок, квадратичний нелишок, алгоритм цифрового підпису, криві Вейєрштрасса, швидкодія.

Аннотация. Преобразование эллиптических кривых, которые используют в национальном стандарте цифровой подписи ДСТУ 4145 2002, соответствуют современным требованиям. Однако, бурное развитие вычислительной техники и значительное повышение интереса к криптологии во всем мире, привлечения огромного количества специалистов, в том числе математиков к работе в данной области, привели к росту объема исследований, постоянного возникновения новых все более мощных методов криптоанализа и, как следствие, к возможному уменьшению срока жизни существующих и новых алгоритмов. В данной статье решена актуальная научно-практическая задача исследования свойств эллиптических кривых в форме Эдвардса над простым полем F_p, де $p \neq 2$, пригодных для использования в алгоритмах асимметричных криптосистем, в частности, в алгоритмах цифровой подписи (ЦП). На основании проведенных исследований было найдено и описано новые способы нахождения базовой точки на кривых в форме Эдвардса. С применением этих способов предложено три новых алгоритма определения базовой точки для построения криптосистемы на полных и скрученных кривых в форме Эдвардса. Также в статье проведен сравнительный анализ быстродействия разработанных алгоритмов нахождения базовой точки для построения криптосистемы на кривых в форме Эдвардса и быстродействия криптоалгоритмов на несуперсингулярних эллиптических кривых в форме Вейерштрасса над полями характеристики 2, преобразования которых используются в криптоалгоритмах ЦП ДСТУ 4145 2002. По результатам анализа установлено, что предложенных три алгоритма быстрее стандартного алгоритма цифровой подписи на кривых в форме Вейерштрасса - соответственно первый алгоритм в 180 раза, второй в 16log (n) (где n$\in \mathbb{P}$) раз и третий алгоритм в 32log (n) (где $n \in \mathbb{P}$) раз. На основании проведенных исследований, в статье доказано, что использование эллиптических кривых в форме Эдвардса над простыми полями, вместо кривых Вейерштрасса, позволяют повысить скорость експоненциювання точки в асимметричных криптосистемах. Результаты работы могут быть использованы в задачах анализа существующих и создание новых алгоритмов и стандартов асимметричной криптографии.

Ключевые слова: скрученные кривые Эдвардса, полные кривые Эдвардса, порядок кривой, порядок точки, базовая точка, квадратичный вычет, квадратичный невычет, алгоритм цифровой подписи, кривые Вейерштрасса, быстродействие.

Summary. Transformations on elliptic curves which are used in the national digital signature standard DSTU 4145 2002, satisfy modern requirements. However, the fast development of computer technologies and a significant interest in cryptology worldwide have led to an increase in research, the constant emergence of new powerful cryptanalysis methods and, as a consequence, to the possible shortening of the lifetime of existing and new algorithms. This article addresses the current scientific and practical problem of investigating the properties of elliptic curves in the Edwards form over a finite field F_p, p ≠ 2, suitable for use in asymmetric cryptosystem, in particular, digital signature algorithms. Based on the research completed, new ways of determination of a base point on Edwards curves were outlined and described. Three new algorithms were proposed for determination of the base point for constructing a cryptosystem on the full and twisted Edwards curves. In this work the comparative analysis of the performance of the developed algorithms of the Edwards curves base point determination and the performance of crypto-algorithms on the non-perpendicular elliptic curves in the Weierstrass form over the fields of characteristic 2 was carried out. The analysis shows that proposed algorithms are faster than the standard Weirstrass digital signature curve algorithm – respectively, the first algorithm – 180 times, the second–$16\log(n)$ $(n \in \mathbb{P})$times, and the third algorithm–$32\log(n)$ $(n \in \mathbb{P})$ times. It is proved that the use of elliptic curves in the form of Edwards over finite field F_p, instead of Weierstrass curves, can increase the speed of operations of adding points in asymmetric cryptosystems. The results of the work can be applied to the analysis of existing problems and creation of new algorithms and standards of asymmetric cryptography.

Keywords: complete Edwards curves, twisted Edwards curves, order of a curve, order of a point, base point, quadratic residue, quadratic nonresidue, digital signature algorithm, Weierstrass curves, exponential speed increase.
DOI: https://doi.org/10.31649/1999-9941-2020-47-1-39-47.

Вступ

Еліптичні криві у формі Едвардса (ЕКФЕ) над простим полем на сьогодні забезпечують найбільшу швидкість та є перспективними для використання в асиметричних криптосистемах. Найвища продуктивність, універсальність закону додавання, унікальна симетрія точок та наявність афінних координат нейтрального елемента групи – головні властивості ЕКФЕ, які були виявлені і обґрунтовані вже в першій роботі [1] фахівцями з криптографії. Важливим є також те, що ізоморфні криві завжди належать одному класу. Також в роботі [2] доведено, що продуктивність операції експоненціювання точки ЕКФЕ, порівняно з кривою у формі Вейєрштрасса, в середньому вище більш ніж в 1,5 рази. На підставі цього та згідно з доведеним ізоморфізмом ЕКФЕ та кривих Вейєрштрасса [1], криві у формі Едвардса можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

У данійстатті розглянуто три варіанта створення алгоритмів пошуку генератора криптосистеми(базової точки) на ЕКФЕ над простим полем. У розділі 1 визначено властивості повних та скручених ЕКФЕ згідно з новою запропонованою класифікації ЕКФЕ [3].Наведено властивості точок простого порядку та методи їх знаходження. У другому розділіописано алгоритм знаходження базової точки на кривих Вейєрштрасса та створено та описано нові алгоритми знаходження базової точки для побудови криптосистеми на повних та скручених ЕКФЕ. У третьому розділі зроблено порівняльний аналіз швидкодії алгоритмів на ЕКФЕ та на кривих, що використовуються в стандартах цифрового підпису (ЦП).

Актуальність

Перетворення еліптичних кривих, що використовують у національному стандарті цифрового підпису ДСТУ 4145 2002, відповідають сучасним вимогам. Однак, бурхливий розвиток обчислювальної техніки та значне підвищення інтересу до криптології в усьому світі, залучення величезної кількості спеціалістів, у тому числі математиків, до роботи у даній галузі, призвели до зростання об'єму досліджень, постійного виникнення нових, все більш потужних методів криптоаналізу і, як наслідок, до можливого зменшення терміну життя існуючих та нових алгоритмів. Це зумовлює актуальність дослідження властивостей ЕКФЕ над простими полями з метою застосування їх у сучасних більш ефективних криптосистемах на еліптичних кривих.

Мета

Метою дослідження є створення більш швидких за існуючі алгоритмів знаходження базової точки з застосуванням перетворень ЕКФЕ які можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

Задачі

1.Визначити необхідні властивості ЕКФЕ які можуть бути використані у створенні більш швидких алгоритмах знаходження базової точки.

2.Створитиалгоритми пошуку базової точки на повних та скручених ЕКФЕ.

3.Провести порівняльний аналіз швидкодії алгоритмів знаходження базової точки для побудови криптосистеми на ЕКФЕ та кривих у формі Вейєрштрасса.

Розв'язання задач

1. Визначення та властивості повних та скручених ЕКФЕ за новою класифікацією

Криву в узагальненій формі Едвардса визначено рівнянням:

$$E_{a,d}:\ x^2 + ay^2 = 1 + dx^2y^2,\quad a,d \in F_p^*, d \neq 1,\ a \neq d,\ p \neq 2. \tag{1}$$

Для форми кривої (1) маємо універсальний модифікований [3] закон додавання точок (2):

$$(x_1,y_1) + (x_2,y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2},\ \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right) \tag{2}$$

що не змінюється і у випадку коли$(x_1,y_1) = (x_2,y_2)$:

$$2(x_1,y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \tag{3}$$

Точка на ЕКФЕ визначена як $\boldsymbol{P} = (x,y)$,зворотна точка як $-\boldsymbol{P} = (x,-y)$, точки малих порядків: $\boldsymbol{O}, \boldsymbol{D}_0$ та $\pm\boldsymbol{F}_0$. На основі нової модифікації ЕКФЕ, введена арифметика для операцій у групі з особливими точками цих кривих, формули зв`язку точок малих порядків і формули, що пов'язують їх з іншими точками кривої. Точка другого порядку $\boldsymbol{D}_0 = (-1,0)$така, що $2\boldsymbol{D}_0 = \boldsymbol{O}$. Нейтральний елемент групи точок $\boldsymbol{O} = \boldsymbol{P} + (-\boldsymbol{P}) = (1,0)$. Залежно від властивостей параметрів *a* і *d,* наведено умови існування двох особливих точок 2-го порядку та умови існування двох або чотирьох точок 4-го порядку $\boldsymbol{F}$, для яких $\pm 2\boldsymbol{F} = \boldsymbol{D}$. Між точками існують залежності:

$(x,y) + (-1,0) = (-x,-y);$
$(x,y) - (0,1) = (-y,x);$
$(x,y) + (0,-1) = (y,-x);$
$(x,y) + (y,x) = (0,1).$

Із застосуванням нової модифікації, на базі аналізу квадратичності параметрів *a* і *d*кривої проведено аналіз ЕКФЕ над простими скінченними полями характеристики $p > 3$ та створено нову повну класифікаціюкривих в узагальненій формі Едвардса [3] (табл.1). За новою класифікацією ЕКФЕ розбиваються на три класи, що не перетинаються:

- *повні* ЕКФЕ з умовою: $\chi(ad) = -1$;
- *скручені*ЕКФЕ з умовами: $\chi(a) = \chi(d) = -1$;
- *квадратичні* ЕКФЕ з умовами: $\chi(a) = \chi(d) = 1$,

де $\chi(a) = \left(\frac{a}{p}\right)$ –символ Лежандра, показник квадратичності параметру.

Таблиця 1 - Нова класифікація ЕКФЕ над простими полями. Координати точок ЕКФЕ 2-го та 4-го порядків

		Параметри	Порядок кривої	Точки 2-го порядку	Точки 4-го порядку
Повні	***1.a***	$\chi(a) = 1$ $\chi(d) = -1$	$N_E = 4n$	$\boldsymbol{D}_0 = (-1,0)$	$\pm\boldsymbol{F}_0 = (0, \pm 1/\sqrt{a})$
	1.b	$\chi(a) = -1$ $\chi(d) = 1$			$\pm\boldsymbol{F}_0 = (0, \pm 1/\sqrt{d})$
Скручені	***2***	$\chi(a) = -1$ $\chi(d) = -1$	$N_E = 4n$	$\boldsymbol{D}_0 = (-1,0)$	$\pm\boldsymbol{F}_{1,2} = (\pm\sqrt[4]{a/d},$ $\pm\sqrt{-1/\sqrt{ad}})$ $p \equiv 3 mod 4$
Квадратичні	***3***	$\chi(a) = 1$ $\chi(d) = 1$	$N_E \geq 8n$	$\boldsymbol{D}_{1,2} = (\pm\sqrt{a/d}, \infty)$	$\pm\boldsymbol{F}_0 = (0, \pm 1/\sqrt{d})$ $\pm\boldsymbol{F}_1 = (\infty, \pm 1/\sqrt{d})$ $\pm\boldsymbol{F}_{2,3} = (\pm\sqrt[4]{a/d},$ $\pm\sqrt{-1/\sqrt{ad}})$

За результатами досліджень різних класів ЕКФЕ було зроблено висновки, що квадратичні ЕКФЕ мають чотири особливих точки та, як наслідок, великий мінімальний кофактор порядку кривої, що збільшує кількість операцій при пошуку генератора та ускладнює роботу з такими кривими. На підставі цього використовувати квадратичні ЕКФЕ в криптоалгоритмах недоцільно, хіба що для теоретичного аналізу, так як квадратичні криві зі скрученими утворюють пару квадратичного крутіння[3].

За аналізом властивостей класів повних та скручених ЕКФЕ було зроблено висновки, що повні та скручені ЕКФЕ можуть бути рекомендовані для використання в криптоалгоритмах, оскільки вони мають циклічну підгрупу групи точок, в якій всі точки не є особливими -це суттєво спрощує реалізацію алгоритмів ЦП та шифрування на ЕКФЕ. Повні та скручені криві мають мінімальний кофактор порядку кривої4. Також вони мають високу швидкість експоненціювання точки, завдяки чому прискорюється виконання алгоритмів ЦПта шифрування[3].На підставі цього розглянемо ЕКФЕ, які належать класам повних та скручених, за новою класифікацією, з метою створення алгоритмів пошуку генератора криптосистеми для використання у протоколах ЦП.

2 Алгоритми пошуку базової точки на повних та скручених ЕКФЕ

Важливою властивістю повних та скручених ЕКФЕ є те, що при $p \equiv 1 mod 4$ вони мають мінімальний парний кофактор порядку кривої 4: $N_E = 4n$ де $n \in \mathbb{P}$. Циклічна підгрупа скручених ЕКФЕ простого порядку n має такі ж самі корисні для криптографічних застосувань і стандартизації властивості,що і повні криві Едвардса[3]. В алгоритмі ЦП важливим кроком є знаходження генератора криптосистеми - тобто базової точки простого порядку n. Для створення алгоритму пошуку базової точки для побудови криптосистеми на повних та скручених кривих було розглянуто декілька варіантів знаходження точок простого порядку.

Один з алгоритмів знаходження базової точки на повних ЕКФЕ було створено на запропонованому методі знаходження точки максимального порядку $4n$ [5], розробленого на підставі 3-х теорем щодо властивостей точок повної ЕКФЕ:

Теорема 1Для будь-якої точки (x,y) повної кривої Едвардса, що не належить колу радіуса 1, існують 2 точки ділення на 2 $\{P, P+D\}$ тоді і тільки тоді, коли $\chi(1 - y^2) = 1$.

Доведення

Скористуємося методом заміни змінної. Якщо взяти лише точки, порядки яких більше 4, та у формулах зробимо заміну

$$X = x_1^2, Y = y_1^2, Z = Y/X, V = XY, X, Y \neq 0.$$

Зробимо заміну у знаменнику (2) на $(X + Y)$ та $(2 - X - Y)$ відповідно. Згідно з (1) та (3) для однієї точки P кривої $ordP > 4$ справедливі вирази:

$$Z^2 - 2x^{-1}Z + 1 = 0,$$
$$dV^2 - 2x^{-1}V + 1 = 0, x \neq 0,1. \quad (4)$$

Дискримінанти

$$\Delta_1 = 4x^{-2}(1 - x^2),$$
$$\Delta_2 = 4x^{-2}(1 - dx^2), \quad (5)$$

та розв'язок

$$Z_{1,2} = x^{-1}\left(1 \pm \sqrt{1 - x^2}\right),$$
$$V_{1,2} = (xd)^{-1}\left(1 \pm \sqrt{1 - dx^2}\right). \quad (6)$$

Необхідність. Подвоєння будь якої точки P з ненульовими координатами згідно з законом (2) породжує єдину точку $2P = (x, y)$, та координати точок P і $2P$ є розв'язок двох рівнянь (4) у полі $\boldsymbol{F}_p$. Необхідною умовою існування розв'язку першого з рівнянь (4), як слідує з (5), є те, що елемент поля $\chi(1 - x^2) = 1$. При виконанні цієї умови окрім точки P, для якої $2P = (x, y)$, існує ще одна точка $P^* = P + D = (-x_1, -y_1)$, для якої $2P^* = 2P + 2D = (x, y)$,так як $2D = 0$. При $\chi(1 - x^2) = -1$ рівняння (4) розв'язків в полі немає. Необхідність умови теореми 1 доведено.

Достатність. Для будь якої точки кривої (1), у якої $ordP > 4$, для якої має місце розв'язок (3), справедливо дві тотожності (4). Достатньо, щоб один з дискримінантів (5) був квадратичним лишком, тоді другий дискримінант теж буде квадратичним лишком. Нехай точка$P = (x, y)$ належить кривій (1) де $a = 1$. Тоді рівняння $x^2 + y^2 = 1 + dx^2y^2$можна записати як $(1 - y^2) = x^2(1 - dy^2)$. Звідси вочевидь випливає, що для будь-якої точки (x, y) кривої вирази$(1 - y^2)$ та $(1 - dy^2)$є обидва квадратичними лишками або нелишками. У першому випадку існує дві точки ділення на 2, а в іншому випадку – не існує. Теорему 1 доведено[6].

Теорема 2 Необхідною і достатньою умовою існування 4-х точок 8-го порядку повної кривої Едвардса є $\chi(1 - d) = 1$.

Доведення

Необхідність. Нехай $Ord(P) = 8$, тоді $2P = F$. Відповідно з формулою (2) для координат $P = (x, y)$ маємо:

$$\frac{2xy}{(1 + dx^2y^2)} = 1, \quad \frac{y^2 - x^2}{(1 - dx^2y^2)} = 0.$$

Звідси $y^2 = x^2 \implies dx^4 - 2x^2 + 1 = 0 \implies x^2 = 1 \pm \sqrt{1 - d}$.

Тобто умова $\chi(1 - d) = 1$ теореми є необхідною умовою існування координат $x = \pm y$.

Достатність. Доведемо, що умова теореми завжди породжує рівно 4 точки 8-го порядку. Так як додаток $(1+\sqrt{1-d})(1-\sqrt{1-d})=d$, то одне з значень у рівності $x^2=1\pm\sqrt{1-d}$ є квадратичним лишком, а друге – нелишком. Якщо вибирати двійковим квадрат з цієї альтернативи $(1+(-1)^{\kappa}\sqrt{1-d})$, $\kappa\in\{0,1\}$, отримуємо 4 точки $(\pm x,\pm y)$ 8-го порядку. Теорему 2 доведено [8].

Теорема 3Для будь-якої точки(x,y) повної кривої Едвардса, що не належить колу радіуса 1, справедлива рівність $\chi(1-x^2)\cdot\chi(1-y^2)=\chi(1-d)$.

Доведення

Для точки (x,y) з урахуванням (1) де $a=1$ запишемо додаток

$(1-y^2)(1-x^2)=1+x^2y^2-x^2-y^2=y^2-dy^2=(1-d)x^2y^2.$

Тоді з останнього співвідношення випливає, що додаток $(1-y^2)(1-x^2)$ є квадратичним нелишком при $\chi(1-d)=-1$, та навпаки, що і доводить твердження теореми 3[6].

Метод знаходження точки максимального порядку полягає у тестуванні значення символу Лежандра або квадратичного характеру виразу $(1-y^2)$. Якщо виконується умова $\chi(1-d)=-1$, то відповідно до теореми 2, крива не має точок 8 порядку і порядок кривої $N_E=4n$,де $n\in\mathbb{P}$. Таким чином якщо $\chi(1-y^2)=-1$, то $\chi(1-x^2)=1$ і навпаки, що дає можливість знайти точку максимального порядку одним тестуванням характеру квадратичності $(1-y^2)$координати випадкової точки кривої. Практично $1/2$ випадкових точок кривої мають порядок $4n$, $1/4$ – порядок $2n$ та $1/4$– порядок n [4].

На базі методу знаходження точки максимального порядку, створено Алгоритм 1(рис.1) обчислення генератора криптосистеми, тобто точки простого порядку *n*на повній ЕКФЕ.

***Алгоритм* 1**:

умови: ЕКФЕ має вигляд (1), де $\chi(ad)=-1$, $N_E=4n, n\in\mathbb{P}, p\equiv 1mod4$.

1. знаходиться випадкова координата x точки $P=(x,y)$;
2. якщо $x=0$, або ±1, або $\pm\frac{1}{\sqrt{d}}$,то перейти до кроку1;
3. обчислюється $z=(1-x^2)(1-dx^2)^{-1}modp$;
4. якщо $\chi(z)\neq 1$, то перейти до кроку 1;
5. обчислюється $y=\sqrt{z}modp$;
6. якщо $\chi(1-y^2)\neq 1$, то $x\leftrightarrow y; P\leftarrow(y,x)$;
7. обчислюється $G=2P$;

вихід: точка $G=(x_G,y_G)$, така, що Ord(*G*) = *n*.

$$\begin{array}{|l|l|}\hline N_E=4n & if\ \chi(1-y^2)=1 \Longrightarrow\ 2P\ \Longrightarrow\ G\\ \forall P=(x,y) & \\ OrdP>4 & if\ \chi(1-y^2)=-1\Longrightarrow x\leftrightarrow y\Rightarrow\chi(1-y^2)=1\Longrightarrow 2P\Longrightarrow G\\ p\equiv 1mod4 & \\ \hline\end{array}$$

Рисунок 1–Алгоритм 1 находження базової точки на повних ЕКФЕ

Згідно з властивостями порядків точок повної ЕКФЕ над полями F_p, де $p\equiv 1mod4$, подвоєння точки максимального порядку $4n$ створює точку, порядок якої дорівнює $2n$. Подвоєння точки порядку $2n$створює точку простого порядкуn.На підставі цієї властивості порядків точок повної ЕКФЕ розроблено Алгоритм 2 (рис.2) знаходження точки простого порядку.

***Алгоритм* 2**:

умови: ЕКФЕ має вигляд за формулою (1) де $\chi(ad)=-1, N_E=4n, n\in\mathbb{P}$, $p\equiv 1mod4$.

1. знаходиться випадкова координата x точки $P=(x,y)$;
2. якщо $x=0$, або ±1, або $\pm\frac{1}{\sqrt{d}}$, то перейти до кроку1;
3. обчислюється$z=(1-x^2)(1-dx^2)^{-1}modp$;
4. якщо $\chi(z)\neq 1$, то перейти до кроку 1;

5. обчислюється $y = \sqrt{z} mod p;$
6. обчислюється $G = 4P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

$$\begin{cases} N_E = 4n \\ p \equiv 1 \bmod 4 \\ OrdP > 4 \end{cases} \quad \forall P \Longrightarrow 4P \Longrightarrow G.$$

Рисунок 2– Алгоритм 2 знаходження базової точки на повних ЕКФЕ

Для скрученої ЕКФЕ знаходження точки простого порядку прискорюється удвічі завдяки одному подвоєнню випадкової точки. На підставі цього створено найшвидший Алгоритм 3(рис.3).

***Алгоритм* 3**:

умови: ЕКФЕ має вигляд за формулою (1) де $\chi(a) = \chi(d) = -1, N_E = 4n, n \in \mathbb{P},\ p \equiv 1 mod 4.$

1. знаходиться випадкова координата x точки $P = (x, y)$;
2. якщо $x = 0$, або ± 1, або $\pm \frac{1}{\sqrt{d}}$, то перейти до кроку1;
3. обчислюється $z = (1 - x^2)(1 - dx^2)^{-1} mod p$;
4. якщо $\chi(z) \neq 1$, то перейти до кроку 1;
5. обчислюється $y = \sqrt{z} mod p;$
6. обчислюється $G = 2P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

$$\begin{cases} N_E = 4n \\ p \equiv 1 \bmod 4 \\ OrdP > 4 \end{cases} \quad \forall P \Longrightarrow 2P \Longrightarrow G.$$

Рисунок 3 – Алгоритм 3 знаходження базової точки на скручених ЕКФЕ

3 Порівняльний аналіз швидкодії алгоритмів знаходження базової точки для побудови криптосистеми на ЕКФЕ та кривих у формі Вейєрштрасса

Алгоритми знаходження базової точки на повних та скручених ЕКФЕ виглядають значно простішими та швидкими у порівняно зі стандартним алгоритмом на канонічній кривій. Необхідно провести порівняльний аналіз швидкодії цих алгоритмів.

Стандартний алгоритм ЦП на еліптичних кривих:

1. знаходиться випадкова точка $P = (x, y)$;
2. обчислюється скалярний добуток nP;
3. якщо $(nP) \neq \mathbf{0}$, то перейти до кроку 1;
4. якщо$(nP) = \mathbf{0}$, то $P = G$;

вихід: точка $G = (x_G, y_G)$.

Знаходження кількості операцій, які потрібно виконати при пошуку точки простого порядку на кривих Вейєрштрасса в стандартному алгоритмі [7]:

- пошук точки, стандартним методом, що належить кривій, потребує 8 кроків до успіху;
- обчислення скалярного добутку nP в проективних координатахпотребує $\log(n)$ подвоєння. Всього $5.67M\log(n)$ операцій. У середньому $0.5\log(n)$додавання точок;
- $0.5 \cdot 11.17M \log(n) = 5.58M \cdot \log(n)$,де M – кількість множень у полі;
- загальне число операцій у полі з урахуванням 4-х кроків (в середньому) до успішного результату:

$$S = 8 \cdot 4 \cdot (5.67 + 5.58)M \cdot \log(n) = 360M \cdot \log(n).$$

Знаходження кількості операцій в запропонованих алгоритмах 1, 2 та 3 виконувався таким же чином [6, 7].

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 1:

- пошук точки. Невдача: $\forall$ точка, якщо $x = 0, \pm 1, \pm\frac{1}{\sqrt{d}}$; та $\forall\, \chi(z) \neq 1$.

Якщо умови x виконуються $\Longrightarrow$ можна вважати, що z– виконуються. $\Longrightarrow p(\chi(z) \neq 1) = \frac{1}{2}$. Тому, імовірність успіху $\geq 1 - \frac{1}{2} - \frac{4}{n} \approx \frac{1}{2} \Longrightarrow$ середня кількість до успіху дорівнює 2 крокам.

- обчислення $(1 - y^2)$ потребує $0{,}67M$ операцій;
- обчислення символу Лежандра $\chi(1 - y^2)$ потребує $M\log(n)$;
- одне подвоєння точки потребує $0{,}67M$ операцій;
- сумарна кількість операцій у полі:

$S_1 = 2 \cdot (5.67 + 0.68 + \log(n)) \cdot M == 2 \cdot (6.34 + \log(n))M.$

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 2:

- пошук точки. Середня кількість до успіху дорівнює 2 крокам. (див. Алгоритм 1);
- обчислення $G = 4P$ потребує два подвоєння;
- сумарна кількість операцій у полі:

$$S_2 = 2 \cdot 2 \cdot 5.67M = 22.68M.$$

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 3:

- Пошук точки. Середня кількість до успіху дорівнює 2 крокам. (див. Алгоритм 1);
- Обчислення $G = 2P$ потребує одне подвоєння;
- Сумарна кількість операцій у полі:

$$S_3 = 11{,}34M.$$

Усі значення кількості операцій у групі, які потрібно виконати при пошуку точки простого порядку в алгоритмах пошуку базової точки,записано у таблиці 2.

Таблиця 2 - Кількості операцій при пошуку генератора криптосистеми

Алгоритми	**Кількість операцій у полі,** **де M– кількість множень у полі**
Стандартний алгоритм	$S = 360M \cdot \log(n)$
Алгоритм 1	$S_1 = 2 \cdot (6.34 + \log(n))M$
Алгоритм 2	$S_2 = 22{,}68M$
Алгоритм 3	$S_3 = 11{,}34M$

На підставі отриманих результатів можна зробити порівняльний аналіз швидкодії та отримати значення виграшу γ для усіх запропонованих алгоритмів.

$$\gamma_1 = \frac{S}{S_1} = \frac{360M \cdot \log(n)}{2 \cdot (6.34 + \log(n))M} \approx 180$$
$$\gamma_2 = \frac{S}{S_2} = \frac{360M \cdot \log(n)}{22{,}68M} \approx 16\log(n)$$
$$\gamma_3 = \frac{S}{S_3} = \frac{360M \cdot \log(n)}{11{,}34M} \approx 32\log(n)$$

За розрахунком значення виграшу нових алгоритмів порівняно зі стандартним алгоритмом, було отримано результати:

- виграш у швидкодії Алгоритму 1 порівняно зі стандартним алгоритмом у $\gamma_1 = \frac{5}{s_1} \approx 180$ разів;
- виграш у швидкодії Алгоритму 2 порівняно зі стандартним алгоритмом у $\gamma_2 = \frac{5}{s_2} \approx 16\log(n)$ разів.
- виграш у швидкодії Алгоритму 3 порівняно зі стандартним алгоритмом у $\gamma_2 = \frac{5}{s_3} \approx 32\log(n)$ разів.

Результати обчислень дають змогу зробити обґрунтовані висновки, що знаходження генератора на ЕКФЕ із застосуванням запропонованих алгоритмів порівняно зі стандартним алгоритмом істотно більш швидше і відповідно ефективніше.

Висновки

1. Устаттірозв'язано актуальну науково-практичну задачу дослідження властивостей еліптичних кривих у формі Едвардса, придатних для використання в алгоритмах асиметричних криптосистем, зокрема, в алгоритмах цифрового підпису, які дозволяють підвищити швидкодію експоненціювання точки в цих криптосистемах.

2. Проведені дослідження дозволили запропонувати три новихалгоритми визначення базової точки для побудови криптосистеми на повних та скручених ЕКФЕ,

3. За результатами досліджень зроблено висновки, що розроблені алгоритми визначення базової точки швидше стандартного алгоритму ЦПна кривих у формі Вейєрштрассау 180, $16\log(n)$ та $32\log(n)$(де$n \in \mathbb{P}$)разів відповідно. Результати роботи можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

Перелік посилань

[1] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[2] Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015. С.58-63.

[3] Бессалов А.В., Цыганкова О.В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоелектроника, Том 14 № 3, 2015. С.197-203.

[4] Bessalov A.V.,Tsygankova O.V. New properties of the Edwards form elliptic curveover a primefield // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №180 2015. pp.137-143.

[5] Bessalov A. V., Tsygankova O.V. Interrelation of families of points of highorderon the Edwards curve over a primefield // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. sci-hub.tw/10.1134/S0032946015040080

[6] Бессалов А.В., Цыганкова О.В. Метод определения точек максимального порядка на кривой Эдвардса. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2(26), 2014. С.18-21.

[7] Bernstein Daniel J.,Birkner Peter, JoyeMarc, Lange Tanja, Peters Christiane. Twisted Edwards Curves.//IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.

[8] Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монографія //изд-во «Политехника», КПИ им. Игоря Сикорского, Киев. 2017. – 272с.

Стаття надійшла: 28.02.2020.

References

[1] Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

[2] Bessalov A.V., Tsygankova O.V. Proyzvodytelnost hruppovykh operatsyi na skruchennoi kryvoi Edvardsa nad prostym polem. // Radyotekhnyka #181, 2015. S.58-63.

[3] Bessalov A.V., Tsygankova O.V. Klassyfykatsyia kryvykh v forme Edvardsa nad prostым polem. // Prykladnaia radyoelektronyka, Tom 14 № 3, 2015. S.197-203.

[4] Bessalov A.V., Tsygankova O.V. New properties of the Edwards form elliptic curveover a primefield // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №180 2015. pp.137-143.

[5] Bessalov A.V., Tsygankova O.V. Interrelation of families of points of highorderon the Edwards curve over a primefield // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. sci-hub.tw/10.1134/S0032946015040080

[6] Bessalov A.V., Tsygankova O.V. Metod opredelenyia tochek maksymalnoho poriadka na kryvoi Эdvardsa. // Spetsialni telekomunikatsiini systemy ta zakhyst informatsii. Zbirnyk naukovykh prats, vypusk 2(26), 2014. S.18-21.

[7] Bernstein Daniel J.,Birkner Peter, JoyeMarc, Lange Tanja, Peters Christiane. Twisted Edwards Curves.//IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.
[8] Bessalov A.V. Эllyptycheskye kryvыe v forme Эdvardsa y kryptohrafyia: monohrafiia // yzd-vo «Polytekhnyka», KPY ym. Yhoria Sykorskoho, Kyev. 2017. – 272s.

Відомості про автора
Циганкова Оксана Валентинівна - без ступеню, без звання, асистент кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського, Київ 02232 просп. Маяковського 71 кв. 2.

О. В. Цыганкова

НОВЫЕ АЛГОРИТМЫ НАХОЖДЕНИЯ БАЗОВОЙ ТОЧКИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В ФОРМЕ ЭДВАРДСА

Национальный технический университет Украины КПИ имени Игоря Сикорского, Киев

O.V. Tsygankova

NEW BASE POINT ALGORITHMS FOR EDWARDS ELLIPTIC CURVES

National Technical University of Ukraine "Igor Sikorsky KPI", Institute of Physics and Technology, Kiev

ДО ВІДОМА АВТОРІВ

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