

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 11, № 1-2

Volume 11, No. 1-2

Одеса – 2021
Odesa – 2021

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 р.

Виходить 4 рази на рік

Published 4 times a year

Заснований Одеським національним політехнічним університетом у 2011 році

Founded by Odessa National Polytechnic University in 2011

Свідоцтво про державну реєстрацію
КВ № 17610 - 6460Р від 04.04.2011р.

Certificate of State Registration
КВ № 17610 - 6460Р of 04.04.2011

Головний редактор: *А.А. Кобозєва*

Editor-in-chief: *A. Kobozeva*

Заступник головного редактора:

Associate editor:

С.А. Положаєнко

S. Polozhaenko

Відповідальний редактор:

Executive editor:

О.А. Стопакевич

O. Stopakevych

Редакційна колегія:

Editorial Board:

*І.І. Бобок, Д. Джухар, А.А. Кобозєва,
В.Ф. Ложечніков, В.В. Любченко,
В.Д. Павленко, В.В. Палагін,
С.А. Положаєнко, О.В. Рибальський,
А.В. Соколов, В.О. Сперанський,
О.А. Стопакевич, О.О. Фомін*

*I. Bobok, J. Juhar, A. Kobozeva,
V. Lozhechnikov, V. Liubchenko, V. Pavlenko,
V. Palahin, S. Polozhaenko, O. Rybalsky,
A. Sokolov, B. Speransky, O. Stopakevych,
O. Fomin*

Друкується за рішенням редакційної колегії та Вченої ради Державного університету
«Одеська політехніка»

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна

Телефон: +38 048 705 8506

Web: <http://immm.opu.ua>

E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine

Tel.: +38 048 705 8506

Web: <http://immm.opu.ua>

E-mail: immm.ukraine@gmail.com

© Державний університет «Одеська політехніка», 2021

ЗМІСТ/CONTENTS

РОЗРОБКА СТЕГАНОГРАФІЧНОГО
МЕТОДУ ВБУДОВИ БІНАРНОГО
ЦИФРОВОГО ВОДЯНОГО ЗНАКУ В
ЗОБРАЖЕННЯ НА ОСНОВІ
ДИСКРЕТНОГО КОСИНУСНОГО
ПЕРЕТВОРЕННЯ

Г.В. Ахмаметьєва, В.О. Кирилюк

5

DEVELOPMENT OF
STEGANOGRAPHICAL METHOD OF
BINARY DIGITAL WATER MARK
INSERT INTO IMAGE BASED ON
DISCRETE COSINUS
TRANSFORMATION

Akhmametieva A., Kyryliuk V.

УПРАВЛІННЯ КОНФЛІКТАМИ ТА
ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ В МЕРЕЖІ INTERNET

В.О. Хорошко, М.М. Браїловський

15

INFORMATION SECURITY CONFLICTS
AND INCIDENTS MANAGEMENT ON
THE INTERNET

Horoshko V., Brailovskyi M.

РОЗРОБКА КОМП'ЮТЕРНИХ
ПРОГРАМ ОПТИМАЛЬНОГО
ПРОЕКТУВАННЯ ДИНАМІЧНИХ
ПРОЦЕСІВ СПІЛЬНОГО
ПІДПРИЄМСТВА З ВИРОБНИЦТВА І
ЗБУТУ ПРОДУКЦІЇ

Н.М. Єршова, Н.О. Вельмагіна,
Н.С. Чуприна

26

COMPUTER PROGRAMS FOR OPTIMAL
DYNAMIC PROCESSES OF JOINT
VENTURE FOR PRODUCTION AND
MARKETING OF GOODS DESIGN
DEVELOPMENT

Yershova N., Velmahina N., Chupryna N.

РОЗРОБКА АЛГОРИТМУ ВИЯВЛЕННЯ
ЗАШУМЛЕННЯ ЯК ФАЛЬСИФІКАЦІЇ
ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, О.Ю. Лебедєва, Н.О. Бензар

39

DEVELOPMENT OF AN ALGORITHM
FOR DETECTION OF
NOISE AS FALSIFICATION OF DIGITAL
IMAGE

Zorilo V., Lebedeva O., Benzar N.

РОЗРОБКА ТРЬОХМОДУЛЬНОЇ
КРИПТОСИСТЕМИ РАБІНА
НА ОСНОВІ ОПЕРАЦІЇ ДОДАВАННЯ

М.М. Касянчук, О.Я. Лотоцький, С.В.
Яцків, С.В. Івасьєв, Л.М. Тимошенко

47

DEVELOPING RABIN THREE-
MODULAR CRYPTOSYSTEM BASED
ON THE OPERATION OF ADDITION

Kasianchuk M., Lototsky O., Yatskiv S.,
Ivasiev S., Tymoshenko L.

ДІАГНОСТИКА ХВОРОБИ СЕРЦЯ НА
ОСНОВІ ДЕРЕВ РІШЕНЬ

В.Г. Пенко, І.М. Шпінарева, О.В. Ярошук

58

DIAGNOSIS OF HEART DISEASE
BASED ON DECISION TREES

Pienko V., Shpinareva I., Yaroshchuk A.

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ПОВЕДІНКИ ВІРТУАЛЬНОГО НАТОВПУ О.М. Симонова, І.І. Бобок	69	DEVELOPMENT OF A MATHEMATICAL MODEL OF VIRTUAL CROWD BEHAVIOR Simonova O., Bobok I.
МОДЕЛЮВАННЯ РОБОТИ СИСТЕМИ АВТОМАТИЗОВАНОГО КЕРУВАННЯ ПРОЦЕСОМ УВАРЮВАННЯ ЦУКРОВИХ УТФЕЛІВ У ВАКУУМ- АПАРАТІ ПЕРІОДИЧНОЇ ДІЇ У СЕРЕДОВИЩІ ПРОГРАМОВАНОГО КОНТРОЛЕРА Ю.М. Скаковський	78	AUTOMATED CONTROL SYSTEM SIMULATION OF SUGAR MASSECUTE BOILING PROCESS IN VACUUM APPARATUS OF PERIODIC ACTION IN THE SOFTWARE ENVIRONMENT OF THE PROGRAMMED CONTROLLER Skakovsky Y.
СИНТЕЗ ТА ДОСЛІДЖЕННЯ АСТАТИЧНИХ ОПТИМАЛЬНИХ ЦИФРОВИХ СИСТЕМ КЕРУВАННЯ РЕКТИФІКАЦІЙНОЮ КОЛОНОЮ А.О. Стопакевич, О.А. Стопакевич	91	SYNTHESIS AND RESEARCH OF AN ASTATIC OPTIMAL DIGITAL CONTROL SYSTEMS OF A DISTILLATION COLUMN Stopakevych A., Stopakevych O.
ДОСЛІДЖЕННЯ МЕТОДУ СТАБІЛІЗАЦІЇ ДИСПЕРСІЇ ВИПАДКОВИХ ВЕЛИЧИН НА ОСНОВІ СТЕПЕНЕВИХ ПЕРЕТВОРЕНЬ ДЛЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ О.О. Фомін, М.М. Масрі, О.А. Туманов, О.В. Сербова, В.В. Ткаченко	104	ANALYSIS OF A METHOD FOR STABILIZING THE VARIANCE OF RANDOM VARIABLES BASED ON POWER TRANSFORMATIONS FOR MACHINE LEARNING MODELS Fomin O., Masri M., Tumanov O., Serbova O., Tkachenko V.
МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ЗА ДАНИМИ АЙТРЕКІНГУ Т.В. Шаманіна, В.Д. Павленко	115	METHOD FOR THE PROTECTION OF INFORMATION IN COMPUTER SYSTEMS ON THE EYE TRACKING DATA Shamanina T., Pavlenko V.
РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ РЕЦЕНЗУВАННЯ СТАТЕЙ ДЛЯ НАУКОВОГО ЖУРНАЛУ Г.О. Шеремет	127	DEVELOPMENT OF ANAUTOMATED ARTICLE REVIEW SYSTEM FOR A SCIENTIFIC JOURNAL Sheremet H.
МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ДИНАМІЧНИХ СТАНІВ ПАРОРІДИННИХ ДВОФАЗНИХ СИСТЕМ С.А. Положаєнко, Д.А. Лись	134	MATHEMATICAL FORMALIZATION OF DYNAMIC STATES OF VAPOR- LIQUID TWO-PHASE SYSTEMS Polozhaenko S., Lys D.

**РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДУ ВБУДОВИ БІНАРНОГО
ЦИФРОВОГО ВОДЯНОГО ЗНАКУ В ЗОБРАЖЕННЯ НА ОСНОВІ
ДИСКРЕТНОГО КОСИНУСНОГО ПЕРЕТВОРЕННЯ****Г.В. Ахматєєва, В.О. Кирилюк**Державний університет «Одеська політехніка»,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: a.v.akhmatieva@opu.ua

В даній роботі запропоновано стеганографічний метод вбудови бінарного цифрового водяного знаку (ЦВЗ) в середньочастотні коефіцієнти дискретного косинусного перетворення (ДКП) цифрового зображення. Для вбудовування ЦВЗ використовується один з середньочастотних коефіцієнтів двох кольорних складових кольорового зображення: одна кольорова складова застосовується для вбудови секретного коефіцієнту, який слугує віддзеркаленням змін в зображенні і сприяє підвищенню якості вилученого цифрового водяного знаку після накладення шумів на стеганоповідомлення. Друга кольорова складова контейнеру використовується для вбудовування самого ЦВЗ. Запропонований метод передбачає автоматичний вибір кольорних складових контейнера для вбудовування ЦВЗ та його попередню обробку для збільшення відстані між його елементами. Стаття містить основні кроки вбудовування і вилучення водяного знаку, а також результати обчислювальних експериментів, спрямованих на оцінку ефективності стеганографічного методу, та порівняння результатів з сучасними аналогами. Ефективність стеганографічного методу оцінюється показником візуальної якості стеганоповідомлень PSNR та різними показниками вилучення повідомлення. Стійкість до атак оцінюється показниками вилучення інформації з модифікованого стеганоповідомлення. В роботі проводиться аналіз розробленого методу при вбудові ЦВЗ в коефіцієнт (5,5) дискретного косинусного перетворення кожного блоку 8×8 цифрового зображення та деякого секретного коефіцієнта, що дорівнює 20. Результати проведених обчислювальних експериментів показали високу візуальну якість отриманих стеганоповідомлень (PSNR становить 50-58 дБ) та стійкість даного методу до шумів, а саме: мультиплікативного, пуасонівського, гаусового та «сіль і перець». У випадку з пуасонівським шумом, цифровий водяний знак видобувається майже без втрат, показники якості вилучення ЦВЗ не були нижчі за 0.97.

Ключові слова: стеганографія, бінарний цифровий водяний знак, дискретне косинусне перетворення, кольорове цифрове зображення

Вступ

В сучасному інформаційно-комунікаційному оточенні, яке охоплює всі сфери людського життя, з проникненням глобальної мережі Інтернет та, як наслідок, різноманітних засобів миттєвого зв'язку зростає необхідність захисту конфіденційних даних, що стосуються людини, організації, держави, та їх інтелектуальної власності, адже за останні роки набули значного поширення інциденти фальсифікації авторства на мультимедійні контенти, такі як аудіо, зображення і відео. Для вирішення проблеми захисту авторських прав в контент, який повинен бути захищений, вбудовують цифрові водяні знаки (ЦВЗ). Основною вимогою до систем вбудови ЦВЗ є стійкість стеганоповідомлень до атак, оскільки часто зловмисники намагаються або видалити наявний ЦВЗ, або підмінити власним, або унеможливити його коректне вилучення.

Серед наукових публікацій за останні роки, присвячених розробці стеганографічних методів, можна помітити тенденцію поєднання різних частотних перетворень, зокрема дискретного косинусного перетворення (ДКП), різновидів вейвлет-перетворення, сингулярного розкладу, тощо – це так звані «гібридні» методи.

У статті [1] наведений метод вбудовування ЦВЗ, стійкий до кількох видів атаки. Запропонована схема водяних знаків базується на ліфтинговому вейвлет-перетворенні (LWT) та розкладанні особливих значень (SVD). Запропонована робота зосереджена на підвищенні стійкості водяних знаків до атак, працюючи в частотній області, і тим самим покращуючи непомітність водяного знаку. За результатами експериментів, наведених в статті, для стеганоповідомлень забезпечується досить висока стійкість до шумів, однак якість стеганоповідомлень залишається невисокою, про що свідчать значення PSNR від 39 до 42 дБ.

У статті [2] алгоритм вбудовування ЦВЗ в контейнер складається з послідовних етапів дискретного вейвлет-перетворення, Z-перетворення, бідіагонального сингулярного розкладання (BSVD) та перетворення Арнольда. Виходячи з результатів, що представлені в статті, можна зробити висновок, що даний алгоритм показав досить високі показники PSNR для стандартних зображень, а саме 68,8925-72,6763 дБ, а при здійсненні різних атак, коефіцієнти кореляції були на високому рівні від 0,97 до 0,99.

В роботі [3] представлений спосіб вбудовування подвійного ЦВЗ з метою, щоб у разі виявлення першого водяного знаку зломисником та подальшого його видалення, можна було за допомогою другого підтвердити авторські права та, як наслідок, звести старання зломисника нанівець. Запропонований метод заснований на поєднанні гомоморфічного перетворення, дискретного вейвлет-перетворення, SVD та перетворення Арнольда і забезпечує високу якість стеганоповідомлень (PSNR 59.1692-60.2320 дБ) та високу стійкість до атак (показники вилучення ЦВЗ наближені до 1).

Як правило, «гібридні» стеганографічні методи забезпечують високу якість стеганоповідомлень і стійкість до атак [4], але основним їх недоліком є висока обчислювальна складність, що обумовлено використанням декількох видів частотних перетворень. Ті ж методи, які застосовують лише один вид частотного перетворення, здебільшого не дають високої якості стеганоповідомлень при забезпеченні стійкості до деяких видів атак.

Зокрема, в статті [5] запропоновано вбудовувати два однакові ЦВЗ в коефіцієнти ДКП. За результатами експериментів, наведених в статті, можна зробити висновок, що даний метод є досить стійким до атак (показники вилучення інформації після атаки Гаусовим шумом становлять 0.9693-1), PSNR стеганоповідомлень становить 45.6513-47.6637 дБ, що для зображень в градаціях сірого є гарним результатом.

Ті методи, які засновані лише на використанні ДКП для кольорових зображень, [6, 7] забезпечують досить низьку якість стеганоповідомлень, виключенням є робота [8], в якій значення PSNR досягають 55 дБ.

Мета і задачі дослідження

Метою роботи є підвищення якості стеганоповідомлень шляхом розробки нового методу вбудови ЦВЗ в область ДКП цифрового зображення.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. розробити метод вбудови ЦВЗ на основі дискретного косинусного перетворення;
2. проаналізувати результати якості стеганоповідомлень і видобутку ЦВЗ для запропонованого стеганографічного методу;
3. провести оцінку ефективності розробленого методу і порівняння його з аналогами.

Основна частина

В статті пропонується блочний метод вбудови бінарного ЦВЗ в область дискретного косинусного перетворення кольорових цифрових зображень. Вбудовування біту ЦВЗ відбувається в середньочастотний коефіцієнт ДКП блоку 8×8

зображення шляхом заміни обраного коефіцієнту $d_{a,b}$ значенням $dw_{i,j} \cdot k$, де $dw_{i,j}$ - біт ЦВЗ, k - коефіцієнт, обчислений для певного зображення. Особливістю даного методу є подвійне вбудовування ЦВЗ в контейнер, що дозволяє підвищити якість вилученого ЦВЗ. Це обумовлено тим, що переведення модифікованих коефіцієнтів ДКП блоку в просторову область впливає на якість вилучення ЦВЗ в тому сенсі, що приховані значення дещо змінені (спотворені), але наближені до дійсних. Повторне вбудовування ЦВЗ у вже модифікований контейнер дозволяє отримати вбудований ЦВЗ майже без помилок, і підвищити стійкість стеганоповідомлення до атак зашумленням, що підтверджують результати обчислювальних експериментів.

Основні кроки запропонованого методу наведені нижче.

Вбудовування ЦВЗ

Для цифрового зображення в C розміром $m \times n \times 3$ і бінарного ЦВЗ dw розміром $h \times w$, при $m > 8h$, $n > 8w$ виконати наступне.

Крок 1. Попередня обробка ЦВЗ.

Модифікувати ЦВЗ за формулою:

$$dw_{i,j}' = dw_{i,j} \cdot 8 + 1,$$

де $dw_{i,j}$ і $dw_{i,j}'$ - значення (i, j) -го пікселя оригінального і модифікованого ЦВЗ відповідно.

Крок 2. Визначення кольірних складових контейнера для вбудовування ЦВЗ.

2.1. Для блоків розміром 8×8 кольірної складової I , $I \in \{R, G, B\}$ обчислити ДКП.

2.2. Знайти середнє значення всіх коефіцієнтів (a, b) ДКП блоків кольірної складової I . Результат av^R, av^G, av^B .

2.3. Обрати для вбудови ЦВЗ кольірну складову $I^{\max}$ з максимальним значенням серед av^R, av^G, av^B .

2.4. Обрати для вбудови значення $20 \cdot k$ матрицю I^{middle} з середнім по порядку значенням серед av^R, av^G, av^B . Оскільки коефіцієнт k є постійним для обраного зображення, має сенс вбудувати його лише в декілька блоків зображення, вибір яких може бути довільним.

Крок 3. Обчислити значення коефіцієнту k :

$$k = \begin{cases} \frac{\text{mean}(av^{I^{\max}})}{\text{mean}(dw')}, & \text{якщо } \text{mean}(av^{I^{\max}}) \geq \text{mean}(av^{I^{\text{middle}}}) + 2, \\ \frac{\text{mean}(av^{I^{\text{middle}}}) + 2}{\text{mean}(dw')}, & \text{якщо } \text{mean}(av^{I^{\max}}) < \text{mean}(av^{I^{\text{middle}}}) + 2, \\ 1, & \text{якщо } \text{mean}(av^{I^{\max}}) < \text{mean}(dw'), \end{cases}$$

де $\text{mean}(dw')$ - середнє значення модифікованого ЦВЗ.

Крок 4. Вбудовувати значення $20 \cdot k$ в коефіцієнти ДКП (a, b) декількох блоків колірної складової I^{middle} за формулою:

$$d_{a,b}^{middle} = 20k,$$

де $d_{a,b}^{middle}$ - (a, b) -ий коефіцієнт ДКП блоку колірної складової I^{middle} .

Крок 5. Обчислити зворотне ДКП обраних блоків колірної складової I^{middle} . Округлити отримані значення яскравості блоків до цілих чисел в діапазоні від 0 до 255.

Крок 6. Вбудовування ЦВЗ.

Для блоків розміром 8×8 колірної складової I^{max} :

5.1. Обчислити ДКП, результат d^{max} .

5.2. Вбудовувати (i, j) -ий біт ЦВЗ в коефіцієнт (a, b) ДКП блоку за формулою:

$$d_{a,b}^{max'} = \begin{cases} -dw_{i,j}' \cdot k, & \text{якщо } d_{a,b}^{max} < 0, \\ dw_{i,j}' \cdot k, & \text{якщо } d_{a,b}^{max} \geq 0, \end{cases}$$

де $d_{a,b}^{max}$ - (a, b) -ий коефіцієнт ДКП блоку зображення.

5.3. Обчислити зворотне ДКП блоку колірної складової I^{max} . Округлити отримані значення яскравості блоків до цілих чисел в діапазоні від 0 до 255.

Крок 7. Сформулювати нове стеганоповідомлення S .

Крок 8. Повторити кроки 4-7 для зображення S , використовуючи коефіцієнт k , обчислений в кроці 3, та обрані в кроці 2 колірні складові I^{max} і I^{middle} .

Видобування ЦВЗ

Для цифрового зображення в S розміром $m \times n \times 3$ виконати наступне.

Крок 1. Визначення колірних складових контейнера для вилучення ЦВЗ.

1.1. Для блоків розміром 8×8 колірної складової I , $I \in \{R, G, B\}$ обчислити ДКП.

1.2. Знайти середнє значення всіх коефіцієнтів (a, b) ДКП блоків колірної складової I . Результат av^R, av^G, av^B .

1.3. Обрати для вилучення ЦВЗ колірну складову I^{max} з максимальним значенням серед av^R, av^G, av^B .

1.4. Обрати для вилучення значення k матрицю I^{middle} з середнім по порядку значенням серед av^R, av^G, av^B .

Крок 2. Видобування значення k з коефіцієнтів ДКП (a, b) декількох блоків колірної складової I^{middle} з подальшим знаходженням їх середнього арифметичного.

Крок 3. Вилучення ЦВЗ.

Для блоків розміром 8×8 колірної складової I^{max} :

3.1. Обчислити ДКП, результат d^{max} .

3.2. Вилучити біт ЦВЗ з коефіцієнту (a, b) ДКП блоку за формулою

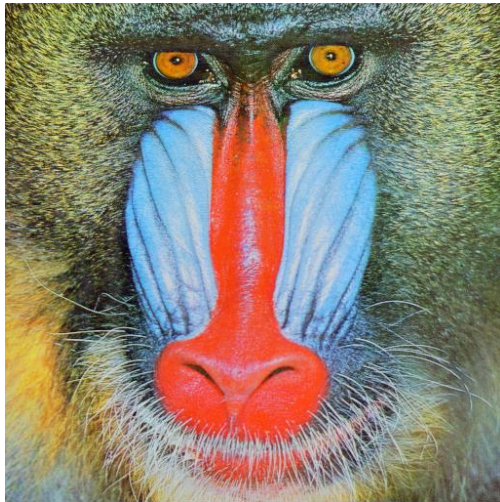
$$dw'_{ij} = \left| \frac{d_{a,b}' \cdot 20}{k} \right|.$$

3.3. Отримане значення відкоригувати у відповідності до формули:

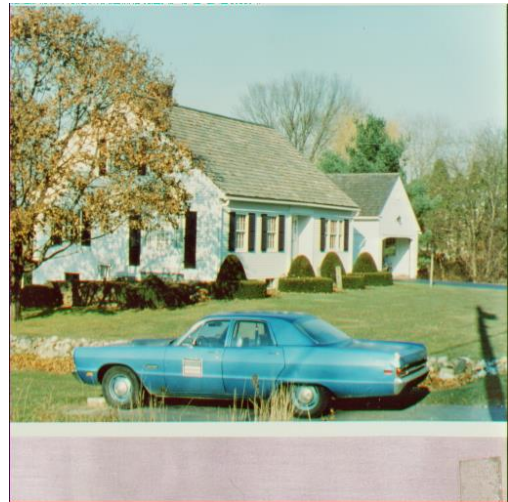
$$dw''_{i,j} = \begin{cases} 1, & \text{якщо } dw'_{i,j} > 4.5, \\ 0, & \text{якщо } dw'_{i,j} \leq 4.5, \\ 0, & \text{якщо } dw'_{i,j} = NaN. \end{cases}$$

Крок 4. Сформувати вихідний ЦВЗ.

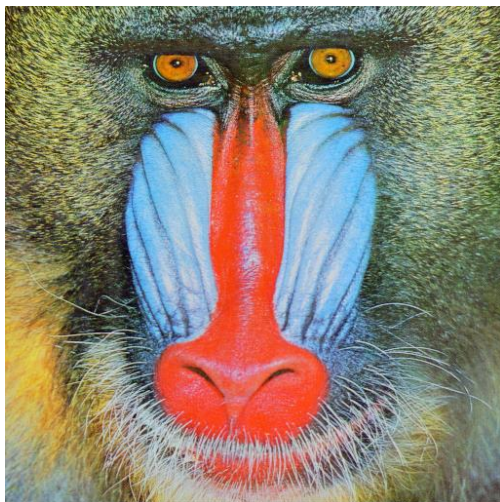
Для оцінки ефективності запропонованого методу був проведений обчислювальний експеримент на основі 200 цифрових зображень, та кількох ЦВЗ. Приклад вбудови та вилучення ЦВЗ в стандартні зображення показаний на рис.1.



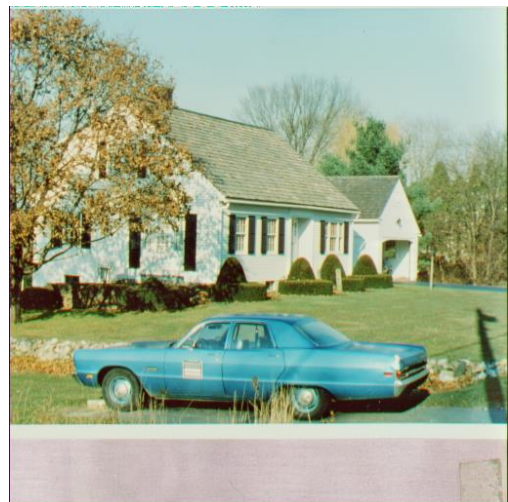
а



б



в



г



Рис. 1. Приклад вбудови ЦВЗ в зображення: а, б – оригінальні контейнери; в, г – стеганоповідомлення, отримані вбудовою ЦВЗ в контейнери; д, е – вилучені ЦВЗ з стеганоповідомлень в і г відповідно.

Якість отриманих стеганоповідомлень будемо оцінювати показниками MSE і PSNR, якість вилучення ЦВЗ з стеганоповідомлення показниками Р [9], NCC [10], NC [11], BCR [12], SIM [13], що обумовлено використанням різними авторами різних показників, які обчислюються за формулами:

$$P = \frac{\text{Кількість біт ЦВЗ, вилучених вірно}}{L},$$

$$NCC = \frac{\sum_{i=1}^L p_i' \times \overline{p_i'}}{L},$$

де p_i - біти вбудованого ЦВЗ, $\overline{p_i}$ - біти вилученого ЦВЗ, $p_i, \overline{p_i} \in \{0,1\}, i = \overline{1, L}$; $p_i' = 1$, якщо $p_i = 1$, і $p_i' = -1$, якщо $p_i = 0$; $\overline{p_i'} = 1$, якщо $\overline{p_i} = 1$, і $\overline{p_i'} = -1$, якщо $\overline{p_i} = 0$, тобто $p_i' \times \overline{p_i'} \in \{-1, 1\}$.

$$NC = \frac{\sum_{l=0}^{L-1} dw_l \cdot dw_l'}{\sum_{l=0}^{L-1} dw_l^2}, \quad SIM = \frac{\sum_{l=0}^{L-1} dw_l \cdot dw_l'}{\sqrt{\sum_{l=0}^{L-1} dw_l^2} \cdot \sqrt{\sum_{l=0}^{L-1} dw_l'^2}}, \quad BCR = \frac{1}{L} \sum_{l=0}^{L-1} \overline{dw_l \oplus dw_l'},$$

де dw_l - l -ий біт вбудованого ЦВЗ довжиною L , dw_l' - l -ий біт вилученого ЦВЗ, $\oplus$ - операція XOR.

Результати експериментів для зображень в умовах відсутності атак та атак накладання шумів продемонстровані в таблиці 1, де остання колонка «СЗ ПВІ» означає середнє значення показників вилучення інформації, тобто середнє значення показників Р, NCC, NC, BCR, SIM.

З таблиці 1 видно, що для запропонованого методу характерна досить висока стійкість до атак накладання шумів, зокрема метод є майже нечутливим до накладання Пуассонівського шуму – всі показники вилучення ЦВЗ наближені до 1. Для Гауссівського, мультиплікативного, «сіть & перець» шумів якість вилучення залежить від дисперсії шуму (чим менше дисперсія – тим менше помилок вилучення ЦВЗ), однак навіть для дисперсії 0.001 забезпечуються достатньо надійне вилучення ЦВЗ – середні значення показників вилучення інформації перевищують 0.92 за виключенням Гауссівського шуму, однак і в цьому випадку середнє значення наближене до 0.9.

Таблиця 1.

Ефективність методу вбудови ЦВЗ в кольорові зображення

	PSNR, дБ	NCC	BCR	SIM	NC	P	СЗ ПВІ
Оригінальні стеганоповідомлення	52.285	0.998	0.999	0.995	0.999	0.999	0.9983
Гаусів шум, $m = 0, d = 0.0001$	39.437	0.988	0.994	0.961	0.969	0.994	0.9811
Гаусів шум, $m = 0, d = 0.0005$	41.856	0.977	0.988	0.925	0.938	0.988	0.9632
Гаусів шум, $m = 0, d = 0.001$	29.741	0.918	0.959	0.742	0.780	0.959	0.8718
Пуасонівський шум	52.296	0.998	0.999	0.995	0.999	0.999	0.9983
«Сіль & перець», $d = 0.001$	34.590	0.982	0.991	0.949	0.986	0.991	0.9797
«Сіль & перець», $d = 0.005$	27.662	0.965	0.982	0.890	0.938	0.982	0.9515
«Сіль & перець», $d = 0.01$	24.712	0.943	0.971	0.827	0.897	0.971	0.9219
Мультиплікативний шум, $d = 0.0001$	43.669	0.998	0.999	0.994	0.998	0.999	0.9975
Мультиплікативний шум, $d = 0.0005$	37.357	0.968	0.984	0.908	0.954	0.984	0.9595
Мультиплікативний шум, $d = 0.001$	34.455	0.949	0.974	0.850	0.909	0.974	0.9313

Для порівняння якості стеганоповідомлень для запропонованого методу та сучасних аналогів будемо використовувати показник PSNR. Однак слід зазначити, що в статтях різних авторів використовуються різні формули для обчислення MSE або PSNR, що позначається на результатах. Саме тому для коректного порівняння з аналогами будемо обчислювати показники MSE та PSNR за тими формулами, що наводяться в статтях. Якщо в статті формула не наведена, будемо вважати, що використовується стандартне обчислення цих показників:

$$MSE = \frac{1}{XY} \sum (C_{x,y} - S_{x,y})^2, \quad PSNR = 10 \cdot \lg \left(\frac{(\max C_{x,y})^2}{MSE} \right). \quad (1)$$

Інші нестандартні, але розповсюджені формули обчислення MSE і PSNR наступні:

$$MSE = \frac{1}{XY} \sum (C_{x,y} - S_{x,y})^2, \quad PSNR = 10 \cdot \lg \left(\frac{256^2}{MSE} \right); \quad (2)$$

$$MSE = \frac{1}{(XY)^2} \sum (C_{x,y} - S_{x,y})^2, \quad PSNR = 10 \cdot \lg \left(\frac{255^2}{MSE} \right). \quad (3)$$

В таблиці 2 наведені показники PSNR, обчислені на основі формул (1)-(3) для стандартних зображень. Оскільки в літературних джерелах, взятих для порівняння, обчислювальні експерименти застосовують не всі розглянуті зображення, а й інші, в таблиці 3 наводиться порівняння середніх значень PSNR для результатів експериментів запропонованого методу і сучасних аналогів.

Таблиця 2.

Порівняння показників PSNR запропонованого методу і сучасних аналогів для стандартних зображень

Зображення	PSNR (1), дБ		PSNR (2), дБ		PSNR (3), дБ	
	[6], 2018	Запропон. метод	[8], 2019	Запропон. метод	[7], 2016	Запропон. метод
Airplane	-	54.2871	55.56	59.0923	-	108.4825
Baboon	-	45.3975	51.22	50.2027	-	99.5829
House	-	53.7728	-	58.5810	-	107.9612
Lena	41.36	53.3097	-	58.1149	32.15	107.4951
Peppers	-	54.24	-	59.0452	-	108.4254
Pot	-	54.8241	-	59.6293	-	109.0095
Sailboat	-	51.4517	-	56.2569	-	105.6371

Таблиця 3.

Порівняння середніх значень PSNR експериментів сучасних аналогів і запропонованого методу

	PSNR (1), дБ		PSNR (2), дБ		PSNR (3), дБ
[1], 2018	41.29	[2], 2019	55.1635	[3], 2016	34.7833
Запропонований метод	52.469	Запропонований метод	57.2746	Запропонований метод	106.6562

Як видно з таблиць 2 і 3, показники PSNR, отримані для запропонованого методу, набагато перевищують показники візуальної якості сучасних аналогів.

Висновки

В роботі розроблений стеганографічний метод вбудови бінарного ЦВЗ в область дискретного косинусного перетворення цифрового зображення. З метою покращення видобутку ЦВЗ при його вбудові, запропоновано комплекс операцій, завдяки яким вдається показати хороші результати при вилученні ЦВЗ, та зберегти досить високу візуальну якість стеганоповідомлень.

В ході проведення обчислювальних експериментів, спрямованих на оцінку ефективності запропонованого методу, було виявлено його високу стійкість до атак накладання шумів, зокрема до Пуасонівського шуму – вилучення ЦВЗ відбувається майже без помилок. Досить надійне вилучення інформації відбувається і при накладанні Гаусового, мультиплікативного, «сіль & перець» шумів з дисперсією 0.001 – показники вилучення в середньому наближені до 0.9, що також є гарним результатом.

Список літератури

1. Manasha Saqib, Sameena Naaz. An Improvement in Digital Image Watermarking Scheme Based on Singular Value Decomposition and Wavelet Transform. *Asian Journal of Computer Science and Technology*. 2019. Vol. 8, No. 1. P. 62-68.
2. Jayashree N., Bhuvaneswaran R.S. A Robust Image Watermarking Scheme Using Z-Transform, Discrete Wavelet Transform and Bidiagonal Singular Value Decomposition. *CMC-Tech Science Press*. 2019. Volume 58, No. 1. P. 263-285.
3. Priyank Khare, Vinay Kumar Srivastava. A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT. *Journal of Intelligent Systems*. 2021. Vol. 30, No. 1. P. 297-311.
4. Mahbuba Begum, Mohammad Shorif Uddin. Analysis of Digital Image Watermarking Techniques through Hybrid Methods, *Advances in Multimedia*. 2020. Volume 2020. P. 1-12.
5. Sunesh R. Rama Kishore. A Novel and Efficient Blind Image Watermarking in Transform Domain. *Procedia Computer Science*. 2020. No. 167. P. 1505-1514.
6. Rand A. Watheq, Fadi Almasalha, Mahmoud H. Qutqut. A New Steganography Technique using JPEG Images. *International Journal of Advanced Computer Science and Applications*. 2018. Vol. 9, No. 11. P. 751-760.
7. Iman M.G. Alwan, Farah Jasim Mohammed. Image Hiding Using Discrete Cosine Transform. *J. Of College Of Education For Women*. 2016. Vol. 27 (1). P. 393-399.
8. Osama F. Abdel Wahab, Aziza I. Hussein, Hesham F.A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf, Hanafy M. Ali. Hiding data in images using steganography techniques with compression algorithms. *TELKOMNIKA*. 2019. Vol. 17, No. 3. P. 1168-1175.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев: «МК-Пресс», 2006. 288 с.
10. Мельник М.А. Методика оценки устойчивости стеганоалгоритма к сжатию. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2013. Вип. 44. С. 121-128.
11. Melad J. Saeed. A new technique based on chaotic steganography and encryption text in DCT domain for color image. *Journal of Engineering Science and Technology*. 2013. Vol. 8, No. 5. P. 508-520.
12. Benoraira A., Benmahammed K., Boucenna N. Blind image watermarking technique based on differential embedding in DWT and DCT domains. *EURASIP Journal on Advances in Signal Processing*. 2017. No. 55. P. 1-11.
13. Jabbar K., Tuieb B. Compare Between DCT and DWT for Digital Watermarking in Color Image. *Information and Knowledge Management*. 2015. No. 5 (7). P. 22-31.

**DEVELOPMENT OF STEGANOGRAPHICAL METHOD OF BINARY DIGITAL
WATER MARK INSERT INTO IMAGE BASED ON DISCRETE
COSINUS TRANSFORMATION**

A.V. Akhmamatieva, V.O. Kyryliuk

State University «Odessa Polytechnic»

This paper describes a steganographic method of embedding a binary digital watermark into the mid-frequency coefficients of discrete cosine transform of a digital image. One of the mid-frequency coefficients of the two-color components of a color image is used to embed the digital watermark: one color component is used to embed a secret coefficient which reflects changes in the image and helps to improve the quality of the extracted digital watermark after applying noise to the stego. The second color component of the container is used for embedding of the digital watermark. The proposed method involves the automatic selection of color components of the container for embedding the digital watermark and its pre-processing to increase the distance between its elements. The article contains the main steps of embedding and extracting of a digital watermark, as well as the results of computational experiments aimed at evaluating the efficiency of the steganographic method, and comparing the results with modern analogues. The efficiency of the steganographic method is evaluated by the indicator of visual quality PSNR of stego and various indicators of message extraction. Resistance to attacks is evaluated by indicators of extraction of information from the modified stego. The paper analyzes the developed method when embedding some secret coefficient equal to 20 and the digital watermark into the coefficient (5.5) of the discrete cosine transform of each 8×8 block of digital image is carried out. The results of computational experiments showed the high visual quality of the received stegan messages (PSNR is 50-58 dB) and the resistance of this method to noise, namely: multiplicative, Poisson, Gaussian and "salt and pepper". In the case of Poisson noise, the digital watermark is extracted almost without loss, the quality of extraction of the digital watermark was not lower than 0.97.

Keywords: steganography, binary digital watermark, Discrete cosine transformation, color digital image.

**УПРАВЛІННЯ КОНФЛІКТАМИ ТА ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ В МЕРЕЖІ INTERNET****В.О. Хорошко¹, М.М. Браїловський²**¹Національний авіаційний університет, просп. Любомира Гузера, 1,
Київ, 03058, Україна; e-mail: professor_va@ukr.net²Київський національний університет імені Тараса Шевченка,
вул. Богдана Гаврилишина, 24, Київ, 04116 Україна, e-mail: bk1972@ukr.net

У статті розглядається проблема підвищення ефективності управління конфліктами і інцидентами інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах, що функціонують на базі мережі Internet. Метою даного дослідження є пропозиція підходу до управління інцидентами і конфліктами інформаційної безпеки в мережах Internet, побудованого за принципом біоаналогів на базі штучних імунних систем. Проведений аналіз показує, що сучасні інфокомунікаційні та інформаційно-технічні системи, що функціонують на базі Internet, налічують тисячі суб'єктів, при цьому, визначальним фактором їх існування і розвитку є наявність захищеної системи обміну інформацією і системою управління конфліктами і інцидентами інформаційної безпеки. Результатами проведених дослідження є: запропонований, логічно обґрунтований і математично формалізований імунний підхід до інтелектуального управління конфліктами і інцидентами інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах, що функціонують на базі Internet; побудована узагальнена модель управління конфліктами і інцидентами, виділення цільових показників імунної системи; обґрунтований підхід з використанням узагальненої моделі управління конфліктами і інцидентами. Показана практична доцільність і прикладне значення отриманих результатів на прикладі застосування прототипу структури і функцій імунної системи управління конфліктами і інцидентами інформаційної безпеки на базі агентно-орієнтованого підходу до побудови розподілених систем. Даний підхід забезпечує динамічне адаптивне управління при виникненні нових конфліктів та інцидентів. Застосування прототипу штучних імунних систем в автоматизації та інтелектуалізації управління конфліктами і інцидентами інформаційної безпеки може дозволити досягти якісно нового рівня забезпечення та управління інформаційної безпеки в інфокомунікаційних та інформаційно-технічних системах, що функціонують на базі Internet. Крім того, в статті для оцінки функціональної безпеки Internet виділені фактори, які найбільшим чином визначають уразливість Internet.

Ключові слова: моделі управління конфліктами і інцидентами, інформаційна безпека, інформаційні системи, імунна система, біоаналогів.

Вступ

Найважливішою проблемою, що визначає темпи і майбутній розвиток Internet, стає інформаційна безпека (ІБ). Глибоке проникнення комп'ютерних інформаційних технологій (ІТ), інфокомунікаційних технологій (ІКТ), Internet в усі сфери людської діяльності і проблеми в їх захисті вимагають ширшого впровадження технологій інформаційного захисту. Вже сьогодні ІТ є тією «нервовою системою», кожної розвиненої держави в світі, яка дозволяє функціонувати іншим його підсистем. А ядром всієї інформаційної інфраструктури стала мережа Internet. В даний час мережа Internet об'єднує мільйони користувачів по всьому світі. Ці комп'ютери контролюють реальні фізичні об'єкти різного, парю критичного, типу. Таким чином, ІТ, ІКТ та Internet

стають критичними інформаційними технологіями, здатними впливати на національну безпеку держави і світу в цілому [1].

Слід враховувати, що глобальний розвиток інформаційних технологій в світі несе не тільки позитивний ефект. Їх зростання і застосування тягне за собою загрози не тільки інформаційної безпеки людей, а й істотно впливає на еволюційний розвиток людства в цілому, в тому числі і негативне. З'явилися і прогресують нові поняття в сфері безпеки. Це кіберзлочинність та кібербезпека, вірусна активність, несанкціонований доступ до інформації і кібершпиунство, інформаційні та гібридні війни.

Відчутним прояви проблеми ІБ є факт наявності зареєстрованих і виникнення нових інцидентів і конфліктів. Причому, спостережуване протягом багатьох років зростання числа інцидентів і конфліктів ІБ [2], змушує замислитися про пошук нових, кардинальних більш ефективних і, можливо, нестандартних шляхів вирішення завдання управління інцидент і конфліктами ІБ.

Це вплив ІТ, ІКТ та Internet на життя людей при збільшенні нових варіантів загроз безпеці змушує задуматися про перспективи і джерелах їх появи. Уявлення про те, що ІТ, ІКТ та Internet - породження людини, а не природи, і тому має повністю перебувати під управлінням людини, не витримує критики. Ці об'єкти сьогодні представляють собою по розмірності величезні і швидко зростаючі новоутворення, які до сих пір не зустрічалися в еволюції людини. Вони впливають на життя людей і в позитивному і негативному аспекті.

Позитивні прогнози розвитку ІТ, ІКТ та Internet в основному виходять від банкірів і фінансистів, що базуються на надіях зростання фінансового прибутку. Ряд негативних прогнозів лунають із боку фахівців в галузі ІТ і захисту інформації.

Всі ці прогнози [3] базуються на основі статистичі відносно не довготривалої історії розвитку ІТ і Internet і не враховують систему популяційної складової, яка важливіша для еволюції людства в цілому.

Розвиток і еволюція інформаційної системи Internet можна порівняти з розвитком природного інформаційної імунною системою людини, яка за кількісними параметрами поки перевершує параметри розвитку ІТ і Internet.

Однак темпи зростання Internet і його вплив на еволюцію популяції людини змушують аналізувати і прогнозувати його розвиток на основі цієї аналогії.

Для оцінки впливу Internet на розвиток і еволюцію людини слід проаналізувати і порівняти кількісні характеристики еволюції інформаційних систем.

Вивчення і прогнозування розвитку Internet з позиції розвитку людства найбільш перспективне і корисно і для Internet, і для людства в цілому. Такий аналіз показує, що подальший розвиток Internet базується, в першу чергу, на організації механізмів і технологій захисту і безпеки інформації (імунології ІТ) і впровадження нових видів обміну інформацією, що відрізняються від існуючих достовірністю і якістю.

Хоча в слідстві деяких прогалин в розумінні механізмів імунної відповіді і міжклітинних взаємодій на сьогодні відсутня єдина теорія імунітету, проте теоретичні передумови біофізичних і медичних досліджень послужили поштовхом до виникнення нового напрямку в інформатиці –іммунокомп'ютернінга. Це дало можливість синтезувати прототипи штучних імунних систем (ШИС) для практичних застосувань [4].

Одним з активно досліджуваних програм ШИС є захист інформації, де природна імунна система (ІС) розглядається як джерело ідей і методів вирішення завдань ІБ. Спираючись на [5] та зробивши пошук по ряду наукових порталів Internet, на сьогодні можна виділити два загальних напрямки дослідження ШИС для ІБ:

1) імунні системи виявлення вторгнень, на базі алгоритму негативного відбору;

2) імунні системи розпізнавання нових комп'ютерних вірусів.

Однак невирішеними залишаються питання застосування імунного підходу для автоматизації та інтелектуалізації процесів управління інцидентами і конфліктами ІБ.

Мета роботи

Метою даного дослідження є пропозиція підходу до управління інцидентами і конфліктами ІБ в мережах Internet, побудованого за принципом біоаналогів на базі ІПС.

Основна частина

Internet - розрахований на багато користувачів (багатосуб'єктовий) комплекс програм, в якому існують користувачі і групи користувачів, які конкурують в частині досягнення своїх цілей, іноді суперечать цілям інших користувачів або їх груп. Частина користувачів переслідує зловмисні цілі з несанкціонованого доступу до інформації інших користувачів, що призводить до виникнення інцидентів і конфліктів.

Постійно мінливий склад програм в Internet і збільшення кількості користувачів функціонування Internet призводить до того, що неможливо передбачити заздалегідь якість функціонування, і вірогідні різні аномалії, що завершуються відмовами, які відбиваються на безпеці і виникненню конфліктів та інцидентів. Необхідно визнати принципові труднощі аналітичного оцінювання і прогнозування значень функціональної безпеки Internet внаслідок непередбачуваності прояви і наслідки загроз безпеки. Це призводить до практичної неможливості досягнення апріорних аналітичних розрахунків функціональної безпеки Internet [6,7].

Безпека Internet в більшості випадків визначається не тільки факторами заподіяння шкоди користувачу і виникненню конфліктів та інцидентів, а й можливістю реалізації цих факторів, тобто загрозами безпеці.

Загрози безпеці з точки зору використовуваних програмних продуктів визначаються їх вразливістю - наявністю в їх конструктивній реалізації місць і можливостей реалізації загроз безпеки [1,8].

Число атак несанкціонованого доступу прогнозується не менше ніж по одній атаці на комп'ютер в мережі на день. Не кожна атака призводить до її реалізації, але при планомірному дослідженні обраного для атаки в мережі Internet комп'ютера кожна невдала атака призводить до наближення до очікуваної мети, тобто до збільшення ймовірності несанкціонованого доступу.

Будь-яка атака, яка діє в мережі Internet, на кожному з наявних у розпорядженні системи захисту інформації (СЗІ) та засобів захисту відіб'ється по-різному: деякі з засобів можуть бути зруйновані повністю; деякі частково виведені з ладу, а для якихось вона виявиться безпечною. Облік цих відмінностей в результатах при запобіганні впливу атаки на засоби захисту та мережі є важливим під час моделювання будь-якої мережі і СЗІ, а також при встановленні стійкості СЗІ та ІБ [9].

Розвивається «некласичний» підхід в теорії управління, що ґрунтується на аналогіях архітектури та цілей функціонування складних технічних і біологічних систем - природних систем управління є найбільш перспективним на сьогоднішній день при формалізації інформаційних систем і мереж. У зв'язку з цим в якості базису для створення принципово нової універсальної моделі мережі були обрані основні принципи функціонування імунної системи людини [9].

Згідно [10] все біологічні системи на рівні клітин і молекул можуть розглядатися як системи обробки інформації. Але тільки нервова і імунна системи мають виняткові здібності до інтелектуальної обробки інформації, включаючи механізми розпізнавання,

ідентифікації, прийняття рішень в умовах невизначеності, навчання і асоціативної пам'яті [5].

ІС являє собою високо паралельну розподілену децентралізовану систему тимчасових колективів клітин [11], здатну до адаптивної інтелектуальної обробки інформації [4]. На даному етапі дослідження обмежимося лише розглядом основних здатностей ІС [4]: розпізнавати своїх або чужих серед величезної кількості молекулярних структур - антигенів з подальшою їх класифікацією і стимуляцією відповідних захисних механізмів. При цьому результатом розпізнавання є навчання і формування пам'яті до антигену. Знання про подібний антиген використовується при реакції на нові інфекції. Так ІС створює, вдосконалює і використовує знання про навколишній світ. Реакція на антиген може відбуватися не тільки на рівні окремих розпізнавальних одиниць, а й на громадському рівні (в залежності від рівня серйозності і способу проникнення інформації [11]). Локальні взаємодії визначають і реалізують глобальну імунну (нервову) реакцію, що в сукупності з безперервною мінливістю і адаптивністю імунної пам'яті по частоті і силі антигенних сигналів, є прикладом ефективного захисту при обмежених ресурсах.

Виходячи зі сказаного, визначимо аналогію функцій природної ІС з основними функціями, які повинна виконувати система управління конфліктами і інцидентами ІБ в мережі Internet:

- реєстрація, виявлення та оцінка серйозності подій, що мають ознаки інциденту і конфлікту, на різних стадіях їх реалізації, збору доказів для подальшого розслідування;
- ідентифікація конфліктності або інцидентства на основі оперативного аналізу доказів, прийняття рішення в умовах неповної визначеності наявної інформацією і, при необхідності, генерації сигналу тривоги;
- обробка і усунення наслідків інциденту або конфлікту шляхом введення в дію відповідних ресурсів безпеки.

Міждисциплінарний підхід до вирішення завдання управління конфліктами і інцидентами ІБ обґрунтовуємо методом індукції через зіставлення та узагальнення фактів виникнення інцидентів і конфліктів інформаційних процесів, які мають місце в системах самої різної природи від інфокомунікаційних та інформаційно-технічних (ІТС), які є складовою частиною Internet, і до біологічних [8-11].

Тому, іммунокомп'ютерінг стосовно до управління інцидентами і конфліктами ІБ в ІКС і ІТС, які функціонують на базі Internet, реалізуються з урахуванням постулатів еволюційної теорії [12]:

- доцільність: «виживають» лише ті ІКС і ІТС (елементи Internet), які найбільшою мірою відповідають ситуації, тобто пристосовуються до інцидентів і конфліктів;
- адаптація: архітектура комплексної системи інформаційної безпеки повинна дозволити динамічно адаптуватися до нових конфліктів і інцидентів, а також до зовнішніх атак;
- самоорганізація: процес еволюції ІКС/ІТС (елементи Internet) призводить до безперервного вдосконалення її структури в зв'язку з перерозподілом ресурсів.

Розглянемо міждисциплінарну декомпозицію властивості безпеки абстрактної системи і взаємопов'язаних з нею понять, а також процесів управління і обробки конфліктів та інцидентів для наступних типів (рівнів) систем: біологічних, ІКС, ІТС та елементів Internet. Завдання управління конфліктами і інцидентами в абстрактній системі є недостатньо формалізованою і невизначеною з точки зору генної структури організації систем і мереж через недостатню розробку більш загальної (в порівнянні з класичною) теорії систем.

Так як кожна ІКС і ІТС включає підсистему ІБ, то математична модель необхідна також для управління інцидентами і конфліктами із залученням сучасного апарату теорії моделювання і складних систем [13,14], а також процесу відбиття атак.

Тепер розглянемо аналогію архітектури та цілей функціонування імунної системи людини з мережею Internet включаючи СЗІ.

При цьому використання імунної системи людини для моделювання ІКС і ІТС (елементів Internet) впливає з очевидною аналогією між обраною біологічною системою і системою ІБ. Слід враховувати, що процес моделювання тут носить комплексний характер і використовує імунну систему, починаючи з форми представлення інформації, програмування інформаційного простору і закінчуючи архітектурою елементів Internet (ІКС і ІТС) з вбудованими механізмами забезпечення ІБ і еволюційного перебігу процесів [9].

Моделювання захищених інформаційних процесів засноване на єдності подання інформації в ієрархії ІС, в якому повідомлення представляється певним структурним інформаційним полем ДНК. Структурований характер мають розподілене інформаційний простір нейронних комплексів ІС, завдяки яким в ІС існує адаптивні механізми пам'яті, які накопичують життєвий досвід. Можливість реалізації адаптивних механізмів пам'яті в штучному інформаційному просторі - основна передумова еволюції Internet. Програмування в ІС носить надлишковий розподілений характер, що забезпечує високу функціональну стійкість інформаційних процесів.

Окремі спотворення інформації, з одного боку, компенсують надмірність інформаційного простору, а з іншого - дозволяють реалізувати механізм мутацій і еволюційні процеси розвитку і відбору. Адаптивні процеси в інформаційному просторі дозволяють Internet розвиватися і накопичувати досвід в умовах розширення загроз, а успадкування досвіду в наступних реалізаціях мережі і системи зводиться до передачі відповідних інформаційних просторів. Ієрархія адаптивної системи ІБ відображає поділ функцій захисту на керуючу і керовану реалізовує взаємодії системи з середовищем (рис.1) [9]. Архітектурною особливістю ІС є внутрішній характер механізмів захисту, що реалізується в ієрархії елементів Internet.

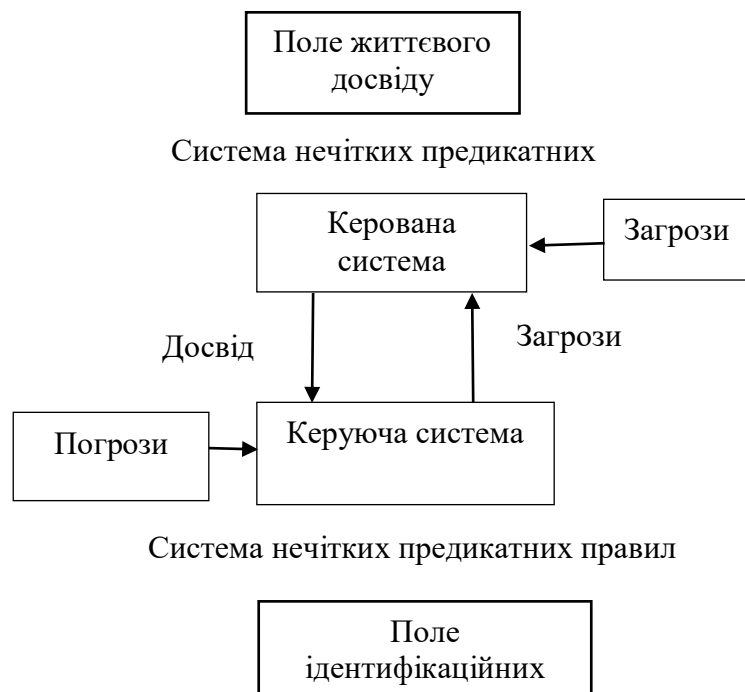


Рис. 1. Ієрархія адаптивної системи ІБ.

При моделюванні штучних систем слід враховувати, що при реалізації адаптивних механізмів ІС та інформаційного простору її функції захисту інформації повинні бути внутрішніми функціями системи.

На основі проведених досліджень приступаємо до розробки узагальненої моделі управління конфліктами і інцидентами.

Застосовуючи формалізм теорії систем [14,15], побудуємо узагальнені моделі систем, які відповідають наступним типам:

1. Для біологічної системи:

$$BioSys = (GN, EC, MB, EV, FC, RP), \quad (1)$$

де GN - генетичне початок;
EC - умови існування;
MB - метаболізм;
EV - еволюція;
FC - функціонування;
RP - репродукція.

2. Для інформаційної системи:

$$ICSys = (IR, EN, TR, CN, QS, SV), \quad (2)$$

де IR - інформаційні ресурси;
EN - середовище;
TR - телекомунікаційні ресурси;
CN - контроль, експлуатація, проектування;
QS - якість;
SV - надійність.

3. Для інформаційно-технічних систем:

$$STSys = (RI, RO, EX, MN, EF, ED), \quad (3)$$

де RI - внутрішні ресурси;
RO - зовнішні ресурси;
EX - виконавці;
MN - менеджмент, реінжиніринг;
EF - ефекти;
ED - навчання, передача знань.

Параметри GN, IR, RI є «вхідні сигнали» кожної з систем; EC, EN, RO - непередбачувані «перешкоди» (зовнішні фактори і загрози); MB, TR, EX - «оператори перетворення» (внутрішні процеси); EV, CN, MN - «зворотний зв'язок» (процеси внутрішнього розвитку і самоорганізації); FC, QS, EF - «сигнал на виході» кожної з систем (критерії ефективності «цільові процеси»); RP, SV, ED - «закінчення циклу» (відтворення, забезпечення переходу до наступних епох життя системи, «новий виток спіралі»).

Можна відзначити паралелі між параметрами моделей кожної з систем. Це підтверджується і в роботах [4,5,10,11,12,15] до розвитку природи і суспільства.

Так само ці питання вирішуються і в дослідженнях [16,17], де показано, що проблема ІБ з точки зору онтології предметної області та математичних моделей представлення знань структурно подібна проблеми захисту біологічних організмів від патогенних факторів.

При цьому слід враховувати, що інформація, що обробляється в ІКС і ІТС, які функціонують на базі Internet, особливо вразлива. Суттєвого підвищення можливості

несанкціонованого використання або модифікації даних, введення в оборот неправдивої інформації в даний час сприяють:

- збільшення обсягу інформації, що обробляється, передається та зберігається;
- зосередження в базах даних інформації різного рівня важливості і конфіденційності;
- розширення доступу кола користувачів до інформації та до ресурсів мережі, що призводить до виникнення конфліктів та інцидентів;
- збільшення числа віддалених робочих місць;
- широке використання для зв'язку користувачів мережі Internet і різних каналів зв'язку;
- автоматизація обміну інформацією між комп'ютерами користувачів.

Тому при розгляді конфліктів та інцидентів необхідно враховувати їх характер та можливості управління ними. При цьому, слід враховувати сучасні підходи до управління з розумінням існуючих підходів і особливостей ІС [11,18,19].

Відповідно до мети дослідження принцип біоаналогів і «організованого підходу», система управління конфліктами і інцидентами ІБ включаючи підсистему виявлення вторгнення (IDS) в рамках комплексної системи інформаційної безпеки (КСІБ) і ІКС і ІТС, що функціонують на базі Internet, повинні грати ту саму роль, що і імунна система в живому організмі.

Стосовно до управління конфліктами і інцидентами ІБ це повинно означати перехід від «механізму» до біологічної аналогії, коли система розуміється як така, що розвивається і розуміється крізь призму еволюційної теорії [4,8,11,19].

На підставі проведених досліджень побудуємо узагальнену модель системи управління інцидентами і конфліктами:

$$IMSys = (INC, SEC, CRI, KBS, X, Y, S, DMF, AGT, ARS, TRS, IRS, MST, T, SYN) \quad (4)$$

де INC - управління інцидентами;

SEC - безпека (мета);

CRI - критерії оцінки стану безпеки;

KBS - база знань про конфлікти і інциденти;

X - вхідні впливу;

Y - реакція на конфлікт або інцидент;

S - стан системи;

DMF - функція прийняття рішень (реагування), яка включає два підетапи: прийняття рішення про включення елемента ARS в набір TRS, і потім, на підставі першого підетапу - прийняття рішення про включення елемента ARS в набір TRS;

AGT - агенти, безліч програмно реалізованих мобільних інтелектуальних агентів;

ARS - агентно-орієнтований набір ресурсів ІБ, тобто безліч всіх доступних для агентів ресурсів безпеки;

IRS - інцидентно-орієнтований і конфліктно-орієнтований набори ресурсів безпеки, тобто підмножина ресурсів, якими володіє агент, і які в сукупності є достатніми для ефективного реагування на конкретний тип конфлікту або інцидент;

TRS - тестовий набір ресурсів безпеки, тобто підмножина ресурсів, які відбирають для імітаційного моделювання прогнозу і адаптації до невідомого типу конфлікту або інциденту;

MST - стратегія управління конфліктами і інцидентами;

T - час;

SYN - самоорганізація.

Створення та розробка методології побудови адекватних систем захисту інформації та управління конфліктами і інцидентами ІБ виходить з принципу подібності механізмів ІБ і імунної системи. При цьому, завданням, що вирішується є

розробка імунної системи управління конфліктами і інцидентами ІБ в складі СЗІ з використанням, як окремих інтелектуальних підходів, так і їх комбінацій для забезпечення розв'язуваної задачі в умовах високої динаміки загроз. Підходи до ІБ та управління конфліктами і інцидентами ІБ в такий вимірjuвальній системі, повинні володіти новими методами і властивостями, аналогічними зокрема методами збереження живучості (працездатності) біологічної популяційної системи живої природи.

Неодмінним властивістю будь-якої системи є наявність структури, яка представляє собою побудову системи, що відображає найбільш суттєві взаємозв'язки між елементами і їх групами (підсистемами), які мало змінюються при змінах в системі і забезпечують стає функціонування системи і її основні властивості.

У мережевої та організаційної архітектурі мережі Internet і її елементів ІКС і ІТС виділимо підсистему автоматичного управління конфліктами і інцидентами ІБ.

При цьому слід враховувати, що для забезпечення і аналізу ІБ необхідно оцінювати напрямок діяльності СЗІ, а для досягнення ефективності в її роботі доцільно виділити наступні напрямки [20]:

- захист об'єкта (мережі та її елементи);
- захист процесів або процедур обробки і зберігання інформації;
- захист каналів зв'язку;
- контроль і управління СЗІ.

Крім цього необхідно усвідомлювати, що конфлікти в мережі можуть виникати при зверненні двох і більше користувачів до одних і тих же ресурсів, каналів зв'язку, тощо. При цьому, інциденти можуть бути як зловмисними, так і випадковими (наприклад, бути наслідком помилки або природних явищ) і можуть виникати в слідстві як технічних, так фізичних засобів. Їх наслідками можуть бути такі події, як несанкціоновані зміни інформації, її знищення або інші події, які роблять її недоступною, нанесення шкоди користувачам [21].

Отже, можемо наразі приступити до побудови системи управління конфліктами і інцидентами ІБ використовуючи імунно-мультіагентну технологію [12,15,17].

Розглянемо 4 класу агентів (рис.2): агенти-детектори; агенти-ідентифікатори; агенти-координатори та агенти-реактори.

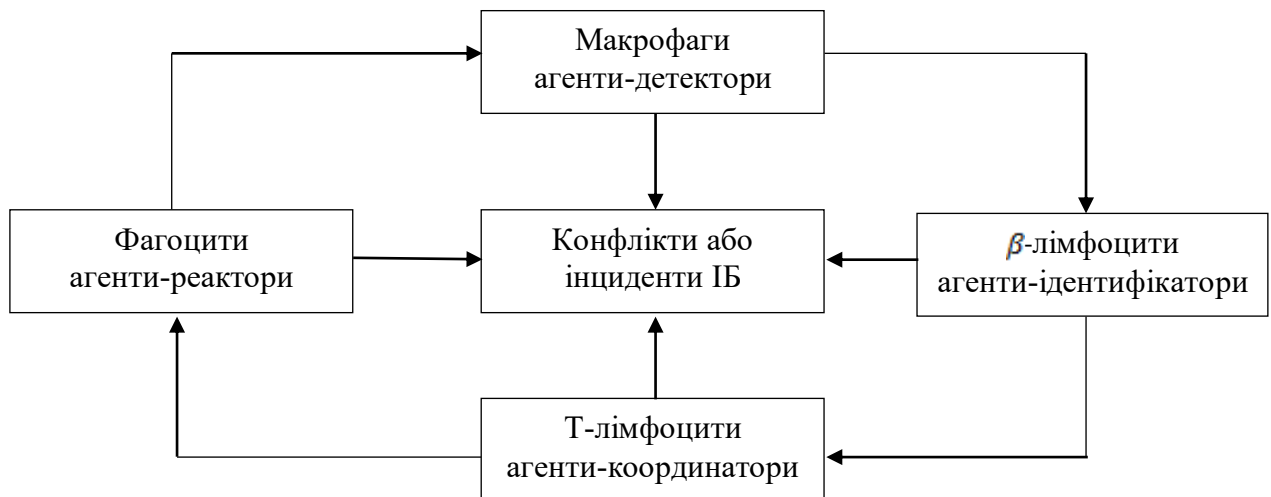


Рис. 2. Цикл і функції управління конфліктами і інцидентами за допомогою ІІС

При цьому, агенти-детектори (рецептори) - відповідають макрофагам і іншим антиген-презентуючим клітинам, які виділяють частки антигену на своїй поверхні, привертаючи увагу β-лімфоцитів для розпізнання. Агенти-ідентифікатори відповідають β-лімфоцитам, які розпізнають антиген і заздалегідь піддавалися «негативного відбору»

в тимусі. Агенти-координатори відповідають лімфоцитам, які виділяються Т-лімфоцитами для активізації β -лімфоцитів. Агенти-реактори відповідають фагоцитам, які мають антитіла для знищення антигену.

Сформулюємо наступні етапи управління конфліктами і інцидентами за допомогою ШІС:

- 1 етап. Індикація агентами-детекторами будь-якої підозрілої активності.
- 2 етап. Розпізнавання агентами-ідентифікаторами ненормальної активності, як певного типу конфлікту або інциденту, за умови знаходження в базі знань відповідної сигнатури або виявлення аномалій по відношенню до еталону поведінки.
- 3 етап. Отримання підсистемою реагування на сигнал від IDS про ідентифікований відомий або невідомий конфлікт або інцидент.
- 4 етап. Ідентифікація атакуючого набору загроз конфлікту або інциденту за умови наявності у базі знань кореляції між характеристиками отриманого сигналу про конфлікт або інцидент і записами про набір атакуючих загроз.
- 5 етап. Формування текстових наборів механізмів захисту згідно з алгоритмом, який генерується базою знань.
- 6 етап. Імітаційне моделювання ефективності перекриття текстовим набором механізмів захисту - набору атакуючих загроз конкретного ідентифікованого конфлікту або інциденту.
- 7 етап. Прийняття рішення щодо вибору конфліктно-орієнтованого або інцидентно-орієнтованого набору механізмів захисту.
- 8 етап. Видача підсистемою обробки сигналу, що управляє агентом-реактором щодо обробки конфлікту або інциденту за допомогою конфліктно-орієнтованого і інцидентно-орієнтованого набору механізмів захисту.
- 9 етап. Самоорганізація та оцінка підсистемою зворотного зв'язку і агентами-детекторами ефективності використання конфліктно-орієнтованого або інцидентно-орієнтованого набору механізмів захисту, поповнення баз знань новим досвідом, розслідування та аналіз конфлікту і інциденту, вироблення керуючого сигналу щодо превентивних дій.

Для того, щоб скласти єдиний організм агенти повинні забезпечити гомеостатичне регулювання мережі Internet в цілому та в її елементах ІКС/ІТС. Під гомеостатичним регулюванням розуміється управління конфліктами і інцидентами, що підтримує цільові характеристики мережі Internet і її складових частин ІКС/ІТС, в межах, що забезпечують її безпеку, якість, надійність і живучість.

Безпека Internet як комплексу ІКС/ІТС визначається мінімізацією вразливостей елементів Internet (ІКС/ІТС) і ступенем захищеності мереж, що функціонують на базі Internet, а також системами управління конфліктами і інцидентами ІБ.

Висновки

Проведений аналіз показує, що сучасні ІКС і ІТС, що функціонують на базі Internet, які налічують тисячі суб'єктів, визначаються фактором їх існування та розвитку, наявністю захищеної системи обміну інформацією і системою управління конфліктами і інцидентами ІБ.

Отримані науково-технічні результати: запропоновано, логічно обґрунтований і математично формалізовано імунний підхід до інтелектуального управління конфліктами і інцидентами ІБ в ІКС і ІТС, що функціонують на базі Internet; побудована узагальнена модель управління конфліктами і інцидентами. Показана практична доцільність і прикладне значення отриманих результатів на прикладі застосування прототипу структури і функцій імунної системи управління конфліктами і інцидентами ІБ на базі агентно-орієнтованого підходу до побудови розподілених систем. Даний підхід забезпечує динамічне адаптивне управління при виникненні

нових конфліктів та інцидентів. Застосування ІІС в автоматизації та інтелектуалізації управління конфліктами і інцидентами ІБ може дозволити досягти якісно нового рівня забезпечення та управління ІБ в ІКС і ІТС, що функціонують на базі Internet.

Список літератури

1. Осовецкий Л.Г. Геном информатизации и корпоративная иммунология интернета. *Системы управления связью и безопасность*. 2016. № 1. С. 191-205
2. Howard J. An Analysis of Security Incidents in the Internet, *CERT//CC*, 2000
3. Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А. Основы корпоративной теории информации. СПб: СПбГУ ИТМО, 2004. 252 с.
4. Искусственные иммунные системы и их применение / под ред. Д. Дасгупты. М.: Физмат, 2006. 344 с.
5. Марчук Г.И. Математические модели в иммунологии. М.: Наука, 2011. 314 с.
6. Звонов Д., Нестерчук Ф.Г., Осовецкий Л.Г. К оценке защищенности корпоративной сети. *НТВ Информационных технологий, механизмов и оптики*, 2018. Т. 6, № 2. С. 156-167.
7. Осовецкий Л.Г., Суханов А.В., Ефимов В.В. Меры по обеспечению безопасности и защиты информации для сложных информационных систем. *Системы управления связи и безопасности*, 2017. № 1. С. 16-25.
8. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236 с.
9. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. К.: ГУИКТ, 2009. 251 с.
10. Караулов, А.В. Иммуитет и инфекционные заболевания: от вакцинации к иммунореабилитации. *Практикующий врач*. 2006. № 3. С. 4-6.
11. Петров Р.В. Иммунология. М.: Медицина, 2007. 436 с.
12. Осовецкий Л.Г., Нестерчук Г.Ф., Бормотов В.М. К вопросу иммунологии сложных информационных систем. *Приборостроение*, 2003. Т. 46, № 7. С. 34-40.
13. Томашевский В.М. Моделирование систем. К.: ВНУ, 2007. 352 с.
14. Вунш Г. Теория систем. М.: Сов. Радио, 1978. 288 с.
15. Гладыш С.В. Применение принципа биоаналогий для синтеза систем интеллектуального управления безопасностью телекоммуникаций. *Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине*. 2006. Вип. 1 (13), С. 57-63.
16. Нестерчук Г.Ф., Осовецкий Л.Г., Нестерчук Ф.Г., Воскресенский С.И., Грибачев В.П. Информационная избыточность нейронечетких средств обеспечения безопасности. *Вопросы защиты информации*. 2003. № 3 (70), С. 12-16.
17. Нестерчук Г.Ф., Осовецкий Л.Г., Харченко А.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов (иммунология систем информационных технологий). СПб.: Гос. ун-т. экономики и финансов, 2003. 364 с.
18. Постон Т. Стюарт И. Теория катастроф и ее приложения. М.: Мир, 1980. 608 с.

19. Єжова Л.Ф., Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. Управління інформаційною безпекою. В 2-х томах. К.: НАУ, 2012.
20. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. К.: Арий. 2008. – Том. 2
21. Капустян М.В., Олешко Т.И., Хорошко В.А. Модели передачи информации с учетом обнаружения, недопущения и устранения тупиковых ситуаций. *Вісник ДУІКТ*, 2006. Т. 4, № 3, С. 156-162.

INFORMATION SECURITY CONFLICTS AND INCIDENTS MANAGEMENT ON THE INTERNET

V.O. Horoshko¹, M.M. Brailovskyi²

¹National Aviation University, Lubomyr Guzar Ave, 1, Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

²Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine; e-mail: bk1972@ukr.net

The article deals with the problem of improving the efficiency of managing the conflicts and incidents of information security in infocommunication and information technology systems operating on the basis of the Internet. The aim of this study is to propose an approach to the management of incidents and conflicts of information security in Internet networks, based on the principle of biosimilarity within the artificial immune systems. The analysis shows that the factor determining the existence and development of modern infocommunication and information technology systems, operating on the basis of the Internet and numbering thousands of entities, is the presence of a secure information exchange system and a system for managing conflicts and incidents. The results of the research are as follows: a logically grounded and mathematically formalized immune approach to the intelligent management of conflicts and incidents of information security in infocommunication and information technology systems operating on the basis of the Internet is proposed; a generalized model for managing conflicts and incidents highlighting the target characteristics of the immune system has been elaborated; an approach using a generalized model of conflict and incident management has been substantiated. The practical feasibility and significance of the results obtained is illustrated by using a prototype of the structure and functions of the immune system for managing conflicts and incidents of information security on the basis of an agent-based approach to building distributed systems. This approach provides a dynamic adaptive management in the event of new conflicts and incidents. The use of artificial immune systems in the automation and intellectualization of management of conflicts and incidents of information security may allow to achieve a qualitatively new level of provision and management of information security in information and communication systems functioning on the basis of the Internet. In addition, the article identifies the factors that have the greatest impact on determining the vulnerability of the Internet with a view to assessing the functional security of the Internet.

Keywords: conflict and incident management models, information systems, information security, immune system, biosimilarity.

**РОЗРОБКА КОМП'ЮТЕРНИХ ПРОГРАМ ОПТИМАЛЬНОГО
ПРОЕКТУВАННЯ ДИНАМІЧНИХ ПРОЦЕСІВ СПІЛЬНОГО ПІДПРИЄМСТВА З
ВИРОБНИЦТВА І ЗБУТУ ПРОДУКЦІЇ****Н.М. Єршова, Н.О. Вельмагіна, Н.С. Чуприна**

Придніпровська державна академія будівництва та архітектури
м. Дніпро, 49000, вул. Чернишевського, 24 а E-mail:
nersova107@gmail.com, velmagina24@gmail.com, coderchan228@gmail.com

Актуальним завданням сьогодняшнього дня є створення стабільно функціонуючих і ефективних спільних підприємств з виробництва і збуту продукції. Для цього необхідно знати значення оптимальних параметрів, які характеризують процес взаємодії підприємств спільного підприємства. Раніше встановлено, що кінцева продукція спільного підприємства, яку поставляють на зовнішнє споживання, залежить від проміжної продукції, що залишається підприємствами на розвиток власного виробництва. Виникає задача, як визначити частки потоку валової продукції, щоповинні направляти підприємства на розвиток власного виробництва для забезпечення ефективної роботи спільного підприємства. Окрім того, важливо знати оптимальні значення параметрів процесу випуску валового продукту підприємства. Комп'ютерних програм для оптимального проектування динамічних процесів виробничих систем не існує. Отже метою даної роботи є розробка комп'ютерних програм для оптимального проектування процесу випуску валового продукту підприємства і процесу взаємодії трьох підприємств спільного підприємства з виробництва і збуту продукції. В основу алгоритмів пошуку проектних рішень закладено матричний метод динамічного програмування Р. Беллмана для безперервних динамічних процесів, що є науковою новизною роботи. Створена комп'ютерна програма «ОРТІМА» призначена для спрощення процесу проектування спільних підприємств шляхом підбору оптимальних параметрів та розрахунку максимально досяжного обсягу кінцевої продукції, що спрямована на зовнішнє споживання. Комп'ютерна програма «SINTEZ» здійснює вибір оптимальних параметрів проектування: коефіцієнтів зростання і вибуття основних виробничих фондів підприємства та виконує розрахунок максимально можливого за наявних вихідних даних обсягу валового продукту. Дана робота є важливим внеском в галузі комп'ютерних наук і програмної інженерії.

Ключові слова: оптимальне проектування динамічних процесів, комп'ютерна програма, спільне підприємство.

Вступ

В даний час багато підприємств, не витримавши конкуренції ринку, припиняють функціонування. Вирішальне значення при використанні обмежених виробничих ресурсів має тісна і безперервна взаємодія підприємств в спільному підприємстві на користь отримання взаємної вигоди при рішенні сумісних задач з задоволення потреб суспільства[8]. Взаємодію підприємств слід розглядати з позиції системного підходу: об'єктом дослідження є не суб'єкти, а процес взаємодії між ними.

Актуальним завданням сьогодняшнього дня є створення стабільно функціонуючих і ефективних спільних підприємств. Для цього необхідно знати значення оптимальних параметрів, які характеризують процес взаємодії підприємств спільного підприємства. На основі моделювання процесу взаємодії підприємств [1] встановлено, що кінцева продукція спільного підприємства, яку поставляють на зовнішнє споживання, залежить від проміжної продукції, що залишається підприємствами на розвиток власного виробництва. Виникає задача, як визначити частки потоку валової продукції, щоповинні направляти підприємства на розвиток власного виробництва для забезпечення ефективної роботи спільного підприємства.

Задачі оптимального проектування зручно вирішувати з допомогою матричного методу динамічного програмування Р. Беллмана. Для реалізації алгоритмів пошуку проектних рішень необхідно створювати відповідні комп'ютерні програми.

Аналіз останніх досліджень і публікацій

В даний час є мало робіт, в яких досліджуються динамічні процеси виробничо-технічних систем. В роботі [5] розглядається оптимальний режим функціонування промислового комплексу в умовах фінансової кризи, в роботі [6] - підприємства в умовах дефіциту попиту. В роботі [12] розглядаються завдання, що розкривають внутрішні резерви окремого підприємства в різних умовах його функціонування. Вперше створено математичну модель життєвого циклу підприємства (ЖЦП) на основі теорії безперервних динамічних процесів, яка дозволяє: прогнозувати поведінку підприємства в майбутньому, планувати його розвиток, аналізувати стійкість функціонування, моделювати кризові ситуації всередині підприємства і його поведінку в ринкових умовах. Виконана оптимізація параметрів процесу випуску валового продукту підприємства за допомогою невизначених множників Лагранжа, принципу максимуму Понтрягіна і матричного методу динамічного програмування Р. Беллмана. Отримано аналітичні залежності для визначення коефіцієнтів росту і вибуття основних виробничих фондів (ОВФ). Моделювання виконувалось в середовищі Excel і системі моделювання PDS (проектування динамічних систем) [7]. Робота [13] присвячена моделюванню процесу взаємодії двох підприємств, що випускають різну продукцію, робота [14] - процесу взаємодії трьох підприємств. Доведено ефективність різних способів процесу взаємодії підприємств. Робота [1] представляє розробку теоретичних основ проектування підприємств і формування виробничих систем. В цих роботах для моделювання використовувалась система моделювання МВТП 3.7 (моделювання в технічних пристроях) [11]. Комп'ютерних програм для оптимального проектування динамічних процесів виробничих систем тоді не існувало.

Мета роботи

Отже, метою даної роботи є розробка комп'ютерних програм для оптимального проектування процесу випуску валового продукту підприємства і процесу взаємодії трьох підприємств спільного підприємства з виробництва і збуту продукції. В основу алгоритмів закладено матричний метод динамічного програмування Р. Беллмана для безперервних динамічних процесів.

Основна частина

Оптимальне проектування процесу випуску валового продукту підприємства

Процес виробництва валового продукту є основою будь-якого підприємства. Він повинен бути безперервним в часі, тобто його можна описати звичайним диференціальним рівнянням. Виробництво валового продукту неможливе без вкладення ОВФ. Отже, параметрами процесу випуску валового продукту повинні бути коефіцієнти зростання і вибуття ОВФ. Виникає проблема: як визначити значення цих параметрів, щоб процес випуску валового продукту був стабільним. Проблема ця не вирішена, хоча вона є дуже актуальною.

В математичну модель процесу випуску валового продукту входить велика кількість параметрів [9]. Стійкість – внутрішня властивість процесу, не залежна від миттєвих значень основних фондів. Підприємство і процес тільки створюються, тому поки не можна судити про рівень їх науково-технічного розвитку. Як припущення

прийнемо постійну фондомісткість. Тоді математична модель процесу випуску валової продукції має вигляд:

$$m\ddot{Y} + \beta\dot{Y} + cY = 0, \quad (1)$$

де m – фондомісткість ОВФ по випуску даної продукції; c – коефіцієнт зростання ОВФ; β_i – коефіцієнт вибуття ОВФ; Y – валовий продукт.

Модель (1) є моделлю-аналогом процесу. Ставиться задача – визначити розрахункові формули параметрів проектування: коефіцієнтів вибуття і зростання ОВФ при постійній фондомісткості.

В матричному методі динамічного програмування диференціальне рівняння проектного процесу записується у вигляді

$$m\ddot{Y} = -F \quad \text{або} \quad \ddot{Y} = -F / m = -u, \quad (2)$$

де u – невідома синтезуюча функція, що є прискоренням процесу випуску валового продукту. Позначимо: $x_1 = Y$; $x_2 = \dot{Y}$, тоді отримаємо

$$\begin{aligned} \dot{x}_1 &= x_2; \\ \dot{x}_2 &= -u. \end{aligned} \quad (3)$$

Запишемо систему (3) в матричній формі

$$\dot{X} = AX + BU, \quad (4)$$

$$\text{де } X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} Y \\ \dot{Y} \end{bmatrix}; \quad U = [u]; \quad A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}; \quad B = \begin{bmatrix} 0 \\ -1 \end{bmatrix}.$$

Як критерій оптимальності прийнемо квадратичний функціонал якості:

$$J = \int_0^{\infty} (\alpha x_1^2 + \gamma x_2^2 + \mu u^2) dt \quad (5)$$

$$\text{або в матричній формі } J = \int_0^{\infty} V dt = \int_0^{\infty} (X' P X + U' G U) dt,$$

де α, γ, μ – вагові коефіцієнти функціоналу. Матриці вагових коефіцієнтів P і G функціоналу (7) мають вигляд:

$$P = \begin{bmatrix} \alpha & 0 \\ 0 & \gamma \end{bmatrix}; \quad G = [\mu].$$

Ставиться задача: визначити синтезуючу функцію рівняння (4), яка мінімізує функціонал якості (5). Фізичний сенс функціоналу – витрати грошових коштів на підтримку стабільності процесу випуску валового продукту підприємства. Крім того, параметри проектування повинні забезпечити отримання максимального значення

обсягу валового продукту.

Необхідною умовою оптимальності є розв'язок нелінійного алгебраїчного рівняння Ріккати

$$P + A'S + SA - SBG^{-1}B'S = 0. \quad (6)$$

З запису його в розгорненому вигляді одержуємо систему нелінійних алгебраїчних рівнянь для визначення елементів симетричної матриці помилки оцінки S .

$$\begin{cases} \alpha - S_{12}^2 / \mu = 0; \\ \gamma + 2S_{12} - S_{22}^2 / \mu = 0; \\ S_{11} - S_{12}S_{22} / \mu = 0. \end{cases} \quad (7)$$

Синтезуюча функція визначається матричним виразом

$$U = -G^{-1}B'SX = \frac{1}{\mu}(S_{12}x_1 + S_{22}x_2) = \frac{1}{\mu}(S_{12}Y + S_{22}\dot{Y}).$$

Після підстановки елементів S_{12} , S_{22} в синтезуючу функцію маємо

$$u = ((\gamma + 2\sqrt{\alpha\mu}) / \mu)^{1/2} \dot{Y} + (\alpha / \mu)^{1/2} Y. \quad (8)$$

Якщо підставити синтезуючу функцію (8) в рівняння (2), то отримаємо

$$\ddot{Y} + a_1 \dot{Y} + a_2 Y = 0, \quad (9)$$

де $a_1 = ((\gamma + 2\sqrt{\alpha\mu}) / \mu)^{1/2}$; $a_2 = (\alpha / \mu)^{1/2}$. Диференційне рівняння моделі-аналога має вигляд

$$\ddot{Y} + a_1 \dot{Y} + a_2 Y = 0, \quad (10)$$

де $a_1 = \beta / m$; $a_2 = c / m$. З порівняння коефіцієнтів a_1, a_2 в цих рівняннях одержуємо аналітичну залежність для коефіцієнтів зростання і вибуття ОВФ:

$$c = m(\alpha / \mu)^{1/2}; \quad \beta = m((\gamma + 2\sqrt{\alpha\mu}) / \mu)^{1/2}. \quad (11)$$

У виробничих системах близьким до оптимального є аперіодичний закон розвитку. Синтезуюча функція повинна бути фізично реалізованою. Для перевірки цього необхідно мати залежність між ваговими коефіцієнтами квадратичного функціоналу якості і діапазон їх змін. Встановлюється залежність за формулами (11) з урахуванням того, що коефіцієнт зростання ОВФ звичайно на два порядки менше коефіцієнта вибуття.

$$\alpha = \mu c^2 / m^2; \quad \gamma = 10^4 \alpha - 2\sqrt{\alpha\mu}. \quad (12)$$

Алгоритм пошуку проектних рішень

При проектуванні процесу випуску валового продукту потрібно вибрати таку сукупність параметрів проектування, яка забезпечить максимум його обсягу.

Алгоритм пошуку проектних рішень наведений на рис. 1.

Комп'ютерна програма «SINTEZ»

Створена комп'ютерна програма «SINTEZ» оптимального проектування процесу випуску валового продукту підприємства. Комп'ютерна програма є прикладною програмою з віконним графічним інтерфейсом користувача. Система створена за допомогою HTML 5, CSS 3 та мови програмування JavaScript.

Програма розповсюджується у вигляді одного файлу з форматом html. Вигляд діалогового вікна на початку роботи показано на рис. 2.

Всі поля форми обов'язкові для заповнення. Дробова частина числа відділяється від цілої крапкою.

Фрагмент роботи програми наведено на рис. 3.

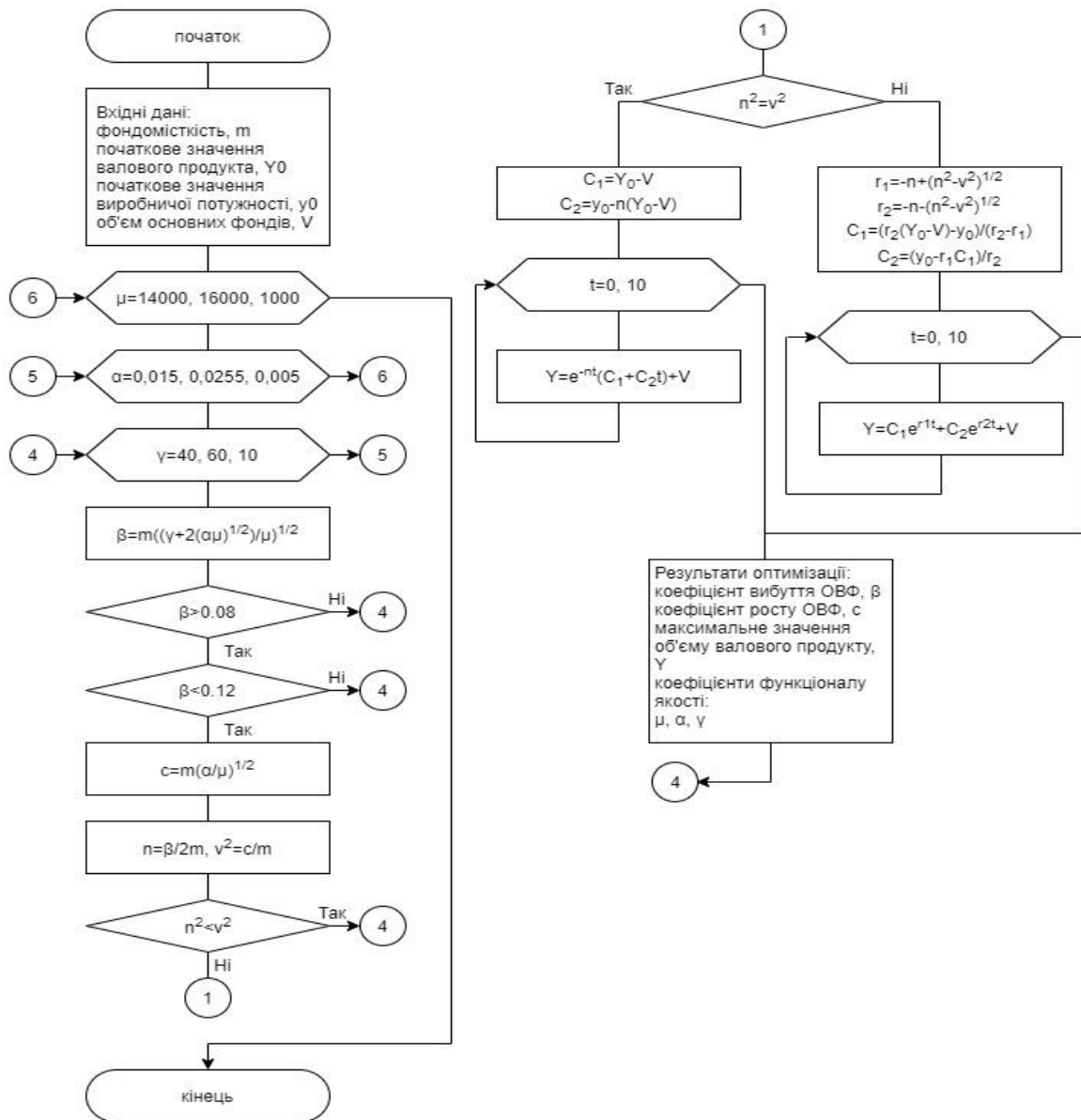


Рис. 1. Алгоритм пошуку проектних рішень

Sintez

Фондоємність (m):

Початкове значення валового продукту (Y0):

Початкове значення виробничої потужності (y0):

Об'єм основних фондів (V), тис. у.о.:

Рис. 2. Діалогове вікно програми на початку роботи.

β	c	α	γ	μ	Макс. Y
0.09991	0.00145	0.01500	40.00000	16000.00000	3647.98672

β	c	α	γ	μ	Макс. Y
0.10672	0.00145	0.01500	50.00000	16000.00000	3576.47856

β	c	α	γ	μ	Макс. Y
0.10323	0.00168	0.02000	40.00000	16000.00000	3604.89742

β	c	α	γ	μ	Макс. Y
0.10983	0.00168	0.02000	50.00000	16000.00000	3536.64129

β	c	α	γ	μ	Макс. Y
0.10607	0.00187	0.02500	40.00000	16000.00000	3642.85340

Рис. 3. Результати оптимізації.

Тестування комп'ютерної програми виконано шляхом комп'ютерного моделювання в середовищі SimlnTech [4] і розрахунком за формулами в середовищі Excel.

Оптимальне проектування процесу взаємодії підприємств спільного підприємства

Спільне підприємство з виробництва і збуту продукції має три підприємства, перше підприємство є фондотворчим. Друге і третє підприємства виробляють взаємозамінну, в сенсі споживання продукцію. Проміжна продукція фондотворчого підприємства йде на розвиток власного виробництва, кінцева продукція порівну розподіляється між двома іншими підприємствами. Друге і третє підприємства залишають проміжну продукцію для розвитку власного виробництва. Кінцева продукція цих підприємств йде на зовнішнє споживання.

Структурна схема процесу взаємодії підприємств спільного підприємства представлена на рисунку 3 [10], де y_{kp} - кінцева продукція спільного підприємства.

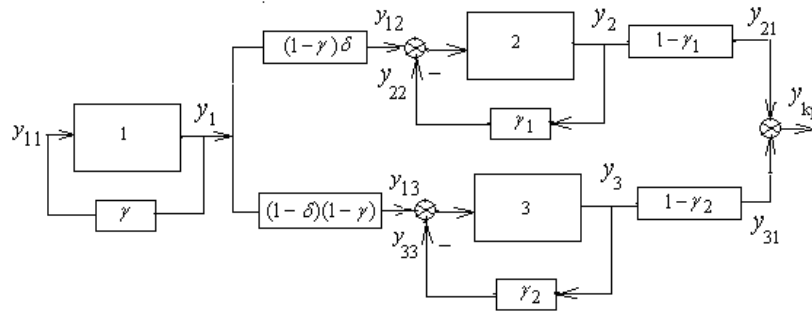


Рис. 3. Структурна схема процесу взаємодії підприємств.

Математична модель процесу взаємодії трьох підприємств має вигляд:

$$\begin{aligned} \dot{y}_1 + a_{11}y_1 &= 0, \quad y_1(0) = y_{10} \\ \dot{y}_2 + a_{22}y_2 &= a_{12}y_1, \quad y_2(0) = y_{20} \\ \dot{y}_3 + a_{33}y_3 &= a_{13}y_1, \quad y_3(0) = y_{30} \end{aligned} \quad (13)$$

де $a_{11} = \frac{\beta_1 - \gamma}{m_1}$; $a_{22} = \frac{\beta_2 - \gamma_1}{m_2}$; $a_{33} = \frac{\beta_3 - \gamma_2}{m_3}$; $a_{12} = \frac{(1-\gamma)\delta}{m_2}$; $a_{13} = \frac{(1-\delta)(1-\gamma)}{m_3}$, y_i – виробнича потужність i -го підприємства; $\gamma, \gamma_1, \gamma_2$ – частка потоку, що випускається, і залишається підприємствами на розвиток власного виробництва; m_i, β_i – відповідно фондомісткість і коефіцієнт вибуття ОВФ i -го підприємства; δ – частка потоку кінцевої продукції, що порівну розподіляється між другим і третім підприємствами.

В роботі [3] доведено, що оптимальні параметри можна визначати на математичних моделях без зовнішнього впливу, так як при будь-якому впливі в синтезуючій функції буде складова, що гасить його. Тому запишемо математичну модель (13) у вигляді

$$\begin{aligned} m_1 \dot{y}_1 + \beta_1 y_1 - \gamma y_1 &= 0; \\ m_2 \dot{y}_2 + \beta_2 y_2 - \gamma_1 y_2 &= 0; \\ m_3 \dot{y}_3 + \beta_3 y_3 - \gamma_2 y_3 &= 0. \end{aligned} \quad (14)$$

Представимо систему (14) в матричній формі

$$\begin{aligned} M\dot{Y} + FY - CY &= 0, \\ M &= \begin{bmatrix} m_1 & 0 & 0 \\ 0 & m_2 & 0 \\ 0 & 0 & m_3 \end{bmatrix}; \quad F = \begin{bmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{bmatrix}; \quad C = \begin{bmatrix} \gamma & 0 & 0 \\ 0 & \gamma_1 & 0 \\ 0 & 0 & \gamma_2 \end{bmatrix}; \\ Y &= \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}; \quad \dot{Y} = \begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \end{bmatrix}. \end{aligned} \quad (15)$$

Математична модель (15) є моделлю-аналогом проектного процесу. Запишемо систему (14) у вигляді

$$\begin{aligned}m_1 \dot{y}_1 &= -\beta_1 y_1 - u_1; \\m_2 \dot{y}_2 &= -\beta_2 y_2 - u_2; \\m_3 \dot{y}_3 &= -\beta_3 y_3 - u_3.\end{aligned}\tag{16}$$

де u_1, u_2, u_3 – невідомі синтезуючі функції.

Представимо систему (16) в матричній формі

$$\dot{Y} = -M^{-1}(FY + BU),\tag{17}$$

де $Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$ – вектор стану процесу; $U = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}$ – вектор управління;

$$F = \begin{bmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad M^{-1} = \begin{bmatrix} 1/m_1 & 0 & 0 \\ 0 & 1/m_2 & 0 \\ 0 & 0 & 1/m_3 \end{bmatrix} \text{ – постійні матриці.}$$

Формулювання задачі синтезу: знайти фізично здійсненну синтезуючу функцію рівняння (17), яка забезпечує мінімум функціоналу (18).

$$J = \int_0^{\infty} \sum_{i=1}^3 (\alpha_i y_i^2 + \mu_i u_i^2) dt\tag{18}$$

або в матричній формі $J = \int_0^{\infty} (Y'PY + U'GU)dt$,

$$\text{де } P = \begin{bmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{bmatrix}; \quad G = \begin{bmatrix} \mu_1 & 0 & 0 \\ 0 & \mu_2 & 0 \\ 0 & 0 & \mu_3 \end{bmatrix} \text{ – матриці вагових коефіцієнтів функціоналу}$$

якості.

Ставиться задача - встановити розрахункові формули для параметрів проектування: частки потоку валової продукції $\gamma, \gamma_1, \gamma_2$, які направляються підприємствами на розвиток власного виробництва. Фізичний сенс функціоналу - витрати грошових коштів на підтримку стабільного функціонування процесу. При цьому кінцева продукція спільного підприємства, яку направляють на зовнішнє споживання, повинна бути максимальною.

Необхідною умовою оптимальності є вирішення нелінійного алгебраїчного рівняння Ріккаті

$$P + SF + F'S - SBG^{-1}B'S = 0,\tag{19}$$

де S – симетрична позитивно визначена матриця. З запису рівняння (19) в розгорнутому вигляді виходить система нелінійних алгебраїчних рівнянь для визначення елементів симетричної матриці S , яку неможливо вирішити.

У матриці S моделі аналога процесу (15) проєктовані параметри $\gamma, \gamma_1, \gamma_2$ розташовані на головній діагоналі, інші елементи матриці дорівнюють нулю. Тому приймаємо $S_{12} = S_{13} = S_{23} = 0$, тоді елементи матриці S легко обчислюються.

Вектор управління визначається матричним виразом

$$U = -G^{-1}B'SY = -\begin{bmatrix} 1/\mu_1 & 0 & 0 \\ 0 & 1/\mu_2 & 0 \\ 0 & 0 & 1/\mu_3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} S_{11} & 0 & 0 \\ 0 & S_{22} & 0 \\ 0 & 0 & S_{33} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = -\begin{bmatrix} S_{11}/\mu_1 & 0 & 0 \\ 0 & S_{22}/\mu_2 & 0 \\ 0 & 0 & S_{33}/\mu_3 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = -DY.$$

Підставимо вектор управління в (17) і врахуємо, що $BU = U$, отримаємо

$$\dot{Y} = -M^{-1}(FY - DY), \text{ або } M\dot{Y} + FY - DY = 0, \quad (20)$$

Порівнюючи (20) з моделлю-аналогом керованого процесу (15), відзначаємо рівність матриць $C = D$, тобто

$$\begin{bmatrix} \gamma & 0 & 0 \\ 0 & \gamma_1 & 0 \\ 0 & 0 & \gamma_2 \end{bmatrix} = \begin{bmatrix} S_{11}/\mu_1 & 0 & 0 \\ 0 & S_{22}/\mu_2 & 0 \\ 0 & 0 & S_{33}/\mu_3 \end{bmatrix} \quad (21)$$

Тому аналітичні залежності для визначення параметрів проєктування $\gamma, \gamma_1, \gamma_2$:

$$\begin{aligned} \gamma_i &= \beta_i + \sqrt{\beta_i^2 + \alpha_i / \mu_i}, i=1,2,3. \\ \alpha_i &= \mu_i(\gamma_i^2 - 2\gamma_i\beta_i); \quad 0 \leq \gamma_i \leq 1; \quad 0,08 \leq \beta_i \leq 0,3. \end{aligned} \quad (22)$$

Алгоритм пошуку проектних рішень

Для формування спільного підприємства з трьох підприємств потрібно вибрати таку сукупність параметрів проєктування, яка забезпечить максимум спрямованої на зовнішнє споживання його кінцевої продукції. Алгоритм пошуку проектних рішень наведений на рис. 4, алгоритм розрахунку кінцевої продукції - на рис. 5.

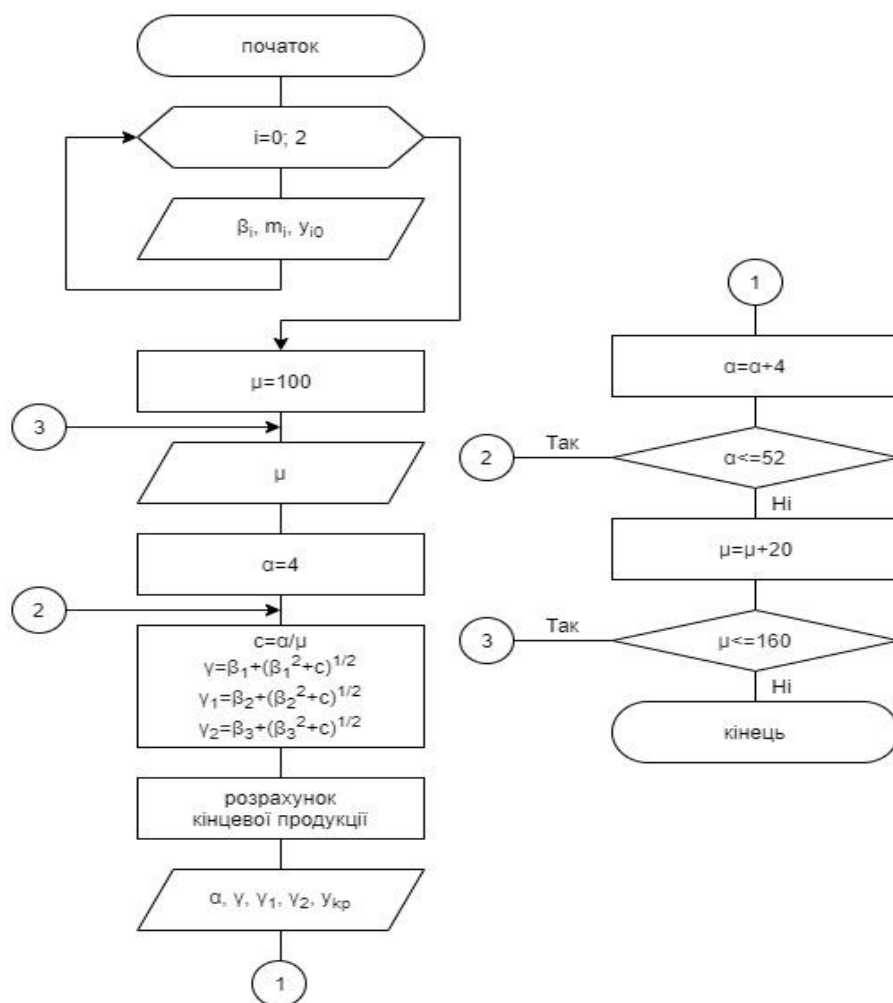


Рис. 4. Алгоритм пошуку проектних рішень.

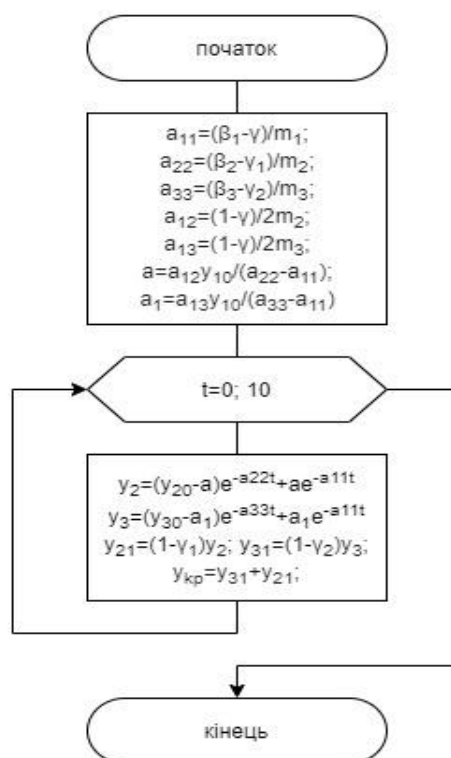


Рис. 5. Алгоритм розрахунку кінцевої продукції спільного підприємства.

Комп'ютерна програма «ОПТИМА»

Створена комп'ютерна програма «ОПТИМА», що містить програмні модулі оптимізації параметрів процесу взаємодії трьох підприємств і розрахунку кінцевої продукції спільного підприємства. Комп'ютерна програма призначена для спрощення процесу проектування спільних підприємств з виробництва і збуту продукції шляхом підбору оптимальних параметрів та розрахунку максимально досяжного обсягу кінцевої продукції, що спрямована на зовнішнє споживання. Це прикладна програма з віконним графічним інтерфейсом користувача. Система створена за допомогою HTML 5, CSS 3 та мови програмування JavaScript.

Вхідні дані для програми: фондомісткості, виробничі потужності та коефіцієнти вибуття ОВФ всіх трьох підприємств, що входять до спільного підприємства.

Дослідимо залежність виробничої потужності підприємств і обсягу кінцевої продукції спільного підприємства від проміжної продукції підприємств при наступних даних [2]:

$m_1=1,4$; $m_2=1,8$; $m_3=2,1$; $\beta_1=0,1$; $\beta_2=0,096$; $\beta_3=0,15$; $y_{10}=500$ тис. у.о./рік; $y_{20}=400$ тис. у.о./рік; $y_{30}=600$ тис. у.о./рік.

Вигляд діалогового вікна на початку роботи показано на рис.6. Всі поля форми обов'язкові для заповнення. Дробова частина числа відділяється від цілої крапкою.

Фрагмент роботи програми представлений на рис.7.

Optima

Коефіцієнт вибуття ОВФ β_1 :

 Фондоємність m_1 :

 Виробнича потужність y_{10} , тис. у.о./рік:

 Коефіцієнт вибуття ОВФ β_2 :

 Фондоємність m_2 :

 Виробнича потужність y_{20} , тис. у.о./рік:

 Коефіцієнт вибуття ОВФ β_3 :

 Фондоємність m_3 :

 Виробнича потужність y_{30} , тис. у.о./рік:

Рис. 6. Діалогове вікно програми «ОПТИМА».

$\mu=120.00000$, $\alpha=36.00000$
 $\gamma=0.65678$, $\gamma_1=0.65207$, $\gamma_2=0.71789$
 Кінцеве y_{kr} :14930.39567

$\mu=120.00000$, $\alpha=40.00000$
 $\gamma=0.68595$, $\gamma_1=0.68128$, $\gamma_2=0.74652$
 Кінцеве y_{kr} :15260.00929

$\mu=120.00000$, $\alpha=44.00000$
 $\gamma=0.71373$, $\gamma_1=0.70909$, $\gamma_2=0.77383$
 Кінцеве y_{kr} :15376.31310

$\mu=120.00000$, $\alpha=48.00000$
 $\gamma=0.74031$, $\gamma_1=0.73570$, $\gamma_2=0.80000$
 Кінцеве y_{kr} :15265.34795

$\mu=120.00000$, $\alpha=52.00000$
 $\gamma=0.76583$, $\gamma_1=0.76124$, $\gamma_2=0.82515$
 Кінцеве y_{kr} :14915.76524

Рис. 7. Результати розрахунку.

Тестування комп'ютерної програми виконане шляхом комп'ютерного моделювання в середовищі SimlnTech і розрахунку за формулами в середовищі Excel.

Висновки

У роботі представлена розробка комп'ютерних програм оптимального проектування процесу випуску валового продукту підприємства «SINTEZ» і процесу взаємодії трьох підприємств спільного підприємства з виробництва і збуту продукції «ОРТІМА». Тестування комп'ютерних програм виконане шляхом комп'ютерного моделювання в середовищі SimlnTech і розрахунком за формулами в середовищі Excel.

Комп'ютерне моделювання та оптимізацію потрібно виконати на першому етапі проектування, що дозволить створювати сучасні об'єкти і скоротити термін їх проектування.

Список літератури

1. Вельмагіна Н.О., Єршова Н.М., Шибко О.М. Розробка теоретичних основ проектування підприємств і формування виробничих систем: монографія. Дніпро: ПДАБА, 2020. 272 с.
2. Евсюкова М.Е., Ершова Н.М. Моделирование производственной мощности предприятий, выпускающих разную экологически чистую продукцию. *Строительство, материаловедение, машиностроение: Сб. научн. трудов. Серия: Компьютерные системы и информационные технологии в образовании, науке и управлении*. Днепр: ПГАСА, 2018. Вып. 106. С. 25-31.
3. Ершова Н.М. Современные методы теории проектирования и управления сложными динамическими системами. Монография. Днепропетровск: ПГАСА, 2016. 272 с.
4. Карташов Б.А., Шабаев Е.А., Козлов О.С., Щекотуров А.М. Среда динамического моделирования SimlnTech: практикум по моделированию технических систем автоматического регулирования. М.: ДМК Пресс, 2017. 424 с.
5. Катулев А.Н., Колесник Г.В., Федоров В.В. Оптимальный режим функционирования промышленного комплекса в условиях финансового кризиса. *Математическое моделирование*, 2001. Т. 13, № 10. С. 77-90.
6. Колесник Г.В. Оптимальный режим функционирования предприятия в условиях дефицита спроса. *Ученые записки*. Тверь: Т. ГУ, 2000. Т. 6. С. 32-36.
7. Котов Е.А., Максимов А.М., Скворцов Л.М. Программный комплекс для автоматизированного исследования и проектирования промышленных роботов. М.: Машиностроение, 1991. 56 с.
8. Микрюков, В.Ю. Теория взаимодействия экономических субъектов. М.: Вузовская книга, 1999. 96 с.
9. Основы теории оптимального управления / под ред. В. Ф. Кротова. М.: Высшая школа, 1990. 430 с.
10. Сиразетдинов Т. К. Динамическое моделирование экономических объектов. Казань: Фан, 1996. 223 с.
11. Системы автоматического регулирования: практикум по математическому моделированию / под ред. Б. А. Карташова. Изд. 2-е, перераб. и доп. Ростов на Дону: Феникс, 2015. 458 с.
12. Шибко О.Н. Управление программой преобразований на предприятии по результатам моделирования его жизненного цикла: дисс. канд. техн. наук. Днепропетровск, 2011. 154 с.

13. Yershova Nina, Velmahina Natalia, Kovtun-Horbachova Tetiana. Simulation of the interaction process of three enterprises in the single production system. *Sustainable housing and human settlement*: Monograph. Dnipro – Bratislava, 2018. P. 222 – 228.
14. Yershova Nina, Velmahina Natalia, Shibko Oksana. Simulation of the interaction of two enterprises in the single production system. *Innovative lifecycle technologies of housing, industrial and transportation objects*: Monograph. Dnipro – Bratislava, 2018. P. 98 – 106.

**COMPUTER PROGRAMS FOR OPTIMAL DYNAMIC PROCESSES OF JOINT
VENTURE FOR PRODUCTION AND MARKETING OF GOODS DESIGN
DEVELOPMENT**

N. M. Yershova, N. O. Velmahina, N. S. Chupryna

Prydniprovskaya State Academy of Civil Engineering and Architecture
24a, Chernyshevskogo Street, Dnipro, 49000, Ukraine. E-mail:
nersova107@gmail.com, velmagina24@gmail.com, coderchan228@gmail.com

Creation of stable-working and efficient joint ventures for production and marketing of goods is the actual problem of the present day. To do that it is necessary to know values of optimal parameters that characterize joint venture enterprises interaction process. It was discovered that end product of joint venture that is supplied for external consumption depends on intermediate product which is left for development of own production by ventures. There is a problem how to define proportions of gross product flow that ventures should send on the development of own production to ensure effective functioning of joint venture. Besides, it's important to know optimal parameters of process of venture's gross product manufacture values. There are no computer programs for optimal production systems dynamic processes design. The purpose of this work is to develop computer programs for optimal venture's gross product manufacture process and three ventures of joint venture for production and marketing of goods interaction process design. Design solutions search algorithms are based on R. Bellman's matrix dynamic programming method for continual dynamic processes, which is scientific novelty of the work. Computer program «OPTIMA» was created to simplify joint ventures design process by optimal parameters selection and maximum achievable end product volume that is supplied for external consumption calculation. Computer program «SINTEZ» chooses optimal design parameters: BPA growth and retirement rates and calculates maximum achievable with available raw data gross product volume. This work is an important contribution in the field of computer science and software engineering.

Keywords: optimal dynamic process design, computer program, joint venture.

РОЗРОБКА АЛГОРИТМУ ВИЯВЛЕННЯ ЗАШУМЛЕННЯ ЯК ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, О.Ю. Лебедєва, Н.О. Бензар

Державний університет «Одеська політехніка»,
1, пр. Шевченка, Одеса, 65044, vikazorilo@gmail.com

Маніпуляції із зображеннями знизили нашу довіру до цифрових зображень, завдяки більш витонченим методам підробок, що стають все більшим викликом цілісності зображень та їх справжності. В епоху цифрових технологій наявність потужного та відносно недорогого програмного забезпечення для редагування зображень означає, що створення візуально переконливих фотопідробок поширюється з неймовірною швидкістю. Зростання маніпуляцій із фотографіями має наслідки майже у всіх сферах – від правоохоронних органів та національної безпеки до наукових видань, політики, засобів масової інформації та реклами. Важливість цього питання стає очевидною, якщо врахувати, що частіше за все в сучасному суспільстві ми все ще покладаємось на людей, які судять про достовірність зображення, але сучасні технології дозволяють обманути людське око. Проблема автентичності поширюється майже на всі цифрові зображення, від тих, які використовують як докази в залі суду, до тих, які ми бачимо щодня в газетах та журналах. Необхідна впевненість в тому, що у використуванні цифрові зображення не були внесені будь-які зміни. Оскільки мало уваги у відкритому друці приділяється виявленню обробки зображення різноманітними фільтрами, зокрема, фільтром графічного редактора AdobePhotoshop – шум з рівномірним розподілом, - метою даної роботи є підвищення ефективності виявлення обробки цифрового зображення шляхом розробки алгоритму виявлення шуму з рівномірним розподілом графічного редактора AdobePhotoshop. Розроблено алгоритм виявлення зазначеного фільтру, заснований на аналізі сингулярних чисел блоків матриці цифрового зображення. Експериментально встановлено, що кількість блоків необробленого зображення, найменше сингулярне число яких буде перевищувати значення 16, відносно до загальної кількості блоків не перевищує 0,14%. На основі результатів обчислювального експерименту розроблено алгоритм, ефективність якого оцінено в термінах помилок 1 і 2 роду: помилки першого роду не були виявлені, а помилки другого роду складають 0,89%.

Ключові слова: цифрове зображення, порушення цілісності цифрового зображення, сингулярні числа, матриця зображення, шум з рівномірним розподілом.

Вступ

Є безліч способів змінити зображення: фотомонтаж, клонування, різні фільтри графічних редакторів. І усі способи підробки впливають на математичні параметри зображення по-різному. Оскільки немає універсального методу виявлення порушень цілісності цифрового зображення, задача створення нових та вдосконалення існуючих методів пошуку слідів підробки є актуальною.

На сьогоднішньому рівні розвитку цифрові технології можуть імітувати майже все – музику, голос, зображення, рухомі об'єкти. Будь-які звуки генеруються в сучасних аудіоредакторах. Створити графічне зображення, яке буде схоже на звичайну фотографію, можна в графічному редакторі. У програмах 3D-моделювання створюють рухливі моделі, які неможливо відрізнити від об'єктів реальної відеозйомки. Всім цим дуже легко ввести в оману людей.

Цифрові зображення часто використовуються в суді в якості речового доказу або демонстративного матеріалу [1]. Тим не менше, ніколи не було так легко зробити так, щоб фотографії спотворювали правду, ніж зараз. Важливо визначити, чи є інформація, надана

слідству, правдивою та чи не спотворена вона.

Демонстративні докази можуть бути потужним інструментом, який допомагає присяжним зрозуміти важку концепцію, підкріпити їхні переконання, або навіть переконати їх повірити у щось. Правила допуску демонстративних доказів є менш суворими, ніж для речових доказів, що створює ще більший потенціал для допущення фальсифікованих цифрових зображень.

Ще однією галуззю, де фальсифікація зображень є важливою проблемою – це наука. В журналі ScientificReports¹⁰ вересня 2018 року було опубліковано суперечливу статтю [2], в якій стверджувалося, що гомеопатичний препарат з рослини отруйного плюща може полегшити біль у щурів. Незважаючи на те, що спочатку шум відбувся через запеклу дискусію щодо ефективності гомеопатії, він посилювався, коли виявилось, що стаття має фальсифіковане зображення [3].

Ще один приклад стався, коли дослідники, пов'язані з Міжнародним агентством Всесвітньої організації охорони здоров'я з дослідження раку (IARC), робили маніпулювання зображеннями в багатьох наукових роботах, які вони публікували протягом багатьох років. У період між 2005 і 2014 роками Массімо Томмазіно, керівник групи інфекцій та біології раку в IARC у Ліоні, Франція, та його колишній колега Узма Хасан опублікували безліч статей із підробленими зображеннями [4].

На нараді з плагіату в Лондоні в 2009 році, Вірджинія Барбур, головний редактор журналу PLoSMedicine, повідомила, що проблема маніпуляції зображеннями «підкралася» до редакторів журналів з моменту появи редагуючого програмного забезпечення, такого як, наприклад, Adobe Photoshop [5].

Часто потрібно більше, ніж добре навчене око, щоб виявити такі маніпуляції. Тут дуже доречні інструменти цифрової криміналістики. Програмне забезпечення використовується для виявлення навмисних змін зображень у наукових роботах. Навчання людей користуванню такими ресурсами також може зайняти час, але, як показують ці тривожні висновки, це є важливим для гарантування достовірності та наукової обґрунтованості.

Щоб впоратися з проблемою фальсифікації зображень, виникла сфера криміналістики цифрових зображень як основна галузь знань, зосереджена на перевірці справжності та цілісності цифрових зображень, яка забезпечила певну довіру до них. Важливість і актуальність криміналістики цифрових зображень залучила різних дослідників до створення методів виявлення фальсифікації зображень.

Методи виявлення цифрової підробки зображень поділяються на два підходи: активний та пасивний [6]. При активному підході цифрове зображення вимагає попередньої обробки зображення, наприклад, вбудовування водяних знаків або формування електронного підпису. Однак для цього типу технологій потрібно спеціальне програмне або апаратне забезпечення, щоб вставити або витягти інформацію.

На відміну від методів, що базуються на водяних знаках та підписах, пасивні методи не потребують цифрового підпису чи вбудовування будь-якого водяного знаку. Основний підхід, який використовується в переважній більшості алгоритмів, полягає в аналізі ковзного вікна [7]. Під ковзним вікном розуміється деяка локальна область зображення, яка послідовно проходить всі пікселі зображення. З порівняння характеристик центрального пікселя вікна з іншими пікселями вікна робиться висновок про його пошкодження. Відмінність методів детектування пошкоджених пікселів один від одного полягає у виборі розмірів ковзного вікна і алгоритму прийняття рішення про пошкодження пікселя [8-10]. Однак ефективність пошуку пошкоджених пікселів істотно залежить від налаштувань. Наприклад, алгоритм SD-ROM, що лежить в основі великої кількості інших алгоритмів, містить чотири параметри, які вибираються користувачем. Варіювання даних параметрів може змінювати ефективність пошуку пошкоджених пікселів від 62% до 96%. При цьому залишається високим відсоток помилкових спрацьовувань.

Поліпшення результатів вдається домогтися з використанням алгоритмів, які аналізують не тільки невелику локальну область, а й все зображення в цілому. В якості таких можна відзначити алгоритми на основі асоціативних правил, методах підтримки прийняття рішень, а також ті, що засновано на методах сегментації зображень. У всіх перерахованих алгоритмах один або два налаштовуваних параметра і досить висока ефективність виявлення пошкоджених пікселів. При цьому вдається істотно знизити відсоток помилкових спрацьовувань.

Один з фільтрів, що їх використовують при обробці цифрового зображення, фільтр графічного редактора AdobePhotoshop–шум з рівномірним розподілом. У відкритому друці не виявлено згадувань про методи виявлення цього шуму.

Мета роботи

Метою роботи є підвищення ефективності виявлення обробки цифрового зображення шляхом розробки алгоритму виявлення шуму з рівномірним розподілом графічного редактора AdobePhotoshop.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- визначити параметри цифрового зображення для аналізу;
- провести обчислювальний експеримент з використанням зображень, оброблених фільтром фоторедактору Adobe Photoshop «Шум з рівномірним розподілом»;
- розробити алгоритм методу виявлення обробки зображення фільтром «Шум з рівномірним розподілом» і провести аналіз його ефективності.

Зазначений фільтр графічного редактора AdobePhotoshop проявляється на зображенні у вигляді випадковим чином розташованих точок, які відрізняються від зображення більш світлим або темним відтінком кольору. Усюди далі під зашумленням ЦЗ будемо розуміти зашумлення з рівномірним розподілом графічного редактора AdobePhotoshop.

Основна частина

Основним параметром зашумлення у редакторі Photoshop є відсоток шуму. Чим більший відсоток, тим сильніший і помітніший шум. Зашумлення з великим відсотком у більшості випадків викликає підозри до ЦЗ, що є небажаним, якщо метою цього зашумлення було приховання результатів стеганографічної атаки чи фальсифікації.

У зв'язку з цим, для проведення дослідження було обрано значення шуму в 8% та 10%. Для цифрових зображень ефект зашумлення таких значень не є помітним при перегляді зображення в цілому. Вплив на ЦЗ шуму з різним відсотком показано на рисунках 1-4.



Рис. 1. Оригінальне зображення.



Рис. 2. Шум 10%.

Як бачимо, для цифрових зображень ефект зашумлення у 10% не є помітним.



Рис. 3. Шум у 50%.

Шум у 50% вже є сильно помітним. Бачимо, що чим більший відсоток зашумлення, тим помітніший шум.

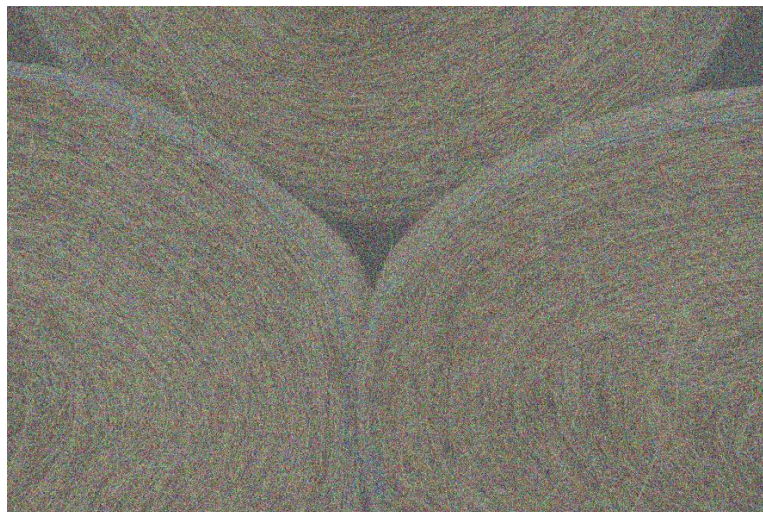


Рис. 4. Шум у 200%.

Вибір параметрів для аналізу обґрунтовано роботами [11-12]. В даних роботах доведено, що сингулярне розкладання однозначно визначає матрицю цифрового

зображення, тобто будь-які зміни в цифровому зображенні позначаються на сингулярних числах і векторах його матриці. Максимальне сингулярне число відповідає головним чином низьким частотам. Зі зменшенням сингулярного числа вклад низьких частот стає меншим, а високих – більшим. Сингулярні числа на відміну від сингулярних векторів є добре зумовленими, тобто зміни сингулярних чисел є порівняними з величиною збурюючої дії. Таким чином, для забезпечення принципової можливості отримання оцінки сили впливу зашумлення як набір формальних параметрів, які характеризують ЦЗ, з урахуванням мети роботи доцільно використовувати сингулярні числа (СНЧ) матриці ЦЗ [11-12].

Для визначення особливості поведінки СНЧ при наявності шуму було проведено аналіз сингулярних чисел блоків 8×8 матриць незашумлених ЦЗ та зображень, що піддавалися процедурі зашумлення. Аналіз проводився на множині V із 300 цифрових зображень, 100 з яких було знято на камеру смартфона Redmi Note 8T та збережено у форматі JPG (множина V_1), 100 – на непрофесійну фотокамеру (множина V_2), які також зберігаються у форматі JPG високої якості, 100 – професійні фотознімки з американської бази фотографій NSCR [13], які було взято у форматі без втрат TIFF (множина V_3). Всі цифрові зображення мали різну глибину різкості зображуваного простору. Шум з рівномірним розподілом в 30% (із 400 можливих) накладався в графічному редакторі Adobe Photoshop за допомогою меню «Додати шум» з типом розподілення «Рівномірний», що рівномірно розподіляє шум, на відміну від розподілу «За Гаусом», що створює різномірну структуру шумів [14]. Такий тип розподілення був обраний тому, що рівнорозподілений шум менш помітний на обробленому зображенні, тому для цілей фальсифікації є більш бажаним.

Усі ЦЗ представлено у колірній моделі RGB. Для роботи із зображенням у контексті поставленої мети не принципово, яку колірну компоненту аналізувати, адже для матриць R, G, B будуть приблизно однакові результати, а перевірка за всіма компонентами зображення значно подовжить тривалість роботи алгоритму. Тому обираємо будь-яку колірну компоненту і аналізуємо блоки цієї матриці.

В результаті аналізу було встановлено, що сингулярні числа блоків матриці зображення зростають до значень, які в нормальних умовах майже не зустрічаються. Тобто накладання шуму збільшує високочастотну складову до аномальних значень, що можна використовувати для ідентифікації шуму на зображенні. Зокрема, знайдено граничне значення найменшого сингулярного числа блоку матриці, рівне 16, що дозволяє відокремити переважну більшість зашумлених ЦЗ від незашумлених.

В результаті проведеного експерименту було визначено, що основна кількість блоків матриці, що мають значення останніх сингулярних чисел більше 16, в незашумлених цифрових зображеннях знаходиться в межах від 0 до 0,14% від загальної кількості блоків матриці ЦЗ (таблиця 1).

Таблиця 1.

Результати аналізу блоків СНЧ незашумлених ЦЗ

Відсоток блоків, що мають значення останнього СНЧ більше 16, відносно загальної кількості блоків	Кількість зображень
0-0,14%	297
$\geq 0,14\%$	3

У зображеннях формату JPG кількість таких блоків у 100% випадків менше 0,14% від загальної кількості блоків. У зображеннях формату TIFF кількість цих блоків в деяких випадках перевищує цей поріг (таблиця 2).

Таблиця 2.

Результати аналізу блоків СНЧ незашумлених ЦЗ різних форматів

Відсоток блоків, що мають значення останнього СНЧ більше 16, відносно загальної кількості блоків	Кількість зображень		
	JPG (V1)	JPG (V2)	TIFF (V3)
0-0,14%	100	100	97
≥0,14%	0	0	3

Дослідження проводилося на тій самій вибірці V із 300 зображень різного формату та різного розміру.

У зображеннях з накладеним шумом у 10% переважна кількість блоків, значення найменших СНЧ чисел яких більше за 16, перевищує 0,14% від загальної кількості блоків матриці зображення. У ЦЗ з шумом у 8% відсоток цих блоків такий, що однозначно відділити зашумлене цифрове зображення від норми неможливо (таблиці 3-4). Тому встановлюємо мінімальний відсоток зашумлення, яке можна виявити – 10%. Поріг кількості блоків цифрового зображення, значення останніх СНЧ яких більше 16, встановлюємо у 0,14% для оптимальної ефективності розпізнавання зашумлення.

Таблиця 3.

Результати аналізу блоків СНЧ ЦЗ з різним відсотком зашумлення

Відсоток блоків, що мають значення останнього СНЧ більше 16, відносно загальної кількості блоків	Кількість зображень	
	10%	8%
0-0,14%	0	251
≥0,14%	300	49

Таблиця 4.

Результати аналізу блоків СНЧ ЦЗ різних форматів з зашумленням 8%

Відсоток блоків, що мають значення останнього СНЧ більше 16, відносно загальної кількості блоків	Кількість зображень		
	JPG (V1)	JPG (V2)	TIFF (V3)
0-0,14%	100	87	64
≥0,14%	0	13	36

На підставі проведених досліджень розроблено алгоритм виявлення зашумлення ЦЗ, який складається з наступних етапів.

1. Отримати матрицю цифрового зображення R .
2. Розбити матрицю R на 8×8 -блоки b_{ij} , що не перетинаються (i, j – індекси блоку, що розглядається; $1 \leq i \leq \lfloor \frac{n}{8} \rfloor$, $1 \leq j \leq \lfloor \frac{m}{8} \rfloor$).
3. Обчислити сингулярні числа для кожного блоку b_{ij} .
4. Обчислити кількість блоків k , значення найменших сингулярних чисел яких більше 16.
5. Визначити відношення до загальної кількості блоків матриці ЦЗ (d).
6. Якщо $d \geq 0,14\%$, то зображення піддавалося процедурі зашумлення за допомогою накладання фільтру «Шум з рівномірним розподілом»; інакше – зображення не піддавалося обробці фільтром.

Аналіз ефективності розробленого методу показав, що помилки 2 роду склали 0,89%, а помилки 1 роду не були виявлені.

Висновки

У результаті виконання роботи було проведено аналіз існуючих методів перевірки цілісності цифрового зображення, який показав, що розробка та реалізація нових алгоритмів для виявлення фальсифікації цифрового зображення є надзвичайно актуальною задачею захисту інформації.

Було досліджено вплив фільтру графічного редактора AdobePhotoshop «Шум з рівномірним розподілом» на сингулярні числа блоків матриці цифрового зображення. В результаті встановлено, що аналіз найменших сингулярних чисел блоків дозволяє відділити оброблене зображення від необробленого.

В якості показника, що вказує на наявність обробки зображення, використано відношення блоків, найменше сингулярне число яких більше 16, до загальної кількості блоків. За результатами обчислювального експерименту встановлено, що коли значення даного відношення перевищує 0,14%, зображення є обробленим, інакше воно не є обробленим зазначеним фільтром.

Розроблено алгоритм виявлення фальсифікації цифрового зображення, кількість помилок 2 роду якого складає 0,89%, помилки першого роду не виявлені.

Список літератури

1. Parry Z. Digital manipulation and photographic evidence: defrauding the courts one thousand words at a time. *Journal of Law, Technology & Policy*. 2009. №2009. P. 175-202.
2. Magar S. Ultra-diluted Toxicodendron pubescens attenuates pro-inflammatory cytokines and ROS- mediated neuropathic pain in rats. *Scientific Reports*. 2018. № 8. P.1-11.
3. Guglielmi G. Peer-reviewed homeopathy study sparks uproar in Italy. *Nature*. 2018. № 562. P. 173-174.
4. Schneider L. Who cures cancer in Photoshop: URL: <https://forbetterscience.com/2018/10/11/who-cures-cancer-in-photoshop>.
5. Gilbert N. Science journals crack down on image manipulation. URL: <https://www.nature.com/articles/news.2009.991/box/1>.
6. Kumar B.S., Karthi S., Karthika K., Cristin R. A Systematic Study of Image Forgery Detection. *Journal of computational and theoretical Nanoscience*. 2018. № 15 (8). P. 2560–2564.
7. Garnett R., Huegerich T., Chui C., He W. A Universal Noise Removal Algorithm with an Impulse Detector. *IEEE Trans Image Process*. 2005. № 14 (11). P. 1747-1754.
8. Сорокин С.В., Щербаков М.А. Реализация SD-ROM фильтра на основе концепции нечеткой логики. *Известия высших учебных заведений. Поволжский регион*. 2017. № 3. С. 56-65.
9. Красовский Г.Я., Усс М.Л. Фильтрация изображений, искаженных импульсными помехами точечного и строчного типа, на основе систем интегрированных функций. *Радиоелектронні і комп'ютерні системи*. 2003. № 2. С. 47-55.
10. Chan R., Ho C., Nikolova M. Salt-and- pepper noise removal by median-type noise detectors and detail-preserving regularization. *IEEE Trans. Image Proc*. 2005. № 14 (10). P. 1479-1485.

11. Кобозева А.А. Использование теории возмущений для обнаружения фальсификации цифрового изображения. *Проблеми інформатиз. та управл. Матеріали міжнар. наук.-техн. конф. «Комп'ютерні системи та мережні технології»*. 2008. № 1. С. 16-22.
12. Кобозева А.А., Рыбальский О.В., Трифонова Е.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала. *Вісник Східноукраїнського національного університету ім. В. Даля*. 2008. № 8 (126), Ч.1. С.62–72.
13. NRCS Photo Gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата звернення: 30.05.2021).
14. Фильтры подменю «Шум» в Photoshop Elements. URL:<https://helpx.adobe.com/ru/photoshop-elements/using/noise-filters.html> (Дата звернення: 30.05.2021).

DEVELOPMENT OF AN ALGORITHM FOR DETECTION OF NOISE AS FALSIFICATION OF DIGITAL IMAGE

Zorilo V., Lebedeva O., Benzar N.

Odessa National Polytechnic University,
1, Shevchenko Ave, Odessa, 65044, Ukraine, whiteswanhelena@gmail.com

Image manipulation has decreased our confidence in digital images, thanks to more refined editing techniques which have become more and more of a factor in the integrity of images and their validity. In the era of digital technology, the availability of powerful and relatively inexpensive image editing software means that the creation of visually reproducible picture frames is expanding at an incredible speed. The growth of manipulations with photographs has consequences in almost all spheres - from law enforcement agencies and national security to scientific publications, politics, mass media and advertising. The importance of this issue becomes obvious, considering that in the modern society we still rely on people to judge the authenticity of the image, but modern technology allows to deceive the human eye. The problem of authenticity extends to all digital images, from those used as evidence in courtrooms to those we see every day in newspapers and magazines. It is necessary to make sure that the figures used have not been altered in any way. Since little attention is paid to the detection of image processing with various filters, in particular, the filter of the graphic editor Adobe Photoshop - noise with even distribution, - The aim of this work is to improve the efficiency of digital image processing by developing an algorithm for detecting noise with a uniform distribution of the graphical editor Adobe Photoshop. Developed an algorithm for detecting the specified filter based on the analysis of singular numbers of the digital image matrix blocks. It was experimentally established that the number of non-cropped image blocks, the smallest singular number of which will exceed the value of 16, in relation to the total number of blocks does not exceed 0.14%. Based on the results of the computational experiment the algorithm was developed, the efficiency of which was evaluated in terms of type 1 and type 2 errors: type 1 errors were not detected, while type 2 errors amounted to 0.89%.

Keywords: digital image, violation of digital image integrity, singular numbers, image matrix, noise with uniform distribution.

РОЗРОБКА ТРЬОХМОДУЛЬНОЇ КРИПТОСИСТЕМИ РАБІНА НА ОСНОВІ ОПЕРАЦІЇ ДОДАВАННЯ

М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко¹

Західноукраїнський національний університет, вул. Львівська, 11,
м. Тернопіль, 46020; E-mail: kasyanchuk@ukr.net,
lmt0902@gmail.com, jazkiv@ukr.net, stepan.ivasiev@gmail.com
¹Державний університет «Одеська політехніка», пр. Шевченка, 1,
Одеса, 65044. lmt0902@gmail.com

Сьогодні одним з найпоширеніших алгоритмів асиметричної криптографії є криптосистема Рабіна. Процес шифрування у ній подібний до криптосистеми RSA, однак замість модулярного експоненціювання використовується операція піднесення до квадрату за модулем. Це забезпечує більшу порівняно з RSA швидкодію алгоритму шифрування без втрати криптостійкості. Однак процес розшифрування вимагає значних обчислювальних та апаратних затрат. Тому метою даної роботи є розробка трьохмодульної криптосистеми Рабіна з використанням тільки операції додавання, а також дослідження її обчислювальної складності. Для виконання операції модулярного множення пропонується використати векторно-модульний метод, в якому множення замінюється операцією додавання відповідних величин. Для пошуку квадратичного лишку та відновлення десяткового числа за його залишками замість використання відповідно символів Якобі або Лежандра та китайської теореми про залишки використовуються методи додавання модуля та додавання добутку модулів. Це дозволяє зменшити обчислювальні складності вказаних операцій. Наведено схему трьохмодульної криптосистеми Рабіна та приклад її реалізації з використанням тільки операції додавання. Використання в даному підході однотипних суматорів замість мультиплексорів та перемножувачів дасть можливість зменшити апаратну та структурну складність схемотехнічного проектування трьохмодульної криптосистеми Рабіна. Для порівняння обчислювальної складності різних реалізацій криптосистеми Рабіна розглянуто її найбільш трудомісткі операції. Проведені дослідження свідчать про те, що реалізація трьохмодульного криптоалгоритму Рабіна за допомогою тільки операції додавання дає можливість зменшити обчислювальну складність базових операцій з кубічної до квадратичної. Представлено графічну залежність обчислювальної складності від розрядності чисел та кількості модулів. Показано, що із збільшенням цих аргументів обчислювальна складність реалізації криптосистеми Рабіна істотно зростає.

Ключові слова: трьохмодульна криптосистема Рабіна, додавання, векторно-модульний метод, обчислювальна складність, квадратичний лишок, китайська теорема про залишки.

Вступ

Використання засобів асиметричної криптографії набуває все більшого поширення в різного роду інформаційних системах [1]. З одного боку, це пов'язано з потребою суб'єктів системи у надійному механізмі забезпечення автентичності даних, які передаються, а з іншого - з тим, що сучасні криптографічні методи мають високий ступінь стійкості до криптоаналізу, що дозволяє суб'єктам системи бути абсолютно впевненими в їх надійності [2].

Однак найбільш поширені асиметричні криптосистеми Ель-Гамала, RSA, Рабіна [3] мають низьку продуктивність процесів шифрування/дешифрування інформації, оскільки їх математична реалізація ґрунтується на складних обчисленнях, що вимагають величезних витрат машинного часу і ресурсів. Крім того, для забезпечення достатнього рівня захисту інформації ставляться жорсткі вимоги до вхідних

параметрів, які повинні бути не меншими 2048 біт. В результаті цього асиметричні криптосистеми переважно використовуються для обміну криптографічними ключами і цифрового підпису.

Можливим рішенням проблеми низької продуктивності процесів шифрування/дешифрування інформації може бути створення асиметричних криптосистем на основі непозиційних систем числення [4], атакож використання векторно-модульного методу привиконання модулярних операцій множення і піднесення до степеня [5]. Найбільш перспективною для цього є система залишкових класів (зокрема, її досконала [6] і модифікована досконала [7] форми), яка дозволяє зменшити обчислювальну складність [8] на основі розпаралелення процесу обчислень, і виконання арифметичних операцій за допомогою векторно-модульного методу.

Аналіз досліджень та публікацій

Аналіз наукових досліджень показує [9, 10], що асиметрична криптосистема Рабіна, у якій процес шифрування подібний до RSA (замість експоненціювання використовується піднесення до квадрату), забезпечує більшу порівняно з RSA швидкодію алгоритму без втрати криптостійкості. Однак процес дешифрування вимагає значних обчислювальних та апаратних затрат у зв'язку з наявністю складних операцій пошуку квадратного кореня за модулем та відновлення десяткового числа за його залишками, який відбувається, як правило, на основі китайської теореми про залишки (КТЗ) [11].

Тому задача зменшення обчислювальної складності процесів шифрування/дешифрування інформаційних потоків у криптоалгоритмі Рабіна з використанням лише обчислювально простої операції додавання є надзвичайно актуальною [12].

Криптосистема Рабіна ґрунтується на складності факторизації та пошуку квадратичного лишку [13, 14]. Починається схема шифрування із генерації відкритого і таємного ключів. Для цього вибирають два простих великих числа p та q , які задовольняють умовам $p \equiv q \equiv 3 \pmod{4}$. Це суттєво спрощує і прискорює пошук квадратних коренів за модулями p та q . Потім обчислюють значення $N = p \cdot q$. Число N виступає відкритим ключем, а p та q - закритим.

Шифрування відкритого повідомлення M відбувається за формулою

$$C = M^2 \pmod{N}. \quad (1)$$

При дешифруванні шифртексту C вводять додаткові допоміжні величини v і m :

$$v = C \pmod{p}; \quad m = C \pmod{q}. \quad (2)$$

Для відновлення M потрібно знайти квадратичні лишки v та m відповідно за модулями p та q :

$$x^2 \equiv v \pmod{p}, \quad (3)$$

$$y^2 \equiv m \pmod{q}, \quad (4)$$

У результаті утворюються чотири системи порівнянь ($i=1 \dots 4$):

$$\begin{cases} M_i \equiv \pm x \pmod{p}; \\ M_i \equiv \pm y \pmod{q}. \end{cases} \quad (5)$$

Один з розв'язків (5), пошук якого здійснюється на основі КТЗ[15], і буде відкритим повідомленням M .

Аналіз літературних джерел дозволив виявити недоліки класичної криптосистеми Рабіна. Зокрема, у [16] авторам вдалося досягнути більшої криптостійкості без збільшення обчислювальної складності шляхом заміни квадратичної конгруенції на кубічне рівняння.

В [17] зазначено переваги використання гаусівських цілих чисел для генерації відкритого ключа криптосистеми Рабіна. Це дозволило розробити відповідну арифметику для теореми Вільсона і КТЗ, а також для обчислення символів Лежандра і квадратичних залишків.

У [10, 18] розглянуто трьох модульну криптосистему Рабіна (або H-Rabin), стійкість якої базується на розкладі добутку трьох чисел $N=pqr$ де p , q та r - прості числа. Це дозволяє збільшити величину блоку відкритого тексту без втрати криптостійкості, що забезпечує більшу захищеність криптосистеми від відповідних видів атак. Крім того, обґрунтовано використання модифікованої досконалої форми системи залишкових класів у криптосистемі Рабіна.

Однак у зазначених удосконаленнях використовуються обчислювально громіздкі модулярні операції множення багаторозрядних чисел, піднесення до квадрату, пошуку квадратичного залишку та оберненого елемента тощо.

Мета і задачі дослідження

Отже, метою даної роботи є розробка трьохмодульної криптосистеми Рабіна з використанням тільки операції додавання, а також дослідження її обчислювальної складності.

Для досягнення поставленої мети потрібно вирішити такі задачі:

- проаналізувати обчислювальні складності основних операцій трьохмодульної криптосистеми Рабіна;
- обґрунтувати використання векторно-модульного методу виконання модулярного множення;
- обґрунтувати використання методів додавання модуля та добутку модулів відповідно для пошуку квадратичного залишку та відновлення десяткового числа за його залишками;
- оцінити обчислювальну складність криптоалгоритму Рабіна на основі використання тільки операції додавання та порівняти його з існуючими методами.

Основна частина

Трьохмодульна криптосистема Рабіна на основі операції додавання.

Для зменшення обчислювальної складності у трьохмодульній криптосистемі Рабіна[10, 18] при шифруванні пропонується використовувати векторно-модульний метод модулярного множення. При цьому на першому етапі вибирають три великих простих числа p , q та r і обчислюють значення $N = p \cdot q \cdot r$, де N - відкритий ключ, числа p , q та r - таємний.

Шифрування відкритого повідомлення M відбувається за допомогою числа N за формулою (1).

На основі векторно-модульного методу модулярного множення значення $M \cdot M \pmod{N}$ шукають таким чином.

Відкритий блок M представимо у двійковій формі: $M = \sum_{i=0}^{n-1} a_i \cdot 2^i$, де $a_i = 0, 1$, n – розрядність модуля. Далі будуємо два вектор-рядки. В першому запишемо елементи a_i , в другому – $h_0 = 2^0 M \bmod N$, $h_i = 2 \cdot h_{i-1} \bmod N$ (таблиця 1).

Таблиця 1.

Вектор-рядки для модулярного множення

i	$n-1$	...	2	1	0
a_i	a_{n-1}	...	a_2	a_1	a_0
$h_i = 2 \cdot h_{i-1} \bmod N$	h_{n-1}	...	h_2	h_1	$h_0 = 2^0 \cdot M \bmod N$

Результат модулярного множення $M \cdot M \bmod N$ шукаємо згідно формули:

$$C = M^2 \bmod N = \left(\sum_{i=0}^{n-1} a_i \cdot h_i \right) \bmod N. \quad (6)$$

Отже, модулярне множення замінюємо операцією додавання тих h_i , для яких відповідні a_i рівні 1. Порівняно з класичними, даний метод характеризується меншою обчислювальною складністю виконання операції модулярного множення.

При дешифруванні криптограми C , аналогічно (2), вводимо допоміжні додаткові величини s , w і u :

$$s = C \bmod p; w = C \bmod q; u = C \bmod r. \quad (7)$$

Відповідно до (3), значення x , y і z шукають з таких порівнянь:

$$x^2 \equiv s \pmod{p}, y^2 \equiv w \pmod{q}, z^2 \equiv u \pmod{r}. \quad (8)$$

Для пошуку x , y та z потрібно обчислити значення квадратного кореня за модулем. Класичні підходи із використання символів Якобі чи Лежандра є досить трудомісткими [19]. Тому доцільно використати метод, що вимагає операції додавання і перевірки, чи є число повним квадратом. Така процедура дозволяє суттєво зменшити обчислювальну складність криптосистеми Рабіна. Отже, для пошуку значення $\sqrt{s} \bmod p$ необхідно виконати таку послідовність дій: $s + p$, $s + 2p$, ..., $s + i \cdot p$, де i – значення, при якому $s + i \cdot p$ буде повним квадратом. Аналогічно обчислимо $y^2 \equiv w \pmod{q}$, $z^2 \equiv u \pmod{r}$. Оскільки розв'язками порівнянь (6)-(8) буде 6 значень, то для пошуку M треба розв'язати вісім систем порівнянь, які утворюються комбінацією всіх можливих варіантів параметрів x , y та z ($i=1 \dots 8$):

$$\begin{cases} M_i \equiv \pm x \pmod{p}; \\ M_i \equiv \pm y \pmod{q}; \\ M_i \equiv \pm z \pmod{r}. \end{cases} \quad (9)$$

Шуканим повідомленням M буде один із розв'язків систем порівнянь (9). Для їх вирішення доцільно використати метод на основі додавання добутку модулів, який дозволяє зменшити обчислювальну складність в порівнянні з класичним: використанням КТЗ та алгоритму Гарнера [20].

На рисунку 1 представлена схема трьохмодульної криптосистеми Рабіна.

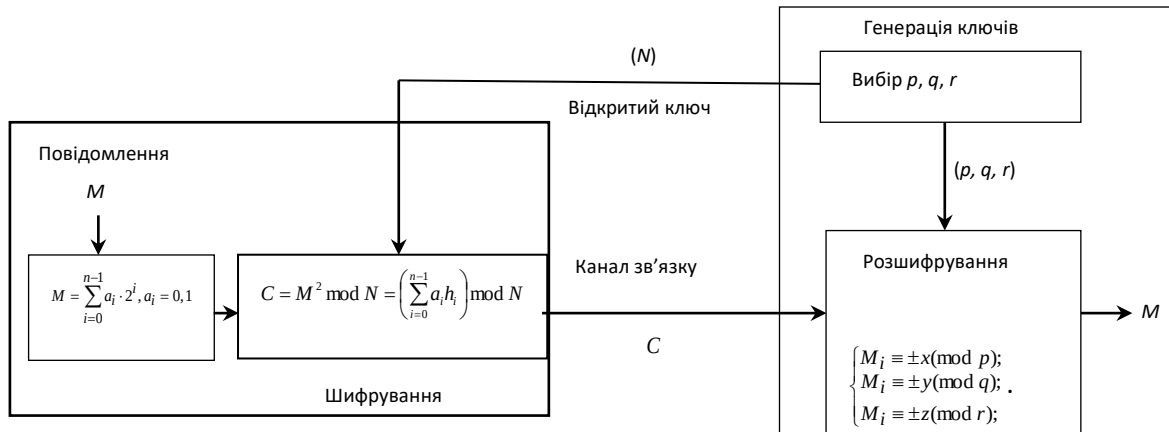


Рис. 1. Схема трьохмодульної криптосистеми Рабіна.

Для прикладу розглянемо одну із систем порівнянь (9), в якій параметри x, y, z додатні. Оскільки будь-яку конгруенцію $x \bmod p = M_1$ можна представити у вигляді $x = \gamma p + M_1$, де $\gamma = 0, 1, 2, \dots$, то до залишку $M_1^{(1)} = x$ потрібно додавати модуль p стільки разів, доки не буде виконуватись конгруенція $M_1^2 \equiv y \pmod{q}$, де $M_1^{(2)} = M_1^{(1)} + \gamma_1 p$. Далі треба додавати добуток pq , доки не буде виконуватись конгруенція $M_1^{(3)} \equiv z \pmod{r}$, де $M_1^3 = M_1^2 + \gamma_2 pq = M_1$. Аналогічно знаходять розв'язки інших систем порівнянь (9).

Слід зазначити, що в КТЗ та алгоритмі Гарнера необхідно шукати мультиплікативний обернений елемент за модулем [21]. При використанні багаторозрядних чисел класичні методи (повним перебором усіх можливих варіантів, використання теореми Ейлера чи алгоритму Евкліда [22]) характеризуються великою обчислювальною складністю, що призводить до збільшення обчислювальних характеристик при реалізації криптоалгоритму Рабіна.

Приклад застосування розробленого методу

Нехай, наприклад, таємним ключем криптосистеми Рабіна буде три простих числа $p=29, q=23, r=17$. Далі обчислюємо значення відкритого ключа: $N = p \cdot q \cdot r = 29 \cdot 23 \cdot 17 = 11339$.

У якості відкритого тексту для шифрування вибираємо повідомлення $M=381$. Тоді за формулою (1) на основі векторно-модульного методу модулярного множення обчислюємо значення $C = 381^2 \bmod 11339$.

Для цього повідомлення M записуємо в двійковій системі числення: $M=381=101111101_2$. Далі здійснюємо побудову двох вектор-рядків. У першому вказуємо елементи a_i , які можуть дорівнювати 0 або 1, в другому - елементи $h_i = 2^0 \cdot 381 \bmod 11339 = 381, h_1 = 2 \cdot 381 \bmod 11339 = 762, h_2 = 2 \cdot 762 \bmod 11339 = 1524, h_3 = 2 \cdot 1524 \bmod 11339 = 3048, h_4 = 2 \cdot 3048 \bmod 11339 = 6096, h_5 = 2 \cdot 6096 \bmod 11339 = 853, h_6 = 2 \cdot 853 \bmod 11339 = 1706, h_7 = 2 \cdot 1706 \bmod 11339 = 3412, h_8 = 2 \cdot 3412 \bmod 11339 = 6824$ (таблиця 2).

Таблиця 2.

Вектор-рядкимодулярного множення $381^2 \bmod 11339$

i	8	7	6	5	4	3	2	1	0
M_i	1	0	1	1	1	1	1	0	1
h_i	6824	3412	1706	853	6096	3048	1524	762	381

Результат модулярного множення $381 \cdot 381 \bmod 11339$ шукаємо за формулою (2):

$$C = 381^2 \bmod 11339 = (381 + 1524 + 3048 + 6096 + 853 + 1706 + 6824) \bmod 11339 = 9093.$$

Отже, модулярне множення замінюємо операцією модулярного додавання тих h_i , для яких відповідні a_i рівні 1.

При дешифруванні криптограми C , згідно (7), визначаємо допоміжні додаткові величини: $s = 9093 \bmod 29 = 16$; $w = 9093 \bmod 23 = 8$; $u = 9093 \bmod 17 = 15$.

Відповідно до (8), значення x , y і z обчислюємо з таких порівнянь: $x^2 \equiv 16 \pmod{29}$, $y^2 \equiv 8 \pmod{23}$, $z^2 \equiv 15 \pmod{17}$.

Отже, значення $\sqrt{16 \bmod 29} = \pm 4 \pmod{29}$. Щоб знайти $\sqrt{8 \bmod 23}$ згідно вище описаного методу, потрібно виконати таку послідовність дій: $8, 8+23=31, 31+23=54, 54+23=77, 77+23=100$. Оскільки 100 є повним квадратом, то $\sqrt{8 \bmod 23} = \pm 10 \pmod{23}$ ($-10 \bmod 23 = 13$). Аналогічно відбувається пошук $z \equiv \sqrt{15 \bmod 17} = \pm 7 \pmod{17}$ ($-7 \bmod 17 = 10$). Відповідно до (9), для розшифрування треба розв'язати вісім систем порівнянь, які утворені комбінаціями всіх можливих варіантів x , y та z ($i=1 \dots 8$):

$$\begin{cases} M_i \equiv \pm 4 \pmod{29}; \\ M_i \equiv \pm 10 \pmod{23}; \\ M_i \equiv \pm 7 \pmod{17}. \end{cases} \quad (10)$$

Розв'язок однієї з восьми систем буде шуканим значенням M . Для зручності доцільно сформувати вісім трійок отриманих залишків: 1) (4, 10, 7); 2) (4, 10, 10); 3) (4, 13, 7); 4) (4, 13, 10); 5) (25, 10, 7); 6) (25, 10, 10); 7) (25, 13, 7); 8) (25, 13, 10). У таблиці 3 продемонстровано процедуру розв'язку систем порівнянь у перших двох випадках, які відрізняються тільки останніми залишками. Видно, що вирішення першої системи отримуємо на п'ятій ітерації - $M_1 = 1367$. Після цього можна продовжити додавання добутку модулів $p \times q = 23 \cdot 29 = 667$ доки на десятій ітерації не буде справджуватися друга система: $M_2 = 4702$. Аналогічно будуюмо таблицю 4 для наступних двох систем конгруенцій.

Таблиця 3.

Процедура розв'язку перших двох систем конгруенцій, які відповідають трійкам (4, 10, 7); (4, 10, 10)

i	$4+(i-1) \times 29$	$(4+(i-1) \times 29) \bmod 23$
1	4	4
2	33	10
$p \times q = 23 \cdot 29 = 667$		
	$33+(i-3) \times 667$	$(33+(i-3) \times 667) \bmod 17$
3	33	16
4	700	3
5	1367	7
6	2034	11
7	2701	15
8	3368	2
9	4035	6
10	4702	10

Таблиця 4.

Процедура розв'язку перших двох систем конгруенцій, які відповідають трійкам (4, 13, 7); (4, 13, 10)

i	$4+(i-1)\times 29$	$(4+(i-1)\times 29)\bmod 23$
1	4	4
2	33	10
3	62	16
4	91	22
5	120	5
6	149	11
7	178	17
8	207	0
9	236	6
10	265	12
11	294	18
12	323	1
13	352	7
14	381	13
$p\times q=23\cdot 29=667$		
	$381+(i-15)\times 667$	$(381+(i-15)\times 667)\bmod 17$
15	381	7
16	1048	11
17	1715	15
18	2382	2
19	3049	6
20	3716	10

Розв'язок третьої конгруенції одержимо на п'ятнадцятій ітерації – $M_3=381$, а четвертої – на двадцятій: $M_4=3716$.

Решту чотири розв'язки можна знайти як різницю відкритого ключа N_i знайдених розв'язків: $M_5=11339-1367=9972$, $M_6=11339-4702=6637$, $M_7=11339-381=10958$, $M_8=11339-3716=7623$.

Отже, розв'язок $M_3=381$ відповідає відкритому тексту, всі інші розв'язки не будуть відповідати правильному випадку шифрування відкритого тексту.

Порівняння обчислювальних складностей криптоалгоритму Рабіна на основі векторно-модульного та класичного методів

Для порівняння обчислювальної складності різних реалізацій криптосистеми Рабіна необхідно розглянути найбільш трудомісткі операції, до яких відносять модулярне множення, пошук квадратичного лишку та відновлення числа за його залишками з використанням китайської теореми про залишки в класичному методі і додавання модулів або добутку модулів у запропонованому підході.

Обчислювальна складність операції модулярного множення векторно-модульним методом, в якому операція множення замінюється операцією додавання, характеризується лінійно-логарифмічною залежністю $O\left(\frac{n}{2}\log n\right)$.

З врахуванням того, що в запропонованому підході процес розшифрування зводиться до відновлення числа за його залишками на основі додавання добутку

модулів зі складностями $O(n)$ і $O(n^2)$ відповідно, то загальна обчислювальна складність становитиме $O\left(n^2\left(\frac{k^2+k}{2}\right) + \frac{n}{2}\log n\right)$, k – кількість модулів. Для прикладу, якщо $k=3$, то складність становить $O\left(6n^2 + \frac{n}{2}\log n\right) \approx O(n^2)$.

У класичній криптосистемі Рабіна, яка ґрунтується на розв'язанні систем конгруенцій з використанням китайської теореми про залишки чи алгоритму Гарнера, обчислювальна складність становить $O_1(kn^3 + n^2(2k+1) + nk) \approx O_1(n^3)$ та $O_2\left(kn^3 + n^2\left(\frac{k^2+k+2}{2}\right)\right) \approx O_2(n^3)$ відповідно.

На рисунку 2 представлена поверхня, яка характеризує графічні залежності обчислювальної складності запропонованого методу від кількості модулів та їх розрядності. Бачимо, що функція складності істотно зростає із збільшенням аргументів.

Проведені дослідження свідчать про те, що реалізація запропонованого алгоритмічного забезпечення трьох модульного криптоалгоритму Рабіна за допомогою тільки операції додавання дає можливість зменшити обчислювальну складність базових операцій з кубічної до квадратичної. Крім того, важливо, що даний підхід повинен спростити апаратну реалізацію та структурну складність при схемотехнічному проектуванні трьохмодульної криптосистеми Рабіна за рахунок використання однотипних суматорів замість перемножувачів та мультиплексорів.

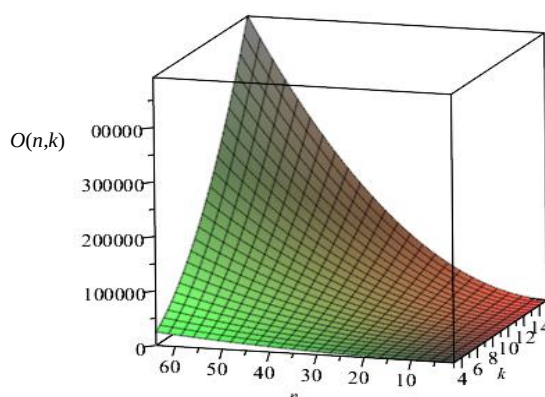


Рис. 2. Графічна залежність обчислювальної складності запропонованого методу від кількості модулів та їх розрядності.

Висновки

У роботі представлено розробку трьохмодульної криптосистеми Рабіна з використанням тільки операції додавання. Використання векторно-модульного методу виконання модулярного множення дозволяє пришвидшити процес шифрування/дешифрування інформаційних потоків шляхом заміни операції множення операцією додавання. Використання методів додавання модуля та добутку модулів замість відповідно символів Якобі або Лежандра та китайської теореми про залишки для пошуку квадратичного лишку та відновлення десяткового числа за його залишками дає можливість зменшити обчислювальну складність вказаних операцій. Даний підхід при схемотехнічному проектуванні трьохмодульної криптосистеми Рабіна дозволяє використовувати однотипні суматори замість мультиплексорів та

перемножувачів, зменшуючи при цьому апаратну та структурну складність реалізації. Проведені дослідження свідчать про те, що реалізація трьох модульного крипто алгоритму Рабіна за допомогою тільки операції додавання дає можливість зменшити обчислювальну складність базових операцій з кубічної до квадратичної. Показано, що із збільшенням розрядності чисел та кількості модулів обчислювальна складність реалізації криптосистеми Рабіна істотно зростає.

Список літератури

1. Adki V., Hatkar S.A Survey on Cryptography Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2016. Vol. 6 (6). P. 469-475.
2. Ambedkar B.R., Gupta A., Gautam P., Bedi S. An Efficient Method to Factorize the RSA Public Key Encryption. *Communication Systems and Network Technologies: Proceeding of International Conference*. 2011. P. 108–111.
3. Касянчук М.М., Якименко І.З., Волинський О.І., Пітух І.Р. Теорія алгоритмів RSA та Ель–Гамала в розмежованій системі числення Радемахера–Крестенсона. *Вісник Хмельницького національного університету. Технічні науки*. 2011. № 3. С. 265-273.
4. Roy R., Datta D., Bhagat S., Saha S., Sinha A. Comparative Study and Analysis of Performance samong RNS, DBNS, TBN Sand MNS for DSP Applications. *Journal of Signal and Information Processing*. 2015. Vol. 6. P. 49-65.
5. Николайчук Я.М., Касянчук М.М., Якименко І.З., Долинюк Т.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера. *Інформатика та математичні методи в моделюванні*. 2011. № 2. С. 123–130.
6. Касянчук М.М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія). Тернопіль: Економічна думка (ТНЕУ), 2019. 224 с.
7. Касянчук М.М. Побудова трьохмодульної модифікованої досконалої форми системи залишкових класів на основі розв'язку квадратного рівняння. *Інформатика та математичні методи в моделюванні*. 2016. Т. 6, №1. С. 19–25.
8. Ananda Mohan P.V. Residue Number Systems: The ory and Applications. Birkhäuser, 2016. 351 p.
9. Elia M., Schipani D. Onthe Rabinsignature. *J. Discrete Math. Sci. Cryptogr.* 2013. Vol. 16. №6, P. 367-378.
10. Kasianchuk M. Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S. Rabin's modified method of encryption using various forms of system of residual classes. *The Experience of Designing and Application of CAD System sin Microelectronics (CADSM-2017): Proceedings of the XIV International Conference*. Polyana-Svalyava. 2017. P. 222-224.
11. HemaV., Ganaga Durga M. Data Integrity Checking Based On Residue Number System and Chinese Remainder Theorem In Cloud. *International Journal of Innovative Researchin Science, Engineering and Technology*. 2014.Vol.3 (3). P. 2584-2588.

12. Касянчук М.М., Якименко І.З., Івасьєв С.В. Криптосистема Рабіна на основі операції додавання. *Математичне та комп'ютерне моделювання: Технічні науки*. 2019. В.19. С.145-150.
13. Hoffstein J., Pipher J., Silverman J. An Introduction to Mathematical Cryptography. Springer Science + Business Media, LLC, 2008. 524 p.
14. Jeffrey H., Jill P., Joseph H. An Introduction to Mathematical Cryptography. Berlin: Springer, 2008. 540 p.
15. Srivastava A., Mathur A. The Rabin cryptosystem and analysis in measure of chinese remainder theorem. *International Journal of Scientific and Research Publications*. 2013. Vol. 3 (6). P. 1-4.
16. Zheng Tian-Xiang. Enhanced Rabincrypto system based on cubic congruence equation. *Journal of Computer Applications*. 2009. №7. P. 121-129.
17. Yahia Awad, Abdu INasser El-Kassar, Therrar Kadri. Rabin Public-Key Crypto system in the Domain of Gaussian Integers. *Proceedings of the International Conference on Computer and Applications (ICCA)*. 2018. P. 1-11.
18. Hayder R.H. H-Rabim Cryptosystem. *Journal of Mathematics and Statistics*. 2014. Vol. 10 (3). P. 304-308.
19. Dasgupta S., Papadimitriou C., Vazirani U. Algorithms. Mc Graw-Hill Science, Engineering, Math. 2006. 336 p.
20. Svidan O., Zilic A. Direct residue-to-analog conversion scheme based on Chinese remainder theorem. *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems*. 2010. P. 687-690.
21. Касянчук М.М., Якименко І.З., Івасьєв С.В., Момотюк О.В. Експериментальне дослідження програмної реалізації методів пошуку оберненого елемента за модулем. *Інформатика та математичні методи в моделюванні*. 2017. Т.7, №3. С. 178-186.
22. Zhengbing Hu., Dychka I., Onai M., Bartkoviak A. The Analysis and Investigation of Multiplicative Inverse Searching Method in the Ring of Integers Modulo M. *International Journal of Intelligent Systems and Applications (IJISA)*. 2016. Vol. 8, №11. P. 9-18.

**DEVELOPING RABIN THREE-MODULAR CRYPTOSYSTEM BASED
ON THE OPERATION OF ADDITION**

Kasianchuk M.M., Lototsky O.Ya., Yatskiv S.V., Ivasiev S.V., Tymoshenko L.M.

West Ukrainian National University, 11, Lvivska Str., Ternopil, 46020, Ukraine;
E-mail: kasyanchuk@ukr.net, lmt0902@gmail.com,
jaskiv@ukr.net, stepan.ivasiev@gmail.com

Nowadays, one of the most common algorithms for asymmetric cryptography is the Rabin cryptosystem. The encryption process is similar to the RSA cryptosystem, but instead of modular exponentiation, the operation of squaring modulo is used. This provides faster performance of the encryption algorithm without the loss of cryptosecurity compared to RSA. However, the decryption process requires considerable time and hardware costs.

Therefore, the purpose of this work is to develop a three-modular Rabin cryptosystem using only the addition operation, as well as to study its time complexity. To perform the operation of modular multiplication, it is proposed to use a modular-vector method, in which multiplication is replaced by the operation of adding the appropriate values. The methods of adding module and product of modules are used to find the quadratic surplus and for decimal number recovery by its residues instead of using the Jacobi or Legendre symbols and the Chinese Remainder Theorem. This makes it possible to reduce the time complexity of these operations.

The scheme of three-modular Rabin cryptosystem and an example of its implementation based only on the addition operation are given. The use of one-type adders instead of multiplexers and multipliers in this approach allows one to simplify the hardware and structural complexities of the circuit design of a three-modular Rabin cryptosystem. To compare the time complexities in different implementations of the Rabin cryptosystem, its most time-consuming operations are considered.

The research conducted show that the implementation of a three-modular Rabin cryptosystem based only on the addition operation makes it possible to reduce the time complexity of basic operations from cubic to quadratic one. The graphical dependence of time complexity on digit capacity and a number of modules is presented. It is shown that with the increase of these arguments the time complexity of the implementation of the Rabin cryptosystem significantly increases.

Keywords: Rabin three-modular cryptosystem, addition, modular-vector method, time complexity, quadratic surplus, Chinese Remainder Theorem.

ДІАГНОСТИКА ХВОРОБИ СЕРЦЯ НА ОСНОВІ ДЕРЕВ РІШЕНЬ**В.Г. Пенко, І.М. Шпінарева, О.В. Ярошук**

Одеський національний університет імені І.І. Мечнікова, вул. Дворянська, 2,
м. Одеса, Україна, e-mail: vpenko@onu.edu.ua,
iryna.shpinareva@onu.edu.ua, ayaroshchuk43@gmail.com

Обсяг медичних даних в світі величезний. Швидко ростуть електронні історії хвороб. Тому для встановлення правильного діагнозу, при великій кількості різних аналізів (КТ, кардіограм і т.д.) на допомогу лікарю приходять інтелектуальні системи прогнозування серцево-судинних захворювань. Задачу прогнозування вирішують методами машинного навчання. Найбільш популярними методами машинного навчання в задачах класифікації та прогнозування є дерева прийняття рішень. Ідея, що лежить в основі дерев рішень, полягає в розбитті безлічі можливих значень вектора ознак (незалежних змінних) на непересічні безлічі і підгонці простої моделі для кожного такого безлічі. Дерева рішень дозволяють отримати високу точність у вирішенні багатьох задач, зберігаючи при цьому високий рівень інтерпретації. Дерево рішень будується автоматично в залежності від статистичних даних. У даній роботі досліджуються методи дерев прийняття рішень: CART, ID3, C4.5, Random Forest, Gradient Boosting. На основі аналізу даних методів кращий результат прогнозування серцево-судинних захворювань отримано алгоритмами Random Forest та Gradient Boosting. Метод випадкових лісів заснований на побудові ансамблю дерев рішень, кожне з яких будується за вибіркою, що отримується з вихідної навчальної вибірки за допомогою бутстрепа (тобто вибірки з поверненням). Іншим ансамблем є метод Gradient Boosting. Його основна відмінність від Random Forest полягає в тому, що в Random Forest дерева будуються незалежно один від одного, в той час як Gradient Boosting на кожному кроці покращує попередню модель. За допомогою дерева рішень (Random Forest та Gradient Boosting) можна з розумною точністю передбачити вразливість до серцевих захворювань у пацієнтів. У роботі пропонуються поліпшення методу Gradient Boosting шляхом модифікації бустінга. А саме, на кожному кроці алгоритму новий елемент ансамблю будується спираючись не на всю навчальну вибірку, а лише на випадкову підвибірку фіксованого розміру. Ця ідея є об'єднанням технік градієнтного бустінга і беггінга. В якості вихідних даних виористовується набір Heart Disease UCI. Для перевірки результатів роботи поліпшеного алгоритму Gradient Boosting використовувалася набір heart_failure_clinical_records. В результаті проведеної роботи отримано алгоритм, який дозволяє збільшити точність прогнозування серцево-судинних захворювань з 89% до 94%.

Ключові слова: інтелектуальна система прогнозування; алгоритм дерева рішень; прогнозування серцевих захворювань; ансамбль дерев рішень.

Вступ

Сьогодні багато країн зіштовхуються з настанням кризи в системі охорони здоров'я через зниження рівня глобального здоров'я населення, зростання поширеності хронічних захворювань (в першу чергу, серцево-судинних, онкологічних, covid), надзвичайно високу вартість лікування невідкладної патології. Тому обсяг медичних даних в світі величезний і швидко зростає у багатьох галузях медицини за останні десятиліття. Майбутнє медицини пропонує персоналізований мультимодальний підхід, орієнтований на інтегровану допомогу пацієнтові інтелектуальними системами підтримки прийняття рішень для лікарів. Системи підтримки прийняття рішень стають дуже важливою частиною прийняття медичних рішень, особливо в тих ситуаціях, коли рішення лікарем повинно прийматися швидко, ефективно і надійно. Оскільки для

виконання таких задач слід розглядати концептуально прості моделі прийняття рішень з можливістю автоматичного навчання, дерева рішень є дуже підходящим кандидатом. Вони вже успішно використовуються для прийняття ефективних рішень в багатьох предметних областях.

Переваги дерев рішень [1].

1. Інтуїтивність дерев рішень.
2. Дерева рішень дають можливість отримувати правила з бази даних на природній мові.
3. Алгоритм конструювання дерева рішень не вимагає від користувача вибору вхідних атрибутів.
4. Висока точність створюваних моделей.
5. Швидкий процес навчання.
6. Більшість алгоритмів конструювання дерев рішень мають можливість спеціальної обробки пропущених значень.

Огляд літератури

Точність прогнозування серцевої хвороби залежить від ефективності алгоритму машинного навчання. А навіть малі помилки в прогнозуванні хвороби можуть привести до смерті людини. На сьогоднішній день багато авторів досліджують методи прогнозування серцево-судинних захворювань.

В роботі [2] виконано прогнозування діагнозу серцевих захворювань за допомогою дерева рішень і наївного байєсівського алгоритму. Результати показують, що точність наївного Байєса і дерева рішень становить 85,03% і 84,01%.

В роботі [3] спочатку великі медичні дані розподілено в різні кластери за допомогою алгоритму KNN. Потім кожен кластер класифікується за допомогою класифікаційного алгоритму випадкового лісу. Порівняно з існуючими системами, експериментальні результати показують, що запропонований алгоритм підвищує точність даних.

Бабу та ін. в роботі [4] виконали діагностику серцевих захворювань з використанням генетичного алгоритму, алгоритму K-Means та дерева рішень. Результати показали, що дерево рішень має велику ефективність після застосування генетичного алгоритму.

В роботі [5] автори продемонстрували кілька моделей CART для прогнозування ішемічної хвороби серця, які демонструють максимально досягнутою точністю 100%. В роботі [6] автори показують, що комбінація алгоритму C4.5 і нечіткої експертної системи в прогнозуванні ішемічної хвороби досягає найвищої точності 81,82%.

Метою роботи є підвищення точності прогнозування захворювання серця шляхом дослідження і модифікації методу дерева рішень.

Алгоритми побудови рішення дерев: CART, ID3, C4.5, Random Forest, Gradient Boosting decision trees

Для прогнозування захворювання серця у пацієнта в роботі були досліджені алгоритми побудови рішення дерев: CART, ID3, C4.5, Random Forest, Gradient Boosting.

Дерево рішень – спосіб прийняття рішення, заснований на застосуванні різних функцій поділу вихідного набору даних, зокрема простих порогових правил [7]. Класифікаційно-регресійні дерева є популярною структурною моделлю прогнозування часових рядів.

Структурні моделі CART розроблені для моделювання процесів, на які впливають як безперервні зовнішні фактори, так і категоріальні.

Етапи побудови дерева рішень включають в себе наступні пункти:

- вибір критерію точності прогнозу;
- вибір типу розгалуження;
- визначення моменту припинення розгалужень;
- визначення відповідних розмірів дерева.

Дерева рішень, як і будь-який інший алгоритм машинного навчання, мають параметри, які визначають мету та напрямок виконання алгоритму і називаються критерієм інформативності.

Критерії інформативності можуть бути різними [7]: функція втрат, критерій Джині, ентропійний критерій і т. д. Також існують різні критерії зупинки.

Головна відмінність зазначених алгоритмів полягає в різних умовах інформативності. В алгоритмі ID3 використовується ентропійний критерій:

$$E(S) = \sum_{i=1}^c -p_i \log_2 p_i, \quad (1)$$

де p_i – частка об'єктів класу i , які потрапили в вершину S .

У алгоритмі C4.5 (поліпшена версія ID3) вибір атрибута відбувається на підставі нормалізованого приросту інформації (Gain Ratio). В алгоритмі CART використовується критерій Джині:

$$\text{Gini}(T) = 1 - \sum_{i=1}^n p_i^2, \quad (2)$$

якщо набір даних T містить дані n класів.

Дерева рішень ID3, C4.5, CART схильні до перенавчання і мають низьку узагальнюючу здатність, тому популярні алгоритми засновані на побудові великої кількості (ансамблю) дерев рішень: Random forest, Gradient Boosting.

Випадковий ліс рішень Random forest замість одного дерева використовує сукупність (ансамбль) дерев рішень, побудованих алгоритмом шляхом модифікації попереднього дерева. При цьому суть боротьби з проблемою неефективного вибору ознак полягає в використанні в процесі побудови дерева деяких випадкових вибірок, що прибирає детермінованість побудови дерева і робить цей процес стохастичним.

Опишемо алгоритм Random forest:

- 1) генерує випадкову підвибірку з повторенням розміром n з початкової вибірки;
- 2) будуємо дерево рішень, яке класифікує приклади такої підвибірки. Причому в ході створення чергового вузла дерева будемо вибирати ознаку, на основі якої проводиться розбивка, не по всіх M ознак, а лише з m випадково обраних. Вибір найкращого з цих m ознак може здійснюватися різними способами;
- 3) дерево будується до повного вичерпання підвибірки і не піддається процедурі відсікання.

Зрозуміло, що така схема побудови відповідає головному принципу ансамблювання: базові алгоритми повинні бути хорошими і різноманітними (тому кожне дерево будується на своїй навчальній вибірці і при виборі розщеплення є елемент випадковості).

Алгоритм Gradient Boosting починає роботу з побудови початкової моделі і коригує її, крок за кроком створюючи послідовність дерев регресії. Кожне дерево в послідовності створюється на підставі залишків моделі, яка зводиться на попередньому кроці. Залишки моделі по суті використовуються в якості цільової змінної. По суті вирішується задача (3).

$$F = \sum_{i=1}^m L(y_i, a(x_i) + b_i) \rightarrow \min \quad (3)$$

де $a(x_i)$ – спочатку побудований алгоритм, b_i – далі вибудовується алгоритм, який здійснює коригування відповідей $a(x_i)$ до вірних. Таким чином, поліпшується функціонал $\varepsilon_i = y_i - a(x_i)$.

Gradient Boosting має три основні компоненти.

1) Функція збитків – роль функції збитків полягає в оцінці того, наскільки модель здатна робити прогнози з урахуванням даних. Класичною функцією збитків є квадратична функція витрат:

$$L = (y - f(x))^2 \quad (4)$$

2) Слабкий учень – метод посилення градієнта, який приймає дійсне значення y і шукає наближення y у вигляді зваженої суми функцій $\hat{F}(x)$ з класу:

$$\hat{F}(x) = \sum_{i=1}^M y_i h_i(x) + \text{const} \quad (5)$$

3) Адитивна модель – це ітеративний та послідовний підхід додавання дерев (слабких учнів) по одному кроку за раз. Іншими словами, кожна ітерація повинна зменшити значення нашої функції витрат.

$$F_m(x) = F_{m-1}(x) + y_m h_m(x) \quad (6)$$

Джерела медичних даних

Джерела медичних даних включають в себе:

- клінічні дані для підтримки прийняття рішень різної спеціалізації (діагностичні, прогностичні, догляд за хворими і т.д.), у вигляді стандартизованих даних з електронних історій хвороби;
- зареєстровані дані з датчиків моніторингу і записуючих пристроїв.

В якості вихідних даних обрано діагностичні дані із набору Heart Disease [8]. Heart Disease містить у собі 303 екземпляри, що складаються з 14 атрибутів, таких як: вік, стать, біль у грудях, тиск, холестерин, цукор у крові, електрокардіографічні зміни у стані спокою, максимальний пульс людини, стенокардія, кількість великих судин, таласемія, наявність серцево-судинних захворювань. Більш точний опис атрибутів можна побачити у таблиці 1.

Для вибору алгоритму прогнозування захворювань в роботі були використані базові моделі алгоритмів ID3, C4.5, CART, Random forest та Gradient Boosting з бібліотеки sklearn. Тестування моделей відбувалося на наборі Heart Disease.

Таблиця 1.

Опис атрибутів	
Атрибут	Опис
age	Вік людини в роках
sex	Стать людини (1 = чоловік, 0 = жінка)
cp	Випробовувана біль в грудях (1: типова стенокардія, 2: атипова стенокардія, 3: чи не стенокардія, 4: безсимптомна)
restecg	Кров'яний тиск в стані спокою (мм рт.ст. при надходженні до лікарні)
chol	Вимірювання холестерину в мг / дл
fbс	Рівень цукру в крові людини натщесерце (> 120 мг / дл, 1 = true; 0 = false)
thalach	Електрокардіографічний вимір в спокої (0 = нормальне, 1 = з аномалією хвилі ST-T, 2 = виявлення ймовірної або певної гіпертрофії лівого шлуночка за критеріями Естес)
exang	Максимальний пульс людини
oldpeak	Стенокардія, індукована навантажувальним тестом (1 = yes; 0 = no)
trestbps	Депресія ST, викликана фізичними вправами щодо стану спокою
slope	Нахил сегмента ST в пік фізичних вправ (1: косовисхідний, 2: плоский, 3: кососпадний)
ca	Кількість великих судин (0-3)
thal	Захворювання крові під назвою таласемія (3 = нормальний; 6 = фікс. дефект; 7 = оборотний дефект)
target	Наявність серцево-судинного захворювання (0 = no, 1 = yes)

З метою підтвердження результативності роботи механізму прогнозування алгоритмів машинного навчання в роботі використовується метрика Ассурасу. Ассурасу – частка правильно класифікованих об'єктів показує ймовірність того, що клас буде передбачений правильно:

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)},$$

де TP -True positive, TN - True negative, FP - False positive, FN - False negative.

На рисунку 1 продемонстровано дерево прогнозування захворювання серця побудоване алгоритмом Random forest.

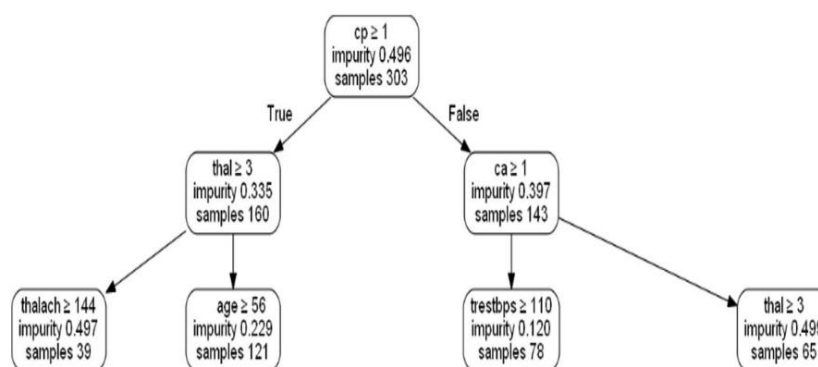


Рис. 1. Дерево рішень побудоване RF

Алгоритми з різними критеріями інформативності мають точність від 75,5% до 89,6% (рис.2).

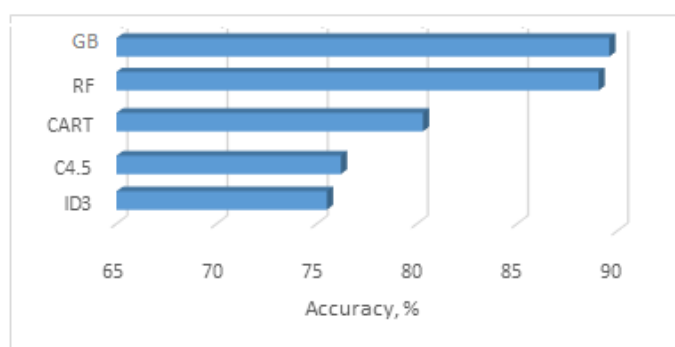


Рис. 2. Результати роботи алгоритмів дерева рішень для прогнозування захворювання

На основі даного аналізу в якості базового алгоритму обраний алгоритм Gradient Boosting, який має найбільшу точність в порівнянні з другими алгоритмами – 89,6%.

Алгоритм Gradient Boosting використовує такі гіперпараметри як:

- min_samples_split: мінімальне число точок, необхідне для розподілення. Корисно, щоб уникнути перенавчання;
- min_samples_leaf: мінімальна кількість елементів у листі або вузлів дерева. Менші значення слід вибирати для незбалансованих вибірок;
- min_weight_fraction_leaf: схожий на попередній, лише замість кількості задає долю від загального числа елементів;
- max_depth: максимальна глибина дерева. Використовується для боротьби з перенавчанням;
- max_leaf_nodes: Максимальне число листів у дерева. Якщо задати цей гіперпараметр, попередній ігнорується;
- max_features: кількість признаков, випробуваних алгоритмом при пошуку кращого розподілення.

Модифікації алгоритму Gradient Boosting

Враховуючи опис вище, реалізовано наступні модифікації базової версії алгоритму Gradient Boosting. Основна причина ефективності бустінга в тому, що алгоритм на кожній ітерації будує базовий алгоритм, який дійсно ефективний лише на частині підвибірки. Цей принцип можна посилити, зробивши модифікацію бустінга. А саме, на кожному кроці алгоритму новий доданок рахується спираючись не на всю навчальну вибірку, а лише на випадкову підвибірку фіксованого розміру. Ця ідея є об'єднанням технік градієнтного бустінга і бегінга. Також можна брати не випадкову підвибірку об'єктів, а ще й випадкову підвибірку ознак об'єктів. Це називається технікою

випадкових підпросторів. Результати роботи таких модифікацій часто помітно перевершують за якістю різні нестохастичні варіанти.

На кожній ітерації градієнтного бустінга алгоритм прагне максимально виправити всі помилки на навчанні. Однак це безглуздо при наявності шуму в вихідних даних і веде до перенавчання. Проблему можна вирішити, враховуючи ваги об'єктів на кожній ітерації, адже по них можна судити про складність навчання. Дійсно, велика вага у об'єкта показує, що попередні алгоритми погано працювали на ньому і, можливо, цей об'єкт шумовий.

Тому для поліпшення роботи алгоритму Gradient Boosting будемо виконувати наступні кроки:

1. отримаємо важливість атрибутів у датасеті;
2. на кожному кроці алгоритму новий доданок рахується спираючись не на всю навчальну вибірку, а лише на випадкову підвибірку фіксованого розміру;
3. на кожній ітерації будемо враховувати ваги об'єктів, адже по них можна судити про складність навчання на них;
4. виконуємо зміну гіперпараметрів: глибину дерева та мінімальну кількість елементів в узлі дерева

Дані для навчання та тестування ділимо у співвідношенні 1/2 на 1/2. Поділ на тестову та тренувальну вибірку реалізується випадковим методом. Набір даних неодноразово підбирався з випадковим поділом даних на навчальний і тестовий набір.

Для виконання таких умов була обрана мова програмування Python. Були використанні такі бібліотеки, як: `matplotlib` – для побудови графіків, `pandas` для перетворення даних, `sklearn.model_selection` – для розбиття даних.

Оцінка ефективності модифікованого алгоритму

Для виконання аналізу результатів потрібно створити порівняння декількох версій створеного алгоритму, щоб побачити чи принесли модифікації позитивний вплив на якість роботи алгоритму, або навпаки.

Для порівняння будуть використані наступні версії:

- базова версія алгоритму Gradient Boosting;
- версія алгоритму з попередньою обробкою даних;
- версія алгоритму з використанням техніки випадкових підпросторів;
- версія з видаленням шуму.

Кількість елементів тестової вибірки залежить від навчальної та складатиме 1/2 від початкової вибірки. Спочатку перевіримо важливості атрибутів, що обчислені в Gradient Boosting (рис.3).

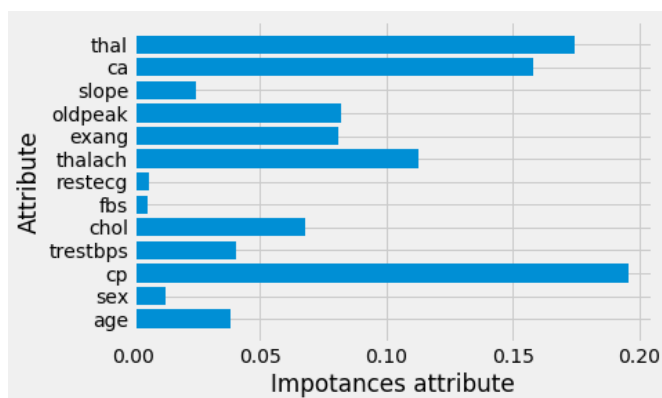


Рис. 3. Важливість атрибутів градієнтного бустінгу.

З цього графіку можна зробити висновок, що такі параметри, як кров'яний тиск в стані спокою та рівень цукру в крові мають найнижчу вагомість серед усіх ознак.

Базова версія цього алгоритму використовує 100 дерев з максимальною глибиною 3 і швидкості навчання 0.1, що дає результат у 84%

Для того, щоб побачити зміни в точності алгоритму, вирішено зробити попередню обробку даних – для цього з набору даних було видалено два атрибути з найменшою важливістю, та залишилися атрибути з важливістю більш рівною від 0.045 до 0.23 (рис.4). Це вплинуло на точності класифікації, яка склала 89%.

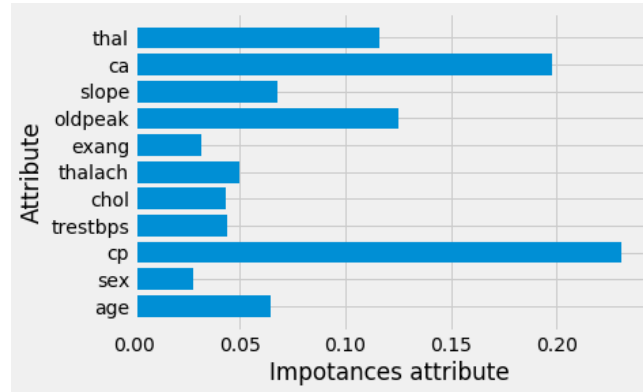


Рис. 4. Важливість атрибутів після попередньої модифікації.

Перевіримо версію алгоритму з використанням випадкових підпросторів, але не використовуємо попередню обробку даних. Будемо використовувати 25 дерев з максимальною глибиною 3 і швидкістю навчання 0.1. Цей алгоритм дав результат 92% точності. Графік залежності точності модифікованого алгоритму на тестовій вибірці на 25 тестах, зображений на рисунку 5.

Розглянемо той самий алгоритм, але з попередньою обробкою даних, де також використовуємо 25 дерев з тими самими параметрами. Результат роботи алгоритму з використанням випадкових підпросторів з попередньою обробкою даних має точність на тестовому наборі 93.814%. Графік залежності точності модифікованого алгоритму на тестовій вибірці, на 25 тестах, зображений на рисунку 6.

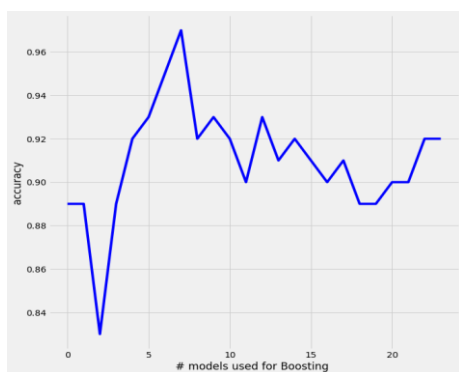


Рис. 5. Результат роботи алгоритму з використанням випадкових підпросторів без попередньої обробки даних

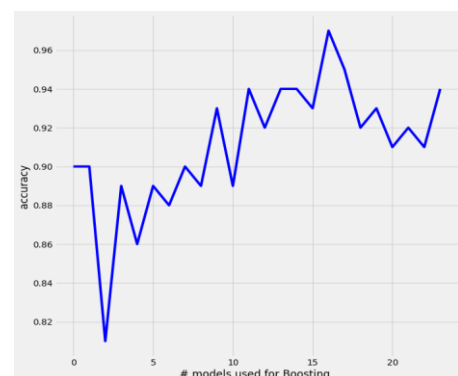


Рис. 6. Результат роботи алгоритму з використанням випадкових підпросторів з попередньою обробкою даних

Розглянемо модифікацію алгоритму з використанням випадкових підпросторів, але не використовуємо попередню обробку даних. Будемо використовувати 25 дерев з максимальною глибиною 2 і швидкості навчання 0.1. Цей алгоритм дав результат у 90% точності (рис. 7).

Розглянемо модифікацію алгоритму з використанням випадкових підпросторів, з попередньою обробкою даних. Використовуємо 25 дерев з максимальною глибиною 2 і швидкістю навчання 0.1. Цей алгоритм дав результат у 92% точності (рис. 8).

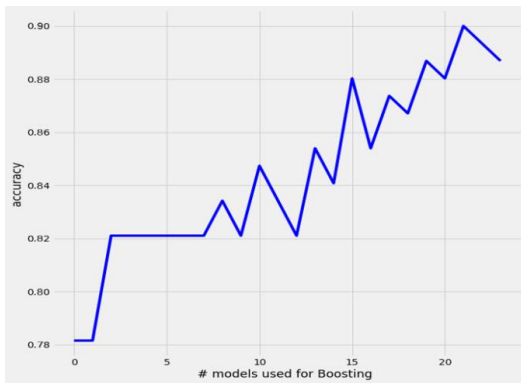


Рис.7. Результат роботи алгоритму з використанням випадкових підпросторів без попередньої обробки даних з глибиною 2

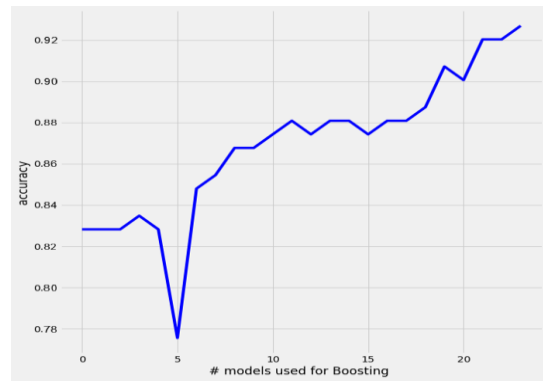


Рис. 8. Результат роботи алгоритму з використанням випадкових підпросторів з попередньою обробкою даних з глибиною 2

Розглянемо версію алгоритму з видаленням шуму без попередньої обробки даних. Запустимо алгоритм з видаленням шуму на наборах даних, з максимальною глибиною 3 та швидкістю навчання 0.1. Результатом роботи цього алгоритму є 85% на тестовій вибірці, та 100% на навчальній (рис.9). З чого можна зробити висновок, що алгоритм видаляє не тільки шуми, але і важливі ознаки, тобто використання цього алгоритму не є доцільним.

Розглянемо цей самий алгоритм з попередньою обробкою даних з тими самими параметрами. Як зображено на рисунку 10, попередня обробка даних не дала поліпшення результатів алгоритму, а навпаки, трохи зменшила точність.

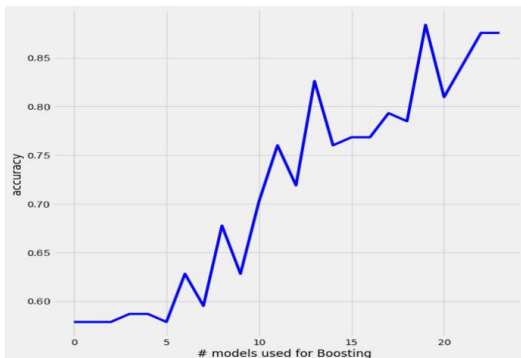


Рис. 9. Результат роботи алгоритму з видаленням шуму без попередньої обробки даних

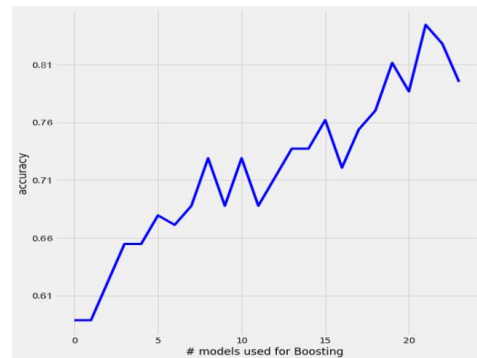


Рис.10. Результат роботи алгоритму з видаленням шуму без попередньої обробки даних

Таблиця 2.

Порівняння результатів роботи алгоритму GB і запропонованого алгоритму

Алгоритм	Accuracy, %
Базова версія алгоритму GB	84
Базова версія алгоритму з попередньою обробкою даних	89
Версія алгоритму з використанням випадкових підпросторів	92
Версія алгоритму з використанням випадкових підпросторів з попередньою обробкою даних	94
Версія алгоритму з видаленням шуму	85
Версія алгоритму з видаленням шуму з попередньою обробкою даних	81

Для того, щоб переконатися в результатах тестування запропонованих варіантів модифікованого алгоритму Gradient Boosting, протестуємо на dataset: kaggle / input /

heart-failure-clinical-data/heart_failure_clinical_records_dataset.csv.

Результати стандартного алгоритму Gradient Boosting тестування з урахуванням всіх параметрів 82.667%, з видаленням незначних параметрів 85.333%. Точність роботи модифікованого алгоритму Gradient Boosting з використанням випадкових підпросторів з $\text{max_dept} = 3$ і з видаленням незначних параметрів на даному датасеті має точність 93.97% (рис.11,12)

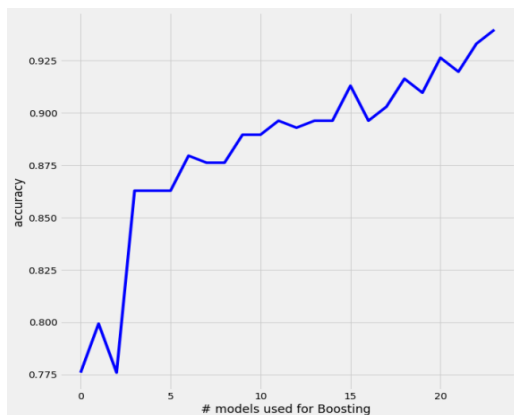


Рис. 11. Результат роботи модифікованого алгоритму Gradient Boosting використанням випадкових підпросторів з $\text{max_dept} = 3$

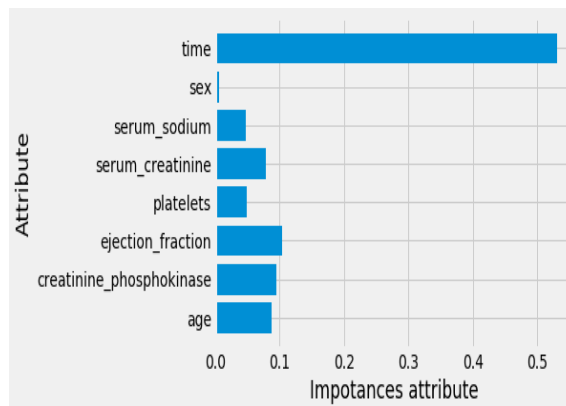


Рис. 12. Важливість атрибутів heart_failure_clinical_records_dataset.csv

Висновки

Аналізуючи алгоритми дерев прийняття рішень в задачі прогнозування серцево-судинних захворювань можна зробити висновок, що дерева рішень ID3, C4.5, CART мають недоліки, а саме, схильні до перенавчання і мають низьку узагальнюючу здатність, тому ефективніше використовувати ансамблі дерев рішень Random forest та Gradient Boosting. Дані методи були навчені і протестовані на базі Heart Disease та дали точність від 75,5 до 89,6. В роботі використано ансамблі дерев Gradient Boosting для прогнозування серцево-судинних захворювань. Виконані модифікації алгоритму Gradient Boosting: урахування важливості параметрів, використано метод випадкових підпросторів, видалення шуму та зміна гіперпараметрів. В результаті проведеної роботи отримано алгоритм, який дозволяє збільшити точність встановлення діагнозів з 89% до 94%.

Список літератури

1. Зайцева Т.В., Васина Н.В., Пусная О.П., Смородина Н.Н. Программная реализация метода деревьев решений для решения задач классификации и прогнозирования. *Научные ведомости. Серия. История. Политология. Экономика. Информатика*. 2013. №7 (150). Выпуск 26/1.
2. Venkatalakshmi B., Shivsankar, M. V. Heart disease diagnosis using predictive data mining. *International Journal of Innovative Research in Science, Engineering and Technology*. 2014. № 3(3), 1873-7.
3. Saravana K.R., Manikandan P. Medical Big Data Classification Using a Combination of Random Forest Classifier and K. Means Clustering, I.J. *Intelligent Systems and Applications*, 2018 №, 11, 11-19
URL: <http://www.mecs-press.org/>.

4. Babu S., Vivek E. M., Famina K.P., Fida K., Aswathi P., Shanid M., Hena M. Heart disease diagnosis using data mining technique. *IEEE International conference. Electronics, Communication and Aerospace Technology (ICECA)*. 2017. Vol. 1.P. 750-753).
5. Ghiasi M.M., Zendeboudia S., Mohsenipourb A.A. Decision tree-based diagnosis of coronary artery disease: CART model. *Computer Methods and Programs in Biomedicine*. 2020. Vol.192.
6. Baihaqi W.M., Setiawan N.A., Ardiyanto I. Rule extraction for fuzzy expert system to diagnose coronary artery disease. *IEEE International Conference in Information Technology, Information Systems and Electrical Engineering (ICITISEE)*.2016. P.136-141.
7. Митрофанов С.А. О модификации алгоритма обучения дерева решений, *Решетневские чтения*, 2018 Т. 2. С. 138-139.
8. Heart Disease Data Set URL: <https://archive.ics.uci.edu/ml/datasets/Heart+Disease>.

DIAGNOSIS OF HEART DISEASE BASED ON DECISION TREES

V.G. Pienko, I.M. Shpinareva, A.V. Yaroshchuk

Odessa I.I.Mechnikov National University, 2 Dvoryanska str.,
Odessa, Ukraine, e-mail: vpenko@onu.edu.ua,
iryna.shpinareva@onu.edu.ua, ayaroshchuk43@gmail.com

The volume of medical data in the world is enormous. Electronic medical records are growing rapidly. Therefore, in order to establish the correct diagnosis, with a large number of different analyzes (CT, cardiograms, etc.), intelligent systems for predicting cardiovascular diseases come to the aid of the doctor. The prediction problem is solved by machine learning methods. The most popular machine learning method for classification and prediction are decision trees. The idea behind decision trees is to split the set of possible values of the feature vector (independent variables) into disjoint sets and fit a simple model for each such set. Decision trees allow you to get high accuracy in solving many problems, while maintaining a high level of interpretation. The decision tree is built automatically depending on the statistical data. This paper examines different types of decision trees: CART, ID3, C4.5, Random Forest, Gradient Boosting. Based on the analysis of these types, the best result for predicting cardiovascular diseases was obtained by the Random Forest and Gradient Boosting methods. The random forest method is based on the construction of an ensemble of decision trees, each of which is constructed from a sample obtained from the original training sample using a bootstrap. Another ensemble is the Gradient Boosting method. Its main difference from Random Forest is that in Random Forest trees are built independently of each other, while Gradient Boosting improves the previous model at every step. Using a decision tree (Random Forest and Gradient Boosting), you can predict the vulnerability to heart disease in patients with reasonable accuracy. The paper proposes improvements to the Gradient Boosting method by modifying boosting. Namely, at each step of the algorithm, a new ensemble item is constructed based not on the entire training sample, but only on a random subsample of a fixed size. This idea is a combination of gradient boosting and bagging techniques. The Heart Disease UCI set is used as initial data. The heart_failure_clinical_records set was used to test the performance of the improved Gradient Boosting algorithm. As a result of the work carried out, an algorithm was obtained that allows increasing the accuracy of predicting cardiovascular diseases from 89% to 94%.

Keywords: intelligent forecasting system; decision tree algorithm; predicting cardiovascular disease; an ensemble of decision trees.

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ПОВЕДІНКИ ВІРТУАЛЬНОГО НАТОВПУ

О.М. Симонова, І.І. Бобок

Державний університет «Одеська політехніка»,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

Прогнозування натовпу є відносно новою задачею при прогнозуванні майбутнього. Сьогодні натовп, який вивчався класичною соціальною психологією, зазнав значних змін, що призвело до появи такого поняття, як «Інтернет-натовп». Технологія «Інтернет-натовпу» на сьогодні використовується для створення «мертвих душ», тобто фейкових акаунтів, з використанням фальшивих імен та адрес, за допомогою яких формується, поширюються думки та/або нав'язується образ думок справжнім користувачам. Метою роботи є розробка математичної моделі віртуального натовпу для прогнозування його поведінки й розрахунок ймовірності переходу віртуального натовпу в реальний. В роботі проведено виокремлення найбільш важливих факторів, що впливають на зародження протестних рухів шляхом формування віртуального натовпу. Показано, що людині, що живе в країні з високим рівнем економічного розвитку, легше прийняти рішення про участь в акції протесту через упевненість в подальшому стабільному розвитку держави. Продемонстровано значення Інтернет-цензури у сучасному світі і можливості впливу цього фактору на утворення первинних груп протестувальників у віртуальному середовищі. Використані в роботі методи математичного моделювання дають змогу отримати науково обгрунтовані варіанти розвитку й ймовірність змін, які віртуальний натовп зазнає в часі, аж до свого переродження у реальний рух. Таким чином, оцінка ймовірності переходу натовпу з віртуального стану в реальний, є важливою і актуальною як з точки зору безпеки окремого громадянина і суспільства, так і з точки зору безпеки держави в цілому. Запропонована модель дасть змогу розробити рекомендації фахівцям, які допомагають забезпечувати високий рівень безпеки в звичайних і екстремальних ситуаціях, оптимізувати розбудову міст з точки зору ефективності проходження людського потоку, а також ефективно управляти транспортним потоком.

Ключові слова: Інтернет-натовп, ймовірність, протестний рух, математична модель

Вступ

Прогнозування натовпу є відносно новою задачею в прогнозуванні майбутнього.

Натовп – це безструктурне скупчення істот, які позбавлені певної спільної мети, але при цьому пов'язані схожим емоційним станом і єдиним об'єктом уваги. Індивід, опинившись в натовпі, втрачає свою своєрідність і дозволяє іншим на себе впливати. Це призводить до того, що натовп, який є скупченням окремих індивідів, втрачає відчуття відповідальності за скоєні вчинки, а окрема людина дозволяє інстинктам взяти гору над розумом [1].

Індивідуальна поведінка людини поза натовпу характеризується великою кількістю чинників, які пов'язані з його інтелектуальною діяльністю. Однак, тим не менше, людина, як частина натовпу, втрачає свою індивідуальність, після чого починає підкорятися звичайним законам поведінки. Через це натовп набуває якості, які не є характерними для її незалежних учасників.

Сьогодні натовп, який вивчався класичною соціальною психологією, зазнав зміни. Це обумовлюється стрімким розвитком і просуванням інформаційних

технологій, що, в кінцевому підсумку, призвело до появи такого поняття, як «Інтернет-натовп».

«Інтернет-натовп», або «мережевий натовп», є технологією для створення «мертвих душ», тобто фейковий акаунтів, з використанням фальшивих імен та адрес, за допомогою яких формується, нав'язується і поширюється думка і образ думок справжнім користувачам [2].

Віртуальний натовп частіше за все покликаний:

- демонструвати, як активно підключається «суспільство» в обговорення рішень, реформ, подій;
- показувати, що «суспільство» не схвалює або гаряче підтримує якісь погляди;
- перемикає увагу аудиторії з однієї теми на іншу;
- дискредитувати авторів думок і творів;
- сіяти сумніви в правдивості популярних фактів, в обґрунтованості аргументів і логічності висновків;
- піднімати онлайн-повстання, утворюючи ефект включеності в протест сотень, тисяч, мільйонів людей [3].

Інтернет-натовп може впливати й на процеси, які пов'язані із національною безпекою. Це своєрідні революційні дії, які свого часу призводили до повалення монархій, до перерозподілу воєнного середовища у світі та інше. Але віртуальний натовп має безліч особливостей, які потребують додаткового дослідження та прогнозування. Прикладом тому служить безліч протестів, влаштованих за допомогою Інтернету (Євромайдан, #BlackLivesMatter тощо), і які у наслідку призводили до значних змін в політичній сфері.

Таким чином актуальність дослідження полягає у тому, що у сучасному світі Інтернет стає вагомим фактором, що впливає на зародження протестних рухів шляхом формування віртуального натовпу. Аналіз подій Арабської весни та Кольорових революцій показав, що спочатку формуються первинні групи у мережі Інтернет – віртуальні натовпи, які потім при певних умовах переходять у реальний натовп на вулицях міст.

Метою роботи є розробка математичної моделі віртуального натовпу для прогнозування його поведінки й розрахунок ймовірності переходу віртуального натовпу в реальний.

Основна частина

Параметри математичної моделі. Формування реального натовпу, шляхом використання Інтернету, можна поділити, як мінімум на два етапи:

- 1) створення Інтернет-натовпу. Поширення однієї або більше публікацій, на соціальну або політичну теми, із зазначенням місця та часу передбачуваної протестної акції;
- 2) утворення реального натовпу. Збори фізичних осіб в зазначений час і місце.

Масштабні акції протесту часто несуть за собою економічні збитки для країни. Передбачається, що людині, що живе в країні з високим рівнем економічного розвитку, легше прийняти рішення стати учасником акції протесту через упевненість в подальшому стабільному розвитку держави.

Одним з економічних показників є валовий національний дохід на душу населення. Цей показник дає уявлення про кількість вироблених товарів і послуг, що припадають в середньому на одного жителя держави. Даний показник визначає приблизний рівень якості життя та добробуту країни.

Інший показник рівня якості життя – очікувана тривалість життя при народженні. Цей показник залежить від багатьох чинників: від способу життя, рівня доходів, виховання і освіти людини, спадковості, рівня забруднення навколишнього середовища, якості харчування, розвитку системи охорони здоров'я, рівня злочинності, можливості спокійно заробляти на життя і багатьох інших.

Індекс людського розвитку (ІЛР) є складовим показником, що фокусується на трьох основних вимірах людського розвитку: здатності вести довге і здорове життя (вимірюваної показником очікуваної тривалості життя при народженні); здатності отримувати знання (вимірюваної середньою тривалістю навчання і очікуваною тривалістю навчання); і здатності досягати гідного рівня життя (вимірюваної показником валового національного доходу на душу населення) [4].

Здатність отримувати знання безпосередньо впливає на здатність вести довге і здорове життя, а також на здатність досягати гідного рівня життя.

Здатність отримувати знання вимірюється середньою тривалістю навчання і очікуваною тривалістю навчання і обчислюється за формулою [5]:

$$EI = \frac{MYSI + EYSI}{2} \quad (1)$$

де $MYSI$ – індекс середньої тривалості навчання (2);
 $EYSI$ – індекс очікуваної тривалості навчання (3).

$$MYSI = \frac{MYS}{15}, \quad (2)$$

$$EYSI = \frac{EYS}{15}. \quad (3)$$

Процес утворення змушує людський мозок працювати і тим самим спонукає до отримання та аналізу інформації з різних зовнішніх джерел. Це дає людині можливість вміти приймати самостійні рішення, безпосередньо впливає на розвиток громадянської позиції кожного індивіда, дає чітке уявлення про історію та культуру його країни, позначаючись на патріотичних почуттях людини. Освіта виступає важливим критерієм соціалізації особистості, а також одним із критеріїв соціальної стратифікації.

Індекс очікуваної тривалості життя обчислюється за наступним виразом [5]:

$$LEI = \frac{LE - 20}{85 - 20}, \quad (4)$$

де LE – очікувана тривалість життя.
Індекс доходу обчислюється за формулою [5]

$$II = \frac{\ln(GNIpc) - \ln(100)}{\ln(75000) - \ln(100)} \quad (5)$$

де GNIpc – валовий національний дохід на душу населення за паритетом купівельної спроможності в доларах США.

ІЛР є середнім геометричним цих трьох індексів [5]:

$$ILP = \sqrt[3]{LEI \cdot EI \cdot II} . \quad (6)$$

Для формування натовпу шляхом використання Інтернету, необхідний достатній відсоток проникнення в Інтернет на території країни. У даній роботі використовуються дані міжнародного веб-сайту Internet World Stats, на якому представлені актуальні дані про світових користувачів Інтернету, статистику населення, соціальних мережах і дані досліджень Інтернет-ринку для більш ніж 250 окремих країн і регіонів світу.

Охоплення аудиторії показує число унікальних користувачів, що побачили публікацію. Щоб користувач був зарахований як "унікальний", йому не обов'язково як-небудь взаємодіяти з публікацією, досить лише одного разу подивитися її. Однак варто зазначити, що охоплення відрізняється від звичайних переглядів. Останні зараховуються під час кожного показу опублікованого контенту, навіть якщо один і той же користувач бачить публікацію кілька разів. Іншими словами, це те, скільки разів була показана публікація. Охоплення ж означає число унікальних користувачів, які переглянули запис. Існує кілька видів охоплення, а саме [6]:

- рекламний, що включає в себе користувачів, які побачили рекламні оголошення на сторінці;
- органічний, що включає в себе тільки підписників сторінки, які побачили публікацію;
- віральний, що включає в себе користувачів, які не були підписані на сторінку, яка зробила публікацію.

Наприклад, сторінка має двісті підписників, з них публікацію подивилися сто п'ятдесят – це буде органічним охопленням публікації, інші п'ятдесят користувачів відносяться до вірального охоплення.

Рівень залученості – це показник, який визначає для контенту рівень віддачі від аудиторії. Він показує кількість людей взаємодіючих з контентом. Фактори, що впливають на залученість, включають коментарі користувачів, репости, лайки і багато іншого.

Коефіцієнт залучення за охопленням (*engagement rate by reach*, ERR) обчислюється за такою формулою [7]:

$$ERR = \frac{\text{залучення на пост}}{\text{охоплення поста}} . \quad (7)$$

При множенні результату на 100, підсумкове значення покаже відсоток людей, які проявили активність до конкретної записи. Так само варто відзначити, що охоплення є відносним показником і може змінюватися під впливом різних факторів: наприклад, від часу доби або вірального охоплення поста.

При високому віральному охопленні публікація може вважатися вірусної. Через це, вийшовши за межі сторінки за допомогою репоста, і опинившись в стрічці підписників, публікація отримає велике охоплення і, щодо загальної цифри охоплення, мале значення залученості. Через це процентний показник ERR публікації впаде.

У соціальних мережах з розумною (алгоритмічною) стрічкою, яка підбирає контент, згідно інтересам користувача, публікацію можуть побачити вузька частина

аудиторії, які проявляють активність, так як спочатку були зацікавлені в контенті. В цьому випадку при низькому охопленні поста буде високий рівень залучення.

Аналізуючи ці два випадки, можна прийти до висновку, що залученість за охопленням підійде в тих ситуаціях, коли потрібно оцінити приблизний відсоток користувачів, які проявляють активність серед переглянутих публікацій, в той час як для порівняння якості публікації використання ERR не буде ефективним.

Дані за охопленням можуть бути доступні лише адміністратору (власнику) сторінки, тому якщо немає даних щодо охоплення, слід використовувати формулу співвідношення залученості на пост і кількості підписників (ER), яка обчислюється за формулою [7]:

$$ER = \frac{\text{залучення на пост}}{\text{кількість підписників}}. \quad (8)$$

Від кількості учасників, залучених в створення віртуальної натовпу, залежить швидкість поширення інформації. Так, одній людині буде потрібно значно більше часу для формування віртуального натовпу, ніж, наприклад, десятком людям, які будуть писати пости з одним і тим же посилком.

Варто зазначити, що поняття «натовп» у багатьох словниках розглядається як «велике скупчення людей», хоча ніде немає точної кількості людей, які утворюють натовп. У роботі під натовпом мається на увазі п'ять і більше осіб.

Передбачається, що кожен користувач, залучений в інформування про заклик до участі в протесті, є потенційним учасником цього протесту. Таким чином, якщо число перших користувачів, які зробили публікацію, менше п'яти, то вони не сформуєть на думку авторів цієї роботи реальну натовп, навіть якщо відвідають вказане ними місце протесту. Однак, іноді пост цілком може стати «вірусним». Йона Бергер у своїй книзі «Заразливий» вивчив більше 7000 статей в New York Times, і виділив шість чинників, які впливають на віральність контенту [8]:

- соціальна валюта: якщо людина ділиться унікальним і корисним контентом, то він тим самим піднімає свій соціальний статус в очах підписників, постає таким собі дослідником, який володіє унікальним доступом до першоджерел;
- тригери: люди говорять про те, що думають, тому за умови, що контент потрапляє в інформаційне поле аудиторії, вони почнуть ділитися ним з іншими;
- емоції: контент, що чіпляє сильні почуття аудиторії, легко отримує вибухову реакцію і, як наслідок, поширення;
- соціальні докази: якщо контент має високу залученість, то подальше поширення публікації буде протікати все легше: це обумовлюється тим, що люди схильні повторювати дії один одного;
- практична цінність: люди охоче діляться контентом, якщо завдяки йому, вони знайшли відповідь на своє питання, змогли або тільки планують чогось навчитися;
- історії: контент може бути проілюстрований історією з життя.

Проте, в різних соціальних мережах можуть діяти різні умови для більшої популярності публікації.

На основі даних статистичного звіту Popsters за 2020 [9] рік була виведена закономірність між кількістю символів в публікації і її вмістом в різних соціальних мережах (Таблиця 1). Наприклад, в Twitter текстової публікації довжиною до 160 символів легше набрати популярність, ніж твіти довжиною більше 160 символів з

наявністю відео. А ось в Tumbler наявність відео краще, а довжина тексту бажана від 160 символів.

Таблиця 1.

Закономірність ефективності публікації у певних соціальних мережах

Соціальна мережа	Обсяг тексту N			Зміст тексту Y		
	Ефективний	Менш ефективний	Неефективний	Ефективний	Менш ефективний	Неефективний
Facebook	$N \leq 160$	$160 < N \leq 1000$	$N < 1000$	Фото		Відео, посилання
Instagram	$160 < N \leq 1000$		$N \leq 160$; $N < 1000$	Фото	Посилання	Відео
Twitter	$N \leq 160$		$N < 280$		Фото, Посилання	Відео
YouTube	$160 < N \leq 1000$	$N < 1000$	$N \leq 160$			
Tumbler	$160 < N \leq 1000$	$N < 1000$	$N \leq 160$	Відео	Фото, Посилання	
Telegram	$N \leq 160$, $160 < N \leq 1000$		$N < 1000$		Фото, Посилання	Відео

Проте, навіть якщо повідомлення мало всі підстави набрати достатньо послідовників для формування реальної натовпу або навіть стати вірусним, при ретельній Інтернет-цензури в країні термін існування цього повідомлення обмежений.

Інтернет-цензура – це контроль та припинення публікації або доступу до інформації в мережі Інтернет. Інтернет-цензура накладає обмеження на те, яка інформація може бути розміщена в Інтернеті.

Цензура в Інтернеті існує з метою:

- запобігати доступ осіб до інформації, захищеної авторським правом;
- заборонити людям переглядати шкідливий або конфіденційний контент;
- просувати певні релігії і політичні ідеї;
- контролювати злочинність, пов'язану з Інтернетом, і злочинність, передану через Інтернет;
- відстежувати мільярди людей в Інтернеті з різними думками і уподобаннями.

Міжнародна правозахисна неурядова організація Freedom House щорічно готує доповідь «Свобода в мережі» (*Freedom on the net*), що включає аналітичні звіти та рейтинги стану свободи Інтернет середовища в 65 країнах світу. Згідно з використаною методикою всі країни поділяються на три групи згідно з статусом доступу до мережі Інтернет: free (вільний); partly free (частково вільний); not free (невільний).

Не виникає сумніву, що ступінь свободи доступу до всесвітньої мережі значно впливає на зародження протестних настроїв у віртуальному середовищі.

З огляду на всі перераховані вище фактори, в роботі пропонується наступна формула для обчислення ймовірності виникнення реальної натовпу, шляхом використання Інтернету:

$$x = \frac{IIP \cdot PPI \cdot ER(ERR) \cdot n \cdot booster \cdot HT \cdot rand(0.5,1)}{IC} \times 100\% \quad (9)$$

де IIP – індекс людського розвитку;
 PPI – рівень проникнення до Інтернету;
 ERR або ER – коефіцієнт залучення;

n – кількість учасників поширення публікації;
 booster – наявність в публікації певних атрибутів (фото, відео тощо);
 Hot topic (HT) – гаряча, широко обговорювана тема поста;
 random – випадкове значення з проміжку $[0.5, 1]$;
 Інтернет цензура (ІЦ) – статус доступу для певної країни.

Значення ІР для певної країни в роботі береться з Доповіді про людський розвиток Програми розвитку Організації Об'єднаних Націй за 2020 рік [10].

Пропонуються для обчислення наступні значення n : якщо $n < 5$ (порівняння з 5 береться, виходячи з того, що у роботі під натовпом мається на увазі п'ять і більше осіб), то значення дорівнює 0,1; якщо в діапазоні $5 \leq n < 20$, то значення дорівнює 0,6; якщо в діапазоні $20 \leq n < 80$, то значення дорівнює 0,9 (значення 0,6 й 0,9 отримані експериментально); якщо $n \geq 81$, то значення дорівнює 1. Так як відстежити перші повідомлення, що вже відбулися протестів практично неможливо, то n теж дорівнює 1.

Значення параметру booster залежить від соціальної мережі, де зроблена публікація. У тому випадку, якщо публікація не має популярних в соціальній мережі атрибутів, booster = 0,9, що зменшує кінцеву ймовірність виникнення реальної натовпу. І кількість символів і зміст публікації можна поділити на три критерії: ефективний, менш ефективний, неефективний, які дорівнюють 0,05, 0,03, і 0 відповідно. Формула для обчислення:

$$booster = 0.9 + N + Y, \quad (10)$$

де N – критерій ефективності, пов'язаний з кількістю символів публікації для певної соціальної мережі;

Y – критерій ефективності, пов'язаний зі змістом публікації для певної соціальної мережі (Таблиця 1).

Якщо публікація торкається широко обговорюваної теми, то HT = 0,9, що зменшує ймовірність виникнення реального натовпу, в іншому випадку HT = 1.

Для кожного статусу доступу до мережі Інтернет пропонуються наступні числові значення: free = 1; partly free = 2; not free = 3.

Апробація запропонованої моделі на прикладі протестів руху #BlackLivesMatter у 2020 року. Для прикладу зроблено розрахунки мінімальної та максимальної ймовірності виникнення реального натовпу завдяки Інтернету, на прикладі протестів #BlackLivesMatter 2020 року, після смерті Джорджа Флойда.

Індекс людського розвитку Сполучених Штатів Америки дорівнює 0,926 [10]. Рівень проникнення до Інтернет дорівнює 89,8% [11]. Нажаль, на даний момент відстежити перше повідомлення неможливо. Припустимо, що хоча б половина підписників людини, що опублікувала це повідомлення, відреагували на нього. З цього ER = 0,5. Загальна кількість учасників віртуального натовпу $n = 1$. Широке обговорювання почалося після публікації відео, тому booster = 1. Події відбулися в час передвиборної кампанії та торкалися гострої для США теми – расизму, тому HT = 1. Інтернет цензура у країні має статус «free», тому значення параметра ІЦ = 1. Для розрахунку мінімальної ймовірності random = 0,5, для максимальної random = 1.

Отже, мінімальна ймовірність:

$$x = \frac{0,926 \cdot 0,898 \cdot 0,5 \cdot 1 \cdot 1 \cdot 1 \cdot 0,5}{1} \times 100\% = 20,79\%, \quad (11)$$

а максимальна ймовірність:

$$x = \frac{0,926 \cdot 0,898 \cdot 0,5 \cdot 1 \cdot 1 \cdot 1}{1} \times 100\% = 41,58\% \quad (12)$$

Невеликий відсоток обумовлений тим, що це ймовірність виникнення лише перших натовпів.

Після того, як віртуальний натовп став реальним, його подальший розвиток буде залежати від інших факторів, Інтернет не завжди буде тому сприятиме. Також слід урахувати, що у роботі не враховуються фактори обходу Інтернет-цензури: VPN, DarkNet та ін.

Висновки

Сучасні протестні рухи часто зароджуються в мережі Інтернет і тільки після досягнення певного рівня розвитку переходять у фазу реальних актів громадянської непокорі.

Побудована в роботі модель дає змогу отримати науково обґрунтовані варіанти розвитку й ймовірність змін, які віртуальний натовп зазнає в часі, аж до свого переродження у реальний рух.

Таким чином, мета, яка була поставлена і досягнута в даній роботі, а саме оцінка ймовірності переходу натовпу з віртуального стану в реальний, є важливою і актуальною як з точки зору безпеки окремого громадянина і суспільства, так і з точки зору безпеки держави в цілому. Крім того, досягнення, поставленої мети, дасть змогу розробити рекомендації фахівцям, які допомагають забезпечувати високий рівень безпеки в звичайних і екстремальних ситуаціях, оптимізувати різні будівлі і споруди з точки зору ефективності проходження людського потоку, а також ефективно управляти транспортним потоком.

Список літератури

1. Приходько І.І., Тімченко О.В., Полторак С.Т. Психологія натовпу й управління ним при виконанні службово-бойових завдань. Х.: НА НГУ, 2015. 250 с.
2. Левчук Н.Н. Феномен виртуальной толпы в процессе достижения информационного доминирования. Веснік БДУ. Сер. 4. 2010. № 1. С. 65-68.
3. Забарин А.В. Психология толпы и массовых беспорядков. М.: Юрайт, 2017. 19 с.
4. UNDP. Statistical Update: Human Development Indices and Indicators 2018. URL: <http://hdr.undp.org/en/content/human-development-indices-indicators-2018>
5. UNDP. 2014 Human Development Report Technical Notes. URL: <http://hdr.undp.org/sites/default/files/hdr14-report-en-1.pdf>.
6. Что такое охват в социальных сетях - полное руководство. URL: <https://popsters.ru/blog/post/83>.
7. Engagement rate: как правильно считать коэффициент вовлеченности в социальных сетях. URL: <https://popsters.ru/blog/post/55>.
8. Бергер Й. Заразительный. Психология сарафанного радио. Как продукты и идеи становятся популярными. М.: АСТ, 2014. 227 с.

9. Кальин А., Кушнир А. Активность аудитории в социальных сетях: Исследование активности в 2020 году. URL: <https://popsters.ru/blog/post/aktivnost-auditorii-v-socialnyh-setyah--issledovanie-aktivnosti-v-2020-godu>.
10. UNDP. Statistical Update: Human Development Indices and Indicators. 2020. URL: <http://report.hdr.undp.org/>.
11. Internet World Stats. URL: <https://www.internetworldstats.com/stats.htm>.

DEVELOPMENT OF A MATHEMATICAL MODEL OF VIRTUAL CROWD BEHAVIOR

O.M. Simonova, I.I. Bobok

National University «Odessa Polytechnic»
Shevchenko Ave., 1, Odessa, 65044, Ukraine; e-mail: onu_metal@ukr.net

Crowd forecasting is a relatively new task in predicting the future. Today, the crowd studied by classical social psychology has undergone significant changes, which has led to the emergence of such a concept as "Internet crowd". Internet crowd technology is now used to create "dead souls", i.e. fake accounts, using fake names and addresses to form, disseminate opinions and/or impose opinions on real users. The aim of the work is to develop a mathematical model of a virtual crowd to predict its behavior and calculate the probability of transition of a virtual crowd to a real one. The paper highlights the most important factors influencing the emergence of protest movements through the formation of a virtual crowd. It is shown that a person living in a country with a high level of economic development, it is easier to decide to participate in the protest because of confidence in the further stable development of the state. The importance of Internet censorship in the modern world and the possibility of the influence of this factor on the formation of primary groups of protesters in a virtual environment are demonstrated. The methods of mathematical modeling used in the work make it possible to obtain scientifically substantiated variants of development and the probability of changes that the virtual crowd undergoes in time, until its rebirth into real motion. Thus, the assessment of the probability of the transition of the crowd from the virtual to the real state, is important and relevant both in terms of security of the individual citizen and society, and in terms of security of the state as a whole. The proposed model will allow to develop recommendations for specialists who help to ensure a high level of safety in ordinary and extreme situations, to optimize urban development in terms of efficiency of human traffic flow, as well as to effectively manage traffic flow.

Keywords: virtual crowd, probability, protest movement, mathematical model.

МОДЕЛЮВАННЯ РОБОТИ СИСТЕМИ АВТОМАТИЗОВАНОГО КЕРУВАННЯ ПРОЦЕСОМ УВАРЮВАННЯ ЦУКРОВИХ УТФЕЛІВ У ВАКУУМ-АПАРАТІ ПЕРІОДИЧНОЇ ДІЇ У СЕРЕДОВИЩІ ПРОГРАМОВАНОГО КОНТРОЛЕРА**Ю.М. Скаковський**Одеська національна академія харчових технологій
65039, Одеса, вул. Канатна, 112, yurysk@ukr.net

Приведені результати дослідження, яке виконувалось в Одеській національній академії харчових технологій в межах госпдоговірної тематики. Розглянуті результати імітаційного моделювання роботи системи автоматизованого керування процесом уварювання цукрових утфелів у вакуум-апараті періодичної дії. Обґрунтована доцільність проведення моделювання у середовищі програмування мікропроцесорного контролера, на базі котрого створюється автоматизоване робоче місце оператора-варщика. Лабораторні дослідження проведені на спеціалізованому стенді із застосуванням узгоджених із замовником промислових мікропроцесорних контролерів та програмних засобів українського виробництва, в тому числі SCADA-системи «ІНДЕЛ». Розроблена спрощена модель процесу уварювання як об'єкта керування за двома основними каналами. Програми, що реалізують алгоритми керування уварюванням цукрового утфелю у апараті, та програма, що реалізує спрощену модель процесу, складена FBD подібною мовою програмування контролера МІК52 українського виробництва. Для зв'язку програмованого контролера та комп'ютера використаний перетворювач інтерфейсів БПІ-52 (MODBUS RTU to USB) також українського виробництва. Аналіз результатів моделювання системи керування, що отримано у виді параметричних діаграм та часових графіків за допомогою SCADA-системи «ІНДЕЛ», дозволив зробити висновки про працездатність розроблених алгоритмів керування і програм, що їх реалізують. На основі отриманих позитивних результатів дослідження було створено промисловий варіант автоматизованого робочого місця оператора апарату. Окрім контролерів в щиті оператора і промислового комп'ютера, розроблено пульт дистанційного керування. Розроблену систему було впроваджено у складі модернізованої АСКТП продуктового відділення на діючому цукровому заводі. Виробничі випробування та експлуатація підтвердили працездатність системи керування процесом уварювання утфелів, яка була розроблена за результатами відповідних лабораторних досліджень. На основі отриманих результатів були визначені напрямки подальших досліджень, як у частині розвитку алгоритмів керування, так і в розвитку функцій САК.

Ключові слова: моделювання, система автоматизованого керування, автоматизоване робоче місце оператора, мікропроцесорний контролер, програма керування, вакуум-апарат періодичної дії, цукровий утфель, продуктове відділення, цукровий завод.

Вступ

Зараз роботи з моделювання різноманітних технологічних і бізнес- процесів дослідники, як правило, проводять у спеціалізованих програмних середовищах. Для імітаційного моделювання динаміки складних технологічних процесів найбільшу популярність отримали такі пакети програм як MATLAB (Simulink), LABVIEW, і ін., які дозволяють, за відсутністю можливості проведення експериментів у виробничих умовах з використанням спеціалізованих керуючих контролерів і інших технічних засобів, отримувати адекватні результати досліджень. Для впровадження у виробництво отриманих програмних результатів з реалізації алгоритмів керування

проводять конвертацію програмного забезпечення (ПЗ) в середовище програмованих керуючих пристроїв (контролерів).

Під час проведення робіт в Одеській національній академії харчових технологій з госпдоговірної тематики для підвищення ефективності функціонування систем автоматизації продуктового відділення Красилівського цукрового заводу Хмельницької області, яке модернізується, виконувались дослідження з розробки системи автоматизованого керування (САК) процесом уварювання цукрових утфелів у вакуум-апараті (ВА) періодичної дії. Технологічна програма, за котрою виконується керування процесом, тип керуючого контролера та SCADA-системи були узгоджені з замовником.

У зв'язку з наявністю спеціалізованого стенду, оснащеного програмованими контролерами та комп'ютером із SCADA-системою «ІНДЕЛ» (розробник ПП «Інфотехпром», м. Полтава) для створення АРМ оператора-варщика, було прийняте рішення проводити імітаційне моделювання у середовищі обраного контролера МІК52 (МПК) українського виробництва з використанням можливостей обраної SCADA-системи. Вибір технічних і програмних засобів ґрунтувався на досвіді останніх впроваджених на заводі розробок, враховуючи досвід робітників служби КВП і А з роботи і обслуговування мікропроцесорних контролерів та регуляторів фірми «МІКРОЛ» (м. Івано-Франківськ), а також SCADA-системи «ІНДЕЛ», яка використана в більшості АРМ операторів на інших ділянках заводу [1].

Імітаційне моделювання в середовищі програмованого контролера, на якому і буде реалізована промислова система керування, дозволяє уникнути етапу конвертації ПЗ, можливих помилок в цьому процесі та знижує обсяги робіт з налагодження САК в промислових умовах.

Аналіз досліджень і публікацій

Уварювання цукрових утфелів першого продукту здійснюється в модернізованому ВА, для інтенсифікації процесів кристалізації в котрому реалізована примусова циркуляція. Процес отримання утфелю першого продукту (кристалізації) традиційно розділяють на наступні етапи (стадії): набір (наповнення) ВА сиропом (вище рівня розташування грючої камери), згущення його до певного стану, коли потрібно заводити у ВА цукрову пудру для створення центрів кристалізації; нарощування кристалів, згущення утфелю, вивантаження звареної маси в мішалку та пропарювання ВА [2]. Традиційний метод проведення всіх етапів отримання утфелю є робота з періодичним введенням у ВА сиропу (вихідного розчину) – так звані «підкачки». Таке технічне рішення пов'язано з високою щільністю вихідних розчинів, що утруднює використання неперервно діючих виконавчих пристроїв (ВП).

Як вихідний розчин використовується сироп із клеровкою (розчин цукру нетоварної якості) та відтоки утфелю першого продукту, який центрифугується (створюється біла та зелена патоки). Як агент, що гріє, використовується, згідно із тепловою схемою заводу, вторинна пара другого корпусу випарної станції (ВС), яка характеризується відносно низьким потенціалом (0,06 – 0,07 МПа), а також частково пара наступного корпусу ВС. Уварювання утфелю здійснюють під розрідженням, за допомогою керування регулюючим органом (РО) на вакуумпроводі до ВА, призначеним для керування температури в просторі ВА.

Принципова схема САК ВА періодичної дії (з циркулятором) зображена на рис.1

На рис.1 приведено корпус ВА, оснащений (ВП) для керування процесом уварювання утфелю та датчиками для отримання поточної інформації про протікання процесу.

Система містить ВП1, який подає грючу пару у ВА, ВП2 для здійснення пропарки ВА між циклами уварювання, ВП3 (основний) зв'язку внутрішнього простору ВА із магістраллю розрідження, ВП4 (допоміжний) для подібного ж зв'язку, ВП5

(основний) для вивантаження готового утфелю у приймальну мішалку, ВП6 (допоміжний) для полегшення роботи ВП5, ВП7 для подачі вихідного розчину у ВА, ВП8 для зв'язку внутрішнього простору ВА із атмосферою, а також датчики рівня 9, температури в ВА10 та консистенції утфелю 11.

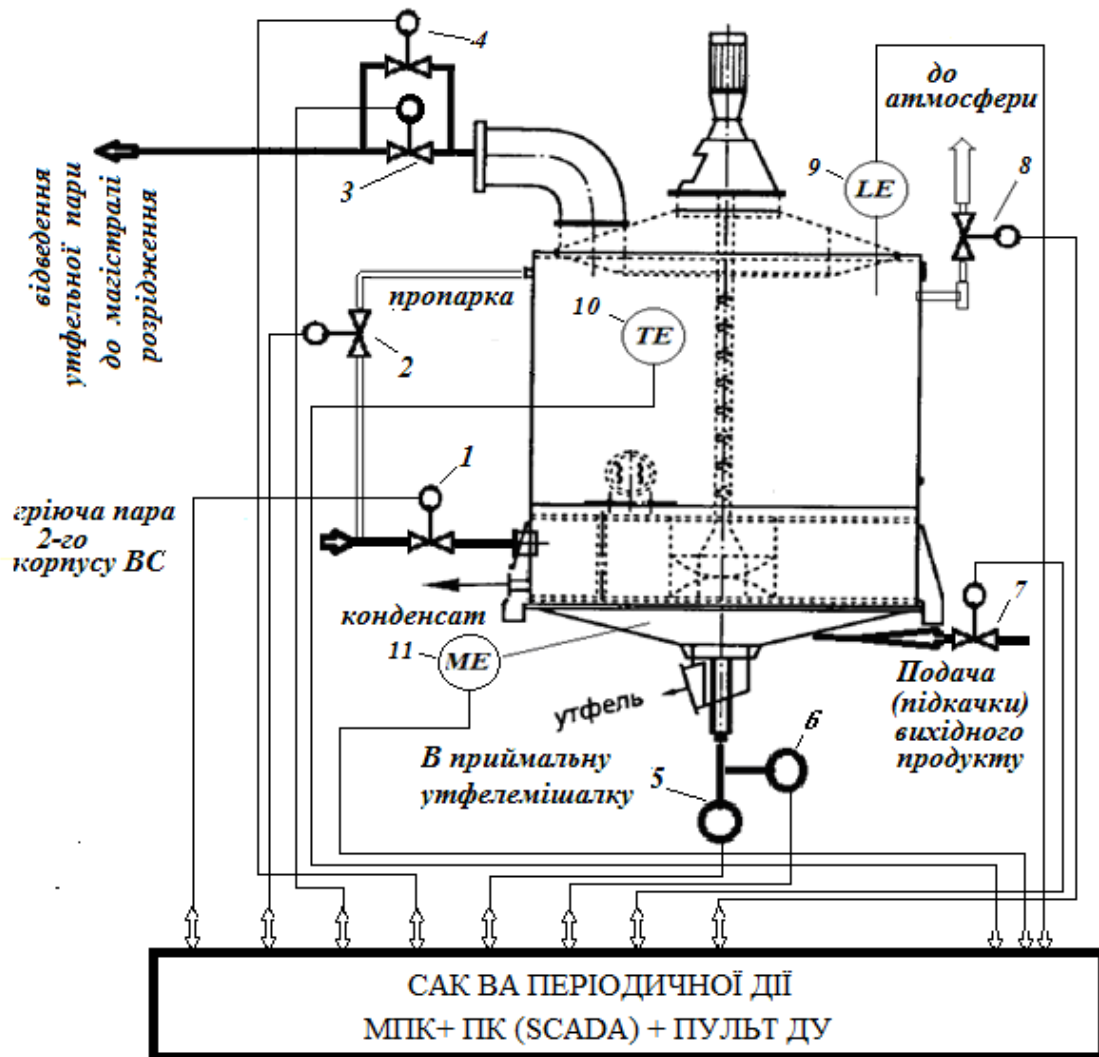


Рис 1. Принципова схема САК ВА

САК ВА включає програмований контролер, комп'ютер зі SCADA-системою та пульт дистанційного керування для реалізації оператором деяких допоміжних операцій.

Мета роботи

Метою роботи є проведення імітаційного моделювання роботи САК процесом уварювання утфелів у ВА для створення, за позитивними результатами, АРМ оператора на базі сучасного програмованого контролера українського виробництва.

Узгоджений із замовником перелік завдань для САК виключав автоматизацію допоміжних операцій (Пуск – Зупинка – Вивантаження), оскільки ці операції оператор виконує в дистанційному режимі з розробленого пульта ВА. Таким чином, створюється не автоматична, а автоматизована система керування.

У перелік завдань дослідження входить: розробка алгоритму і програми уварювання утфелю з використанням мови програмування мікропроцесорного

контролера МІК52 та дослідження роботи САК в лабораторних умовах і, за отриманням успішного результату, створення промислового АРМ оператора на базі зазначеного контролера з використанням SCADA-системи «ІНДЕЛ» українського виробництва, що дозволить у подальшому включити цей АРМ у склад АСКТП і підключення її до існуючої заводської інформаційної мережі.

Імітаційне моделювання проводилося на лабораторному стенді, який містить: промислові контролери (МІК52, МІК112), імітатори аналогових та дискретних сигналів, блок перетворення інтерфейсів (БПІ-52), комп'ютер із встановленим програмним забезпеченням, в тому числі, драйвером для БПІ-52, SCADA-системою «ІНДЕЛ» з драйвером MODBUS RTU, що забезпечує зв'язок із мережею контролерів за допомогою двохпроводного інтерфейсу RS-485.

Вибір налаштувань інтерфейсів виконувався з урахуванням відомої інженерної методики, яка базується на наслідку із теореми Котельникова, що забезпечує оптимальний період опитування даних із виключенням втрати інформації.

Основний розділ

На першому етапі дослідження була складена структурна схема САК уварювання утфелів у ВА, що включає об'єкт керування (ОК) та керуючий пристрій. САК можна представити у вигляді схеми, яка приведена на рис. 2.

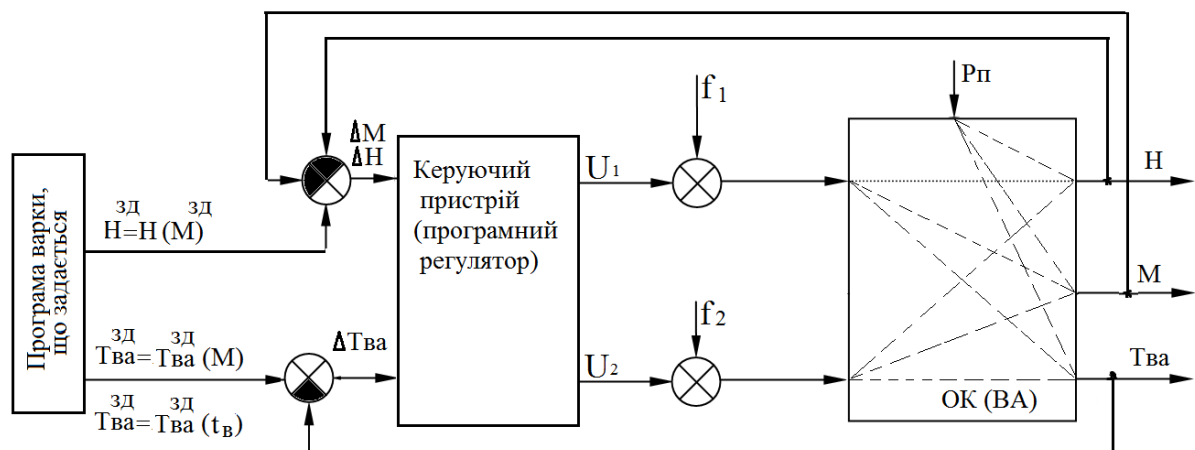


Рис. 2. Структурна схема САК уварювання утфелю у ВА

Позначення на схемі:

H – рівень продукту у ВА, %;

M – структурна в'язкість продукту у ВА (за ротаційним датчиком), %;

$T_{ва}$ – температура в просторі ВА, °C;

P_p – тиск пари, що гріє, МПа;

U_1 – положення регулюючого органу, що керує подачею вихідного розчину у ВА, %;

U_2 – положення регулюючого органу, що керує зв'язком простору ВА з магістраллю розрідження, %;

t_v – час в циклі уварювання;

f_1, f_2 – вектори неконтрольованих збурень.

ВА періодичної дії як об'єкт керування має ряд особливостей. У ньому присутні перехресні зв'язки змінних та велика кількість впливів, які збурюють, і автоматичний контроль значної кількості яких є дуже утрудненим, оскільки пов'язаний із якісним

складом вихідних розчинів та продукту у ВА, що уварюється. Суттєвий вплив на вихідні змінні оказує тиск гріючої пари, який йде як вторинна із другого корпусу ВС [2]. Крім того, відомо, що в циклі варки ВА витрати пари, котра гріє, є нерівномірними і залежними від стадії варки та конструктивних особливостей ВА. В [3] приведені подібні залежності, які були отримані експериментально для конкретної модифікації ВА продуктового відділення цукрорафінадного заводу, але розповсюджувати їх для всіх аналогічних конструкцій ВА бурякоцукрового виробництва є недоцільним без дослідження індивідуальних характеристик ВА та процесів варки в них утфелю. У тому ж джерелі приведена рекомендація щодо зменшення коливань тиску гріючої пари для групи ВА періодичної дії, яка базується на оптимальному керуванні моментом запуску в роботу кожного окремого апарата в групі. Проведення аналогічних експериментальних досліджень для кожного ВА є достатньо витратними та технічно складними.

Відомі також дослідження з пошуку оптимальних змін в часі $T^{зд} = T^{зд}(t)$ заданої температури в просторі ВА в процесі уварювання утфелю у ВА та додавання до складу пари, що гріє, парів четвертого корпусу ВА, з метою скорочення загального часу циклу уварювання утфелю та енергозбереження. В той же час, на ці залежності також суттєво впливають індивідуальні особливості конструкції ВА та складу вихідних продуктів, тому оцінювання параметрів цих залежностей доцільно проводити експериментально під час роботи САК, яка здійснює автоматичну варку. При цьому доцільним є пошук оптимальної, за критерієм мінімального часу циклу уварювання зі збереженням потрібної кристалоструктури, залежності $T_{ва}^{зд} = T_{ва}^{зд}(M)$.

З урахуванням вище зазначеного, було прийняте рішення в даному дослідженні зосередитись на розробці саме програми керування уварюванням утфелю у ВА, реалізації цієї програми в середовище програмування контролера МІК52 та промислового комп'ютера із SCADA-системою «ІНДЕЛ» для створення АРМ оператора-варщика. Провести лабораторні та промислові дослідження працездатності розробленої системи автоматичного уварювання утфелю.

Дослідження згаданих вище залежностей між змінними процесу варки у ВА доцільно проводити на діючому ВА, котрий керується автоматично у складі АРМ оператора-варщика.

Технологічна програма уварювання утфелю у ВА була запропонована за результатами передпроектних досліджень й узгоджена із замовником у вигляді залежності $H=H(M)$, методика отримання якої традиційно використовується в САК уварювання утфелів. Побудова такої програми аналітичними методами, оптимальної з точки зору якості отриманих кристалів цукру та мінімального часу циклу уварювання, стикається із проблемою багатофакторності збуджуючих впливів, автоматичний контроль значної кількості яких є дуже утрудненим. Тому традиційно використовуються експериментальні експертні методи. Програма варки для нового ВА була розроблена у вигляді допоміжної форми для налаштування, в складі АРМ оператора-варщика (рис. 3).

Режим керування подачею вихідного розчину у ВА є двопозиційним: за відкриттям (100%) регулюючого органу (РО) – порція вихідного розчину подається у ВА, за закриттям РО (0%) – провадиться згущення розчину в ВА внаслідок випаровування вологи з нього. При цьому, пара подається в гріючу камеру за повністю відкритою паровою засувкою впродовж всього циклу уварювання. Використання інших режимів керування нею недоцільно, внаслідок відносно невеликого тиску зазначеної пари, що гріє, із ВС.

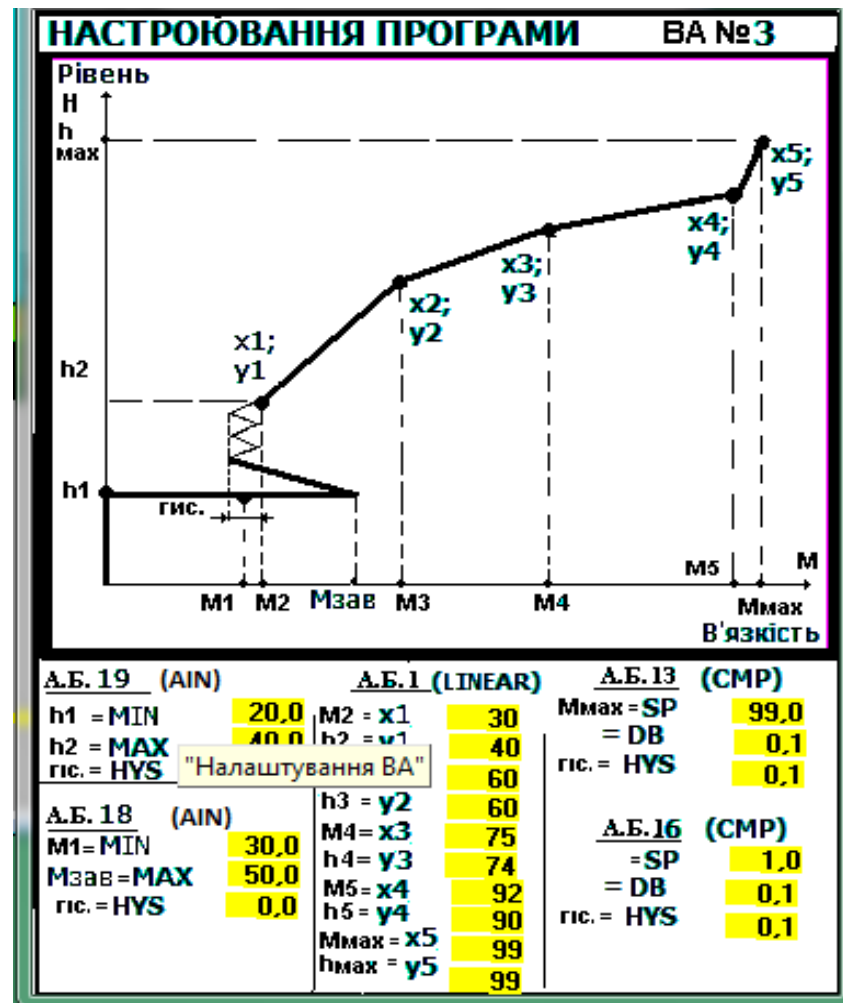


Рис. 3. Допоміжна екранна форма для налаштування програми уварювання утфелю

Серед органів дистанційного керування, які розміщено на пульті ВА, слід виділити насамперед тумблери Т1 (Набір) та Т2 (Підкачка), а також тумблери, які формують склад вихідного розчину, що подається через гребінку (колектор вихідних розчинів) та РО (U_1) у ВА.

Дії оператора під час керування циклом варки полягають у наступному. Після пропарювання апарата й виконання допоміжних операцій із включення ВА у роботу в дистанційному режимі, оператор включає тумблер Т1. Після цього, програма автоматичної варки здійснює керування ВП7 (U_1). На етапі НАБІР апарат наповнюється вихідним розчином до рівня h1, після чого здійснюється згущення продукту у ВА, зі стабілізацією рівня h1, шляхом підкачки порцій свіжого розчину. Консистенція продукту зростає після закриття РО (внаслідок випаровування вологи) і зменшується під час відкриття РО. Протилежні зміни, вочевидь, здійснюються відносно рівня продукту у ВА. За досягненням консистенції продукту $M = M_{зав}$, оператор отримує звуковий, світловий сигнали, а також повідомлення на екрані комп'ютера про необхідність перевірки стану готовності ВА до «заведення» пудри (центрів кристалізації). Оператор вимикає Т1 і вводить в ВА цукрову пудру. Після перевірки стану продукту, в тому числі з використанням органолептичних методів, вмикає тумблер Т2 (підкачка). Програма керує ВП 7 і забезпечує реалізацію процесу так званої першої глибокої підкачки, що призводить до збільшення рівня у ВА та зменшення консистенції до точки M2, після чого реалізується режим стабілізації консистенції зі

зростанням рівня у ВА до значення h_2 . На цьому етапі починають формуватися кристали цукру навколо дрібнодисперсних кристалічних центрів, тобто окремих часток попередньо «заведеної» цукрової пудри. Далі починається стадія «зростання кристалу», відображення котрої наведено на рис. 3 від точки з координатами (x_1, y_1) до точки (x_5, y_5) , програма реалізує керування процесом із використання кусочно-лінійної функції. Після досягнення точки (x_5, y_5) , що відповідає готовності апарату, тобто стан апарату відповідає повному робочому рівню готового продукту (утфелю) у ВА, оператор отримує звуковий та світловий сигнали, а також повідомлення про закінчення варки на екрані АРМ. Оператор перевіряє стан продукту у ВА, і, за підтвердженням готовності, здійснює вивантаження утфелю в мішалку, виконує необхідні допоміжні операції та пропарює апарат для початку наступного циклу уварювання [4].

Кожна з наведених на екранній опорних точок (див. рис. 3), може бути уточнена в процесі налаштування відповідної програми, шляхом введення скоригованих значень.

Моделювання поведінки ОК під керуванням САК здійснювалось в контролері, де сумісно функціонувала програма керування з програмою реалізації моделі ОК. Обидві програми складені FBD подібною мовою «а», яка призначена для програмування контролерів фірми «МІКРОЛ».

Спрощена модель ОК за каналами $U_1 \rightarrow H$; $U_1 \rightarrow M$ (див. рис.2) розглядалася як два інтегруючих ланцюжки із різними знаками та коефіцієнтами, що посилюють. Така структура моделі відповідає процесам періодичного додавання порції вихідного розчину та випарювання вологи з розчину у ВА. Оцінювання відповідних коефіцієнтів виконувалось за результатами обробки експериментальних даних, отриманих на працюючих ВА з попередніми версіями САК.

Аналіз результатів моделювання роботи САК з використанням наведеної моделі ОК зручно проводити за допомогою засобів налагодженої SCADA-системі «ІНДЕЛ».

На рис. 4 наведена діаграма у координатах «структурна в'язкість продукту у ВА, %» – «рівень продукту у ВА, %», яка відображає стадії: набору рівня у ВА (1), згущення розчину (2), «заведення» цукрової пудри (3), першої глибокої підкачки (4), формування (5) та початку зростання кристалу (6).

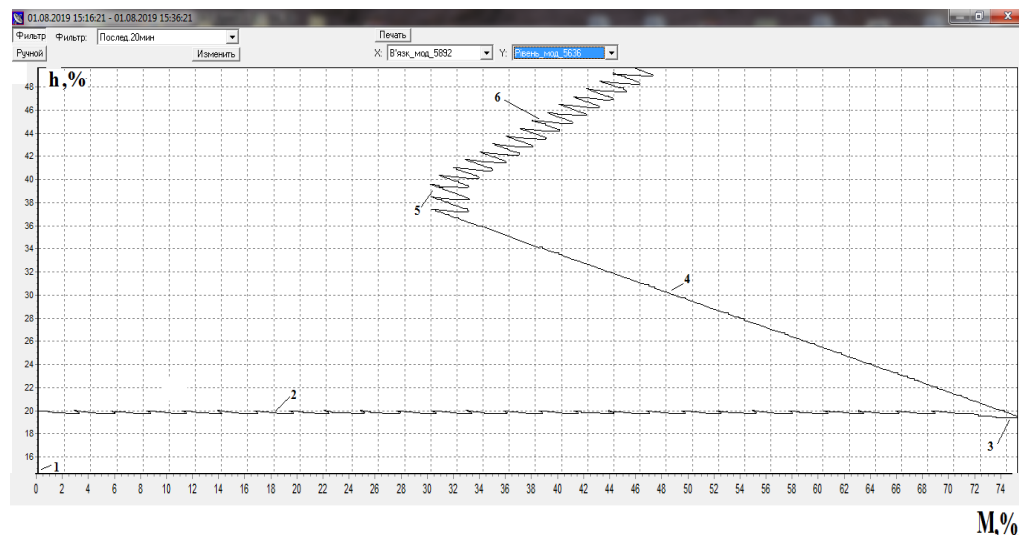


Рис. 4. Діаграма процесу уварювання продукту у ВА на початкових стадіях

На рис. 5 приведена програма імітаційного моделювання, яка включає фрагмент програми керування процесом уварювання утфелю у ВА (зверху) та програму моделі, яка імітує ОК за приведеними каналами (знизу).

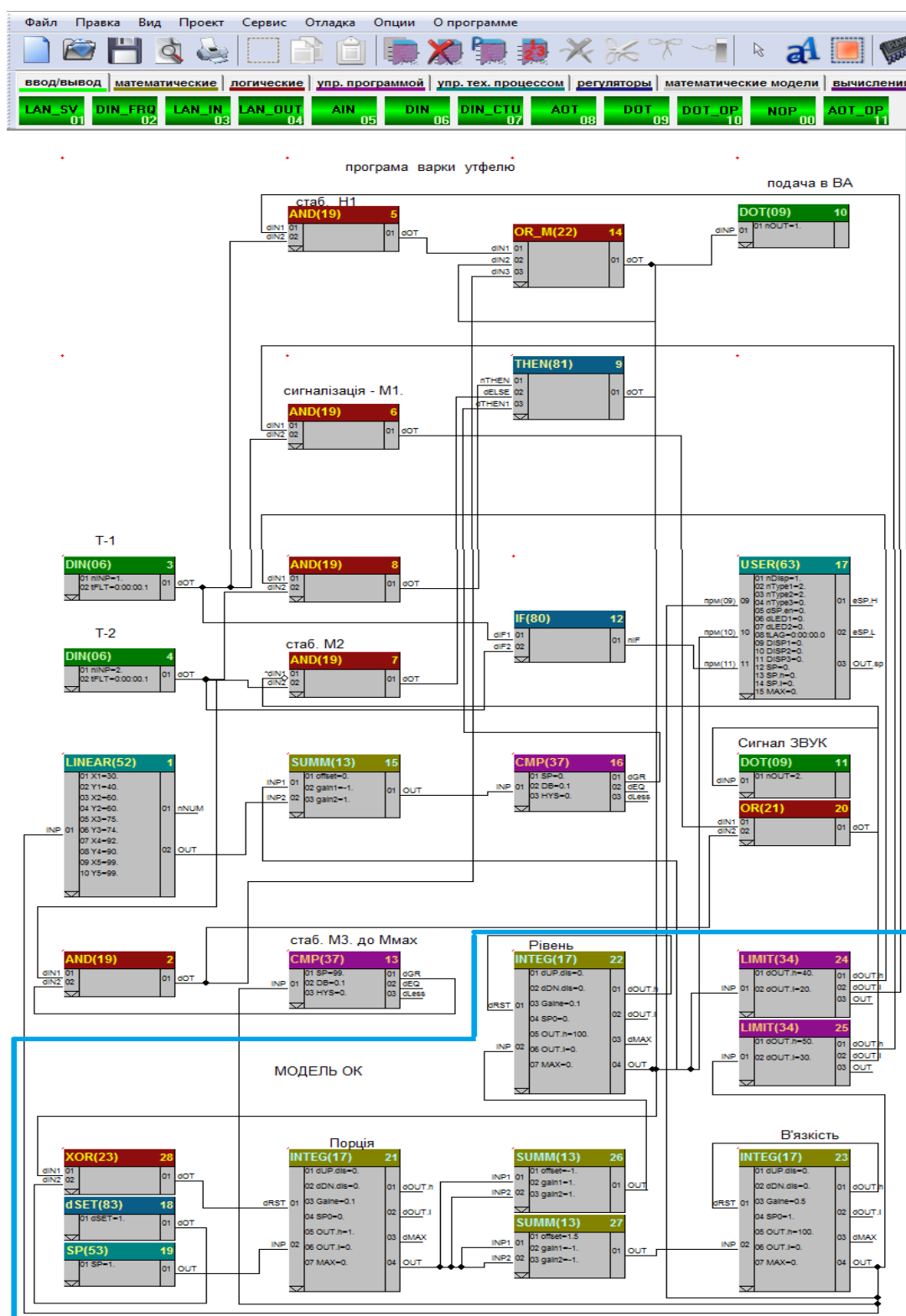


Рис. 5. Програма для імітаційного моделювання поведінки САК процесу уварювання утюг у ВА

Вид основної екранної форми для АРМ оператора за моделюванням проведення початкових стадій набору продукту у ВА та згущення наведено на рис. 6, а відповідно, за моментом «заведення» кристалу на рис.7.

Масштаб часу в моделі ОК та реальному ОК має співвідношення 1:3.

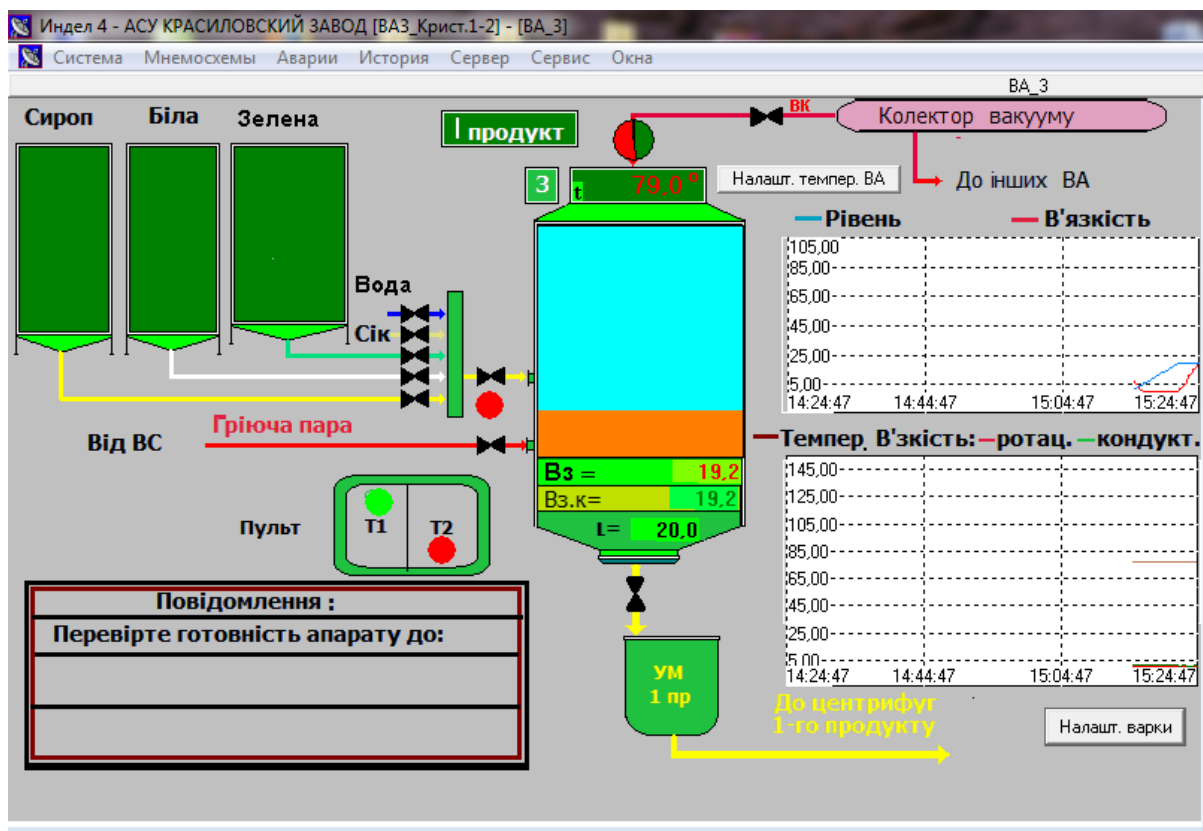


Рис. 6. Основна екранна форма АРМ оператора-варщика на початкових стадіях уварювання: набору продукту у ВА та згущення.

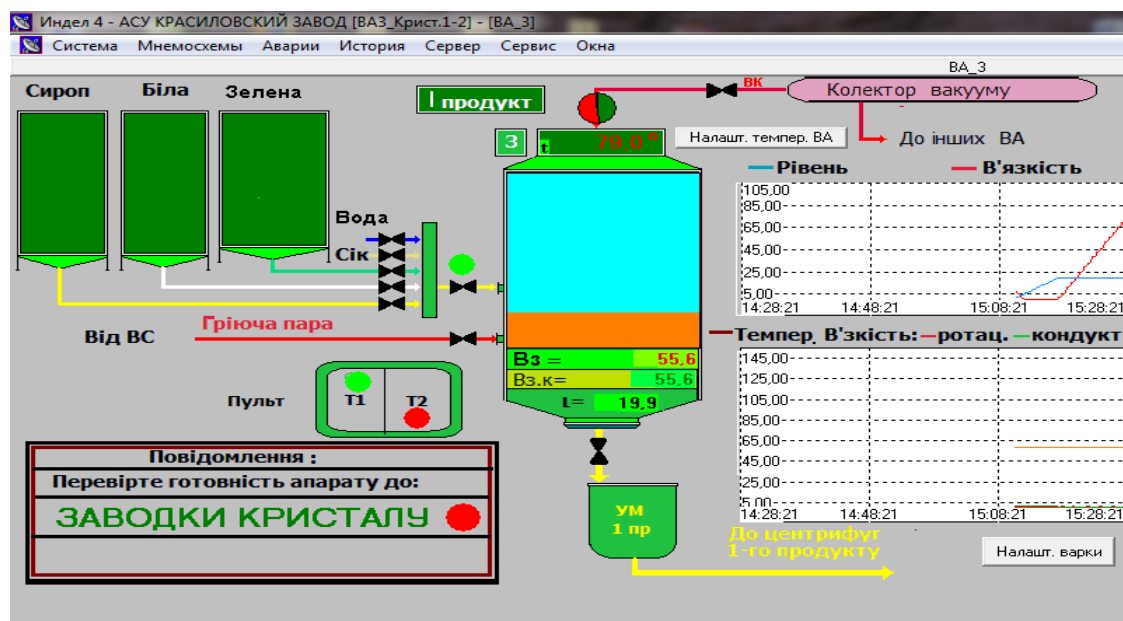


Рис. 7. Основна екранна форма АРМ оператора-варщика на стадії «заведення» кристалу.

Звернемо увагу, що на обох наведених стадіях: початкового згущення продукту та заведення кристалу рівень у ВА, згідно до програми уварювання, однаковий, а структурна в'язкість продукту у ВА збільшилась від 19,2% до 55,6%.

Діаграма, що отримана за моделюванням кінцевих стадій уварювання: закінчення зростання кристалу у ВА (1) та закінчення уварювання (2) наведено на рис. 8, відповідна екранна форма АРМ оператора на кінцевій стадії уварювання на рис. 9.

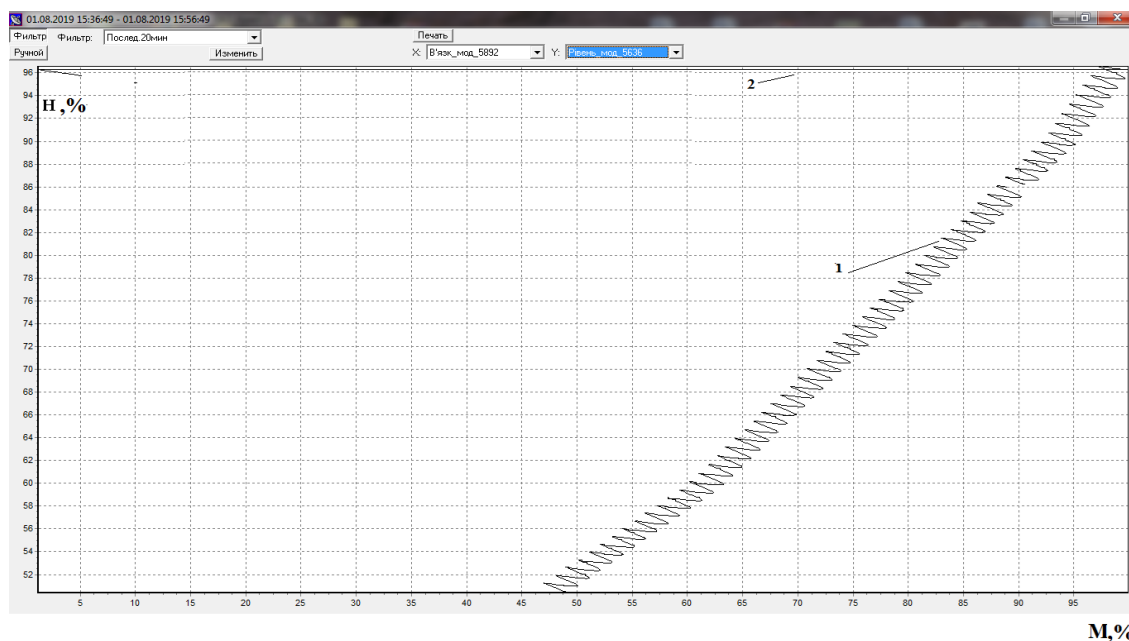


Рис. 8. Діаграма процесу уварювання продукту у ВА на кінцевих стадіях.

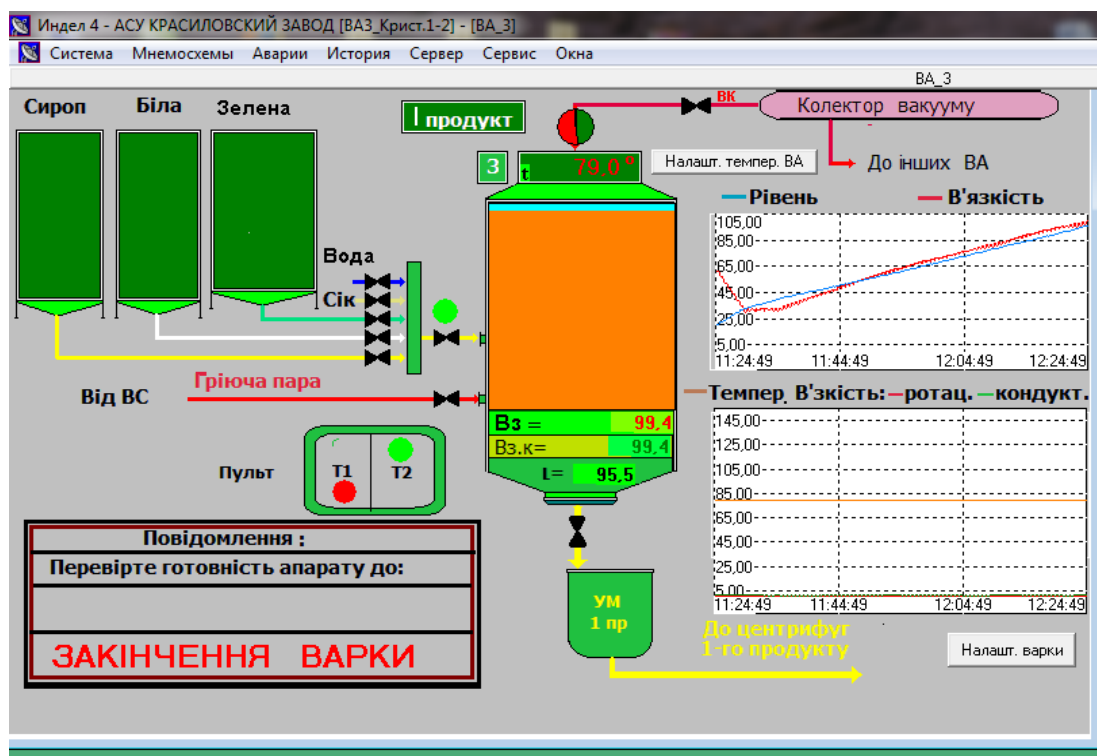


Рис. 9. Екранна форма АРМ оператора на кінцевих стадіях уварювання продукту у ВА.

Аналіз отриманих результатів моделювання роботи САК за повний цикл уварювання проводився також засобами SCADA-системи «ІНДЕЛ» з використанням часового графіка змінних: 1 – «структурна в'язкість продукту у ВА, %», 2 – «рівень продукту у ВА, %», що наведений на рис. 8.

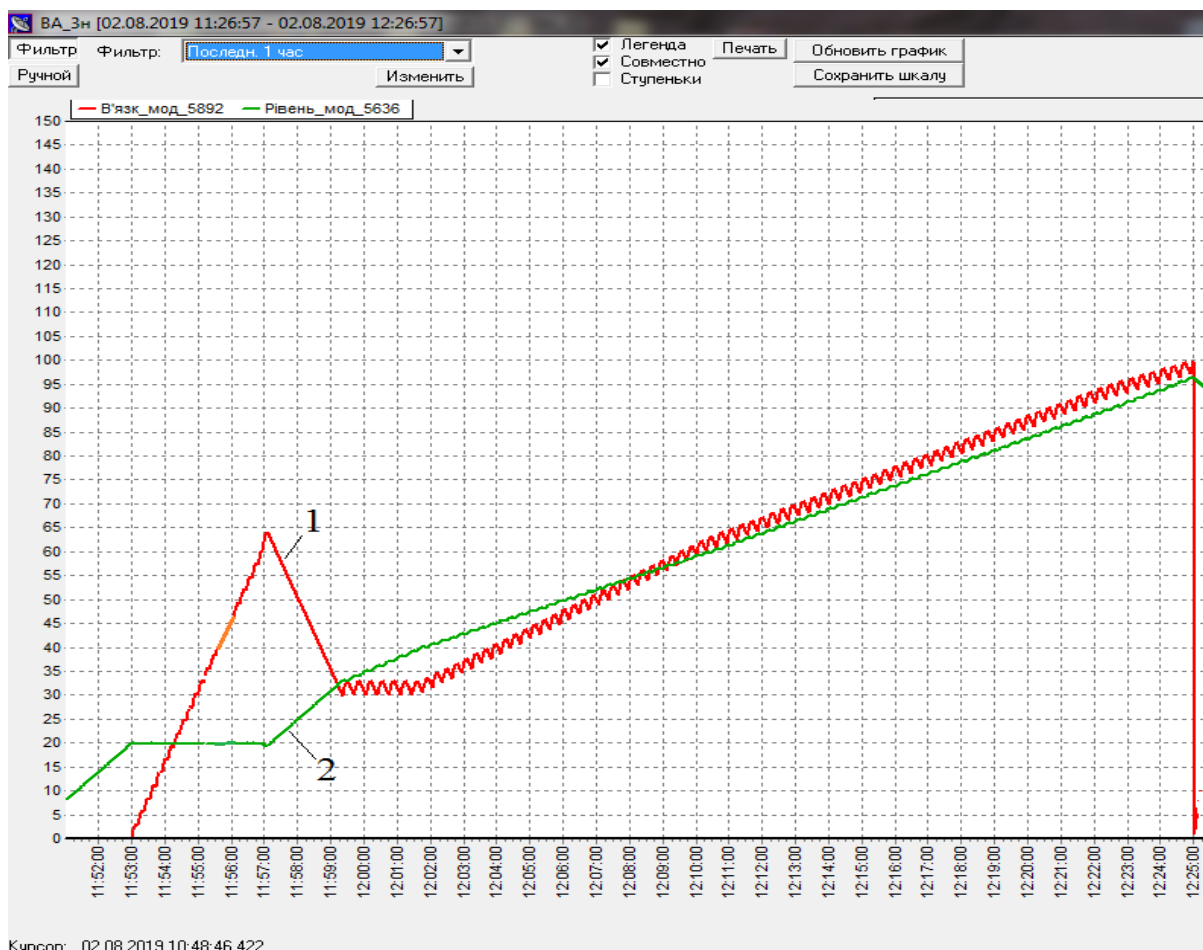


Рис. 10. Часовий графік за результатами моделювання процесу керування уварюванням продукту у ВА, отриманий за повний цикл.

Результат та обговорення

Проведений аналіз отриманих результатів моделювання роботи САК уварюванням утфелю у ВА періодичної дії показав працездатність системи керування. Модель ОК за обраними для дослідження каналами: $U_1 \rightarrow H$; $U_1 \rightarrow M$ є достатньо адекватною і вірно відображає процеси накопичення та випарювання продукту у ВА, що підтверджено наведеними діаграмами та часовим графіком. Потрібно зауважити, що ступінь точності складених моделей не має вирішального значення для оцінювання працездатності САК.

Визначено доцільним проведення імітаційного моделювання процесів керування уварюванням утфелю у ВА періодичної дії у середовищі програмування мікропроцесорного контролера, котрий в наступному використаний у промисловому АРМ оператора.

Отримані результати дослідження дозволили сформулювати рекомендації щодо доцільності використання розробленої програми варки утфелю в промисловій реалізації

АРМ оператора-варщика на базі обраних технічних і програмних засобів, а також щодо розвитку інтелектуальних функцій САК [5].

Реалізація промислової САК була виконана у складі модернізованої системи керування продуктового відділення Красилівського цукрового заводу, де були проведені її виробничі випробування.

У системі керування, що впроваджена, був використаний промисловий комп'ютер ARK-3403-D6A1E/BTO2 із встановленою операційною системою XP E (MS Windows Embedded). Застосування промислового комп'ютера було обумовлено складними умовами повітряного середовища операторського пункту (ОП) продуктового відділення, а саме високою температурою та підвищеною вологістю. Для зменшення цих шкідливих факторів як для оператора, так і для технічних засобів в ОП використана примусова вентиляція.

Виробничі випробування показали працездатність розробленої САК. При цьому, проведені варки із використанням розробленої програми керування дозволили отримати утфель з потрібною якістю кристалів та задовільною тривалістю загального циклу його уварювання.

Висновки

Передпроектні дослідження, що проведені з використанням методів імітаційного моделювання на спеціалізованому стенді, котрий було обладнано промисловим устаткуванням: контролерами та регуляторами, комп'ютером із SCADA-системою «ІНДЕЛ», українського виробництва, дозволили розробити комплекс технічних рішень, що забезпечив успішну експлуатацію АРМ оператора-варщика в складі існуючої автоматизованої системи керування продуктового відділення цукрового заводу.

Промислові випробування та наступна експлуатація підтвердили працездатність розробленої САК, а також дозволили визначити подальші напрямки досліджень. Основна складова ефективності системи керування полягає в зменшенні питомих витрат енергоносіїв за збереженням якості отриманого готового продукту.

Використані у складі АРМ оператора-варщика технічні і програмні засоби українського виробництва забезпечують точність підтримання регламентів ведення процесу, досить комфортні умови праці, як оперативному персоналу, так і технічним керівникам підприємства для аналізу технологічних процесів.

Комплекс досліджень, що був виконаний, дозволяє зробити висновок про доцільність продовження робіт із модернізації систем керування підприємства, використовуючи принцип проектування АСКТП «знизу вгору», а також приведені методи й підходи до прийняття основних технічних рішень.

Список літератури

1. Жуковський Е.Й., Скаковський Ю.М., Вітвицький В.Д., Бабков А.В. Багаторівнева АСУТП цукрового заводу. *АВТОМАТИКА-2011: Матеріали 18 міжнар. конф. з автоматичного управління*. Львів, 2011. С.256-257.
2. Штангеев В.О., Кобер В.Т., Белостоцкий Л.Г., Штангеева Н.И. Современные технологии и оборудование свеклосахарного производства. Часть 2. Киев: Цукор України, 2004. 320 с.
3. Скаковский Ю.М. Автоматизированная система управления технологическими потоками и производительностью сахарного завода /

- Диссертация на соискание ученой степени кандидата технических наук: 05.13.07. Одесса, 1987. 319 с.
4. Скаковський Ю.М., Бабков А.В., Мандро О.Ю. Модернізація системи автоматизованого керування вакуум-апаратом періодичної дії цукрового виробництва на базі технічних і програмних засобів українського виробництва. *Автоматизація технологічних і бізнес-процесів*. 2019. №11(3), С. 4-14.
 5. Скаковський Ю.М. Автоматизація оперативного обліку цукрового утфелю в модернізованій системі керування для продуктового відділення цукрового заводу. *Автоматизація технологічних і бізнес-процесів*. 2020. №12(3), С. 19-28.

AUTOMATED CONTROL SYSTEM SIMULATION OF SUGAR MASSECUITE BOILING PROCESS IN VACUUM APPARATUS OF PERIODIC ACTION IN THE SOFTWARE ENVIRONMENT OF THE PROGRAMMED CONTROLLER

Skakovsky Y.M.

Odessa National Academy of Food Technologies
65039, Odessa, Kanatna Street , 112, yurysk@ukr.net

The results of the research carried out at the Odessa National Academy of Food Technologies within the framework of state-contracted topics are presented. The outcomes of the automated control system simulation of sugar massecuite cook process in vacuum apparatus of periodic performance are presented. The feasibility of simulation in the environment of microprocessor controller was substantiated, on its basis the automated workplace of the operator is created. Laboratory research was carried out at the bench agreed with the Customer of industrial microprocessor controllers and software of Ukrainian production, including SCADA-system "INDEL". Simplified model of boiling process as an object of control by two main channels is developed. The programs executing control algorithms for sugar massecuite boiling process in VA as well as the program executing the simplified model was created by FBD-like programming language of Ukrainian MK52 controller. For the connection between the software controller and computer the converter of interfaces type BPI-52 (MODBUS RTU to USB) Ukrainian production was used. Analysis of the control system results simulation obtained in the form of parametric diagrams and time graphs using SCADA-system "INDEL" allowed to make conclusions about the propriety of the developed control algorithms and implemented programs. On the basis of researches positive results, commercial version the VA operator automated workplace was created. The developed system was implemented as a part of upgraded ACS of process by Food Department of active sugar factory. Production testing and operation has confirmed the validity of the ACS through the boiling process of sugar massecuite which was developed according to the results of the relevant laboratory studies. On the basis of the obtained results were determined directions for further research, both in terms of control algorithms and SAC functions development.

Keywords: simulation, automated control system, automated operator workplace, microprocessor controller, control program, vacuum apparatus of periodic action, sugar massecuite, Food Department, sugar factory.

СИНТЕЗ ТА ДОСЛІДЖЕННЯ АСТАТИЧНИХ ОПТИМАЛЬНИХ ЦИФРОВИХ СИСТЕМ КЕРУВАННЯ РЕКТИФІКАЦІЙНОЮ КОЛОНОЮ**А.О. Стопакевич, О.А. Стопакевич**

Державний університет інтелектуальних технологій та зв'язку,
1, Кузнечна, Одеса, 65029, stopakevich@gmail.com
Державний університет «Одеська політехніка»,
1, пр. Шевченка, Одеса, 65044, stopakevich@opu.ua

Проблема синтезу систем керування ректифікаційними колонами є актуальною вже не перше десятиліття, однак більшість публікацій присвячена темі не оптимального синтезу систем керування, а синтезу децентралізованих систем керування з автономними регуляторами неперервного часу. Хоча такі системи керування майже апіорі не дозволяють досягти теоретичного максимуму в сенсі класичних інтегральних критеріїв оптимальності в задачі керування складними технологічними об'єктами, такими як ректифікаційна колона, вони мають практичні переваги – проблема їх цифрової реалізації може не розв'язуватись при умові коректної реалізації цифрового алгоритму в керуючому пристрої. Однією з причин меншої уваги дослідників до задачі оптимального багатовимірного керування ректифікаційними колонами є більша складність задачі синтезу придатних до промислової експлуатації багатовимірних систем керування. В роботах, які розглядають цю задачу, часто не досліджується проблема цифрової реалізації таких систем, їх стійкості при різних типах невизначеності та їх придатності до застосування в умовах структурної, а не тільки параметричної невизначеності моделі об'єктів керування. В статті розглядається задача синтезу оптимального цифрового лінійно-квадратичного багатовимірного регулятора ректифікаційною колоною з застосуванням наглядача й моделі збурень. Досліджено питання оптимальної структури моделі для спрощення задачі вибору вагових матриць при розв'язку рівняння Ріккати. Продемонстровано чіткий зв'язок між кроком дискретності і якістю керування. Сформульована задача синтезу системи керування з одним й з двома наглядачами (другий – для відтворення інтегральних станів). Продемонстрована процедура вибору вагових матриць, що спрощена до вибору лише вагових коефіцієнтів, в умовах параметричної й структурної невизначеності об'єкту керування. В якості об'єкту керування розглядається бражна колона спиртового виробництва. Цей об'єкт є доволі показовим і є одним з основних споживачів пари в брагоректифікаційній установці. Для того, щоб покращити якість процесів керування при всіх основних видах збурень необхідно застосування для керування бражною колоною багатовимірних регуляторів, що враховують вплив перехресних зв'язків між каналами. Застосування обох сформульованих задач синтезу дозволило отримати цифрові системи керування, що задовольняють вимогам виробництва та мають властивості параметричної й структурної робастності.

Ключові слова: Дискретна система автоматичного керування, лінійно-квадратичний регулятор, ректифікаційна колона, бражна колона, спирт, робастність, параметрична невизначеність, структурна невизначеність-

Вступ

Проблема розробки промислових систем керування ректифікаційними колонами привертає увагу дослідників багато років, однак більшість робіт, що присвячені цій темі, розглядають задачу синтезу децентралізованих систем керування з використанням класичних одновимірних регуляторів. Однак ректифікаційні колони мають значні перехресні зв'язки, тому децентралізовані системи керування навіть теоретично не можуть бути оптимальними. Між тим, технологія виробництва продукту високої якості вимагає високої якості керування. Наприклад, відхилення температури на контрольні тарілці колони повинно бути дуже малим при суттєвих збуреннях витрат й

концентрацій компонентів на вході в колону. Потрібну якість керування в умовах реального виробництва можуть дати тільки багатовимірні оптимальні цифрові регулятори. Хоча розробці таких регуляторів теж присвячено чимало досліджень, однак робіт, присвячено розробці астатичних багатовимірних систем керування ректифікаційними колонами, є мало. Звернемо увагу, що при розробці систем, які включають наглядач повного порядку, можливі два підходи. Перший підхід полягає у тому, що багатовимірний інтегратор включається до складу розширеного об'єкта керування, внаслідок чого наглядач відновлює стани об'єкту керування наряду зі станами інтегратора. Другий підхід полягає у тому, що наглядач відновлює тільки стани об'єкту керування, а стани багатовимірного інтегратора є доступними безпосередньо. Порівняльний аналіз вказаних підходів до синтезу багатовимірних систем керування ректифікаційною колоною є важливим для використання таких систем в промисловості.

Аналіз літературних джерел

Ректифікаційні колони застосовуються в багатьох галузях промисловості і задача синтезу систем керування для них розв'язується з використанням однакових принципів. Об'єктом нашого дослідження є задача автоматизації ректифікаційної колони спиртової промисловості. Ця задача є актуальною для економіки України й досліджується в ряді робіт, наприклад, в сучасних роботах [0-6].

Харчовий етиловий спирт виробляється на багатоколонних установках, які називають брагоректифікаційними (БРУ). Ці установки складаються з трьох чи більше колон. Типові БРУ, які експлуатуються в Україні, обов'язково містять бражну колону (БК), яка є першою й найбільш залежить від зовнішніх збурень за сировинним потоком. Оскільки ця колона значно впливає на якість спирту, подальшу увагу спрямуємо саме на задачу керування цим апаратом в найбільш поширеному типі установки – установці непрямої дії, в якій гостра нагрівальна пара подається на кожний апарат окремо.

Мета функціонування БК – це перетворення бражки (концентрація етанолу коливається, як правило, від 3 до 10%) в бражний дистилят (концентрація біля 40%). Задача аналітичного математичного моделювання бражної колони є складною [1], однак досвід показав, що з практичної точки зору моделі каналів з достатньою для синтезу систем керування точністю, можуть бути описані моделям в вигляді передатних функцій (ПФ) першого чи другого порядку з запізненням. Доцільність застосування моделей низького порядку продемонстрована, наприклад, в роботі [2] на аналітичній потарілчастій моделі БК, яка майже без втрат точності редукується до моделі другого порядку з запізненням. А в роботі [4] розроблена придатна для синтезу багатовимірних систем керування комплексна модель усієї БРУ, моделі каналів якої описуються маловимірними моделями.

В сучасній теорії задача синтезу системи керування ставиться, виходячи з динаміки об'єкту керування у цілому [7, 8]. Наявність перехресних зв'язків, які можуть бути описані лінійними передатними функціями, не є проблемою для синтезу більшості регуляторів сучасної теорії керування, зокрема оптимальних регуляторів [9]. Водночас необхідно зазначити, що задача керування БК, як й іншими колонами, має врахувати проблеми робастності. Постановка задачі в термінах стійкості до відхилення параметрів лінійних моделей в заданих діапазонах не завжди є достатньою. Більш продуктивною є перевірка працездатності системи керування також й відносно структурної невизначеності моделі [9].

Прямим технологічним показником якості системи керування БК є точна підтримка концентрації спирту в бражному дистиляті X_d . Ця концентрація залежить від великої кількості впливів, основними з яких є: концентрація спирту в бражці і її склад, температура бражки, витрата бражки, витрата й температура пари [19]. Хоча вимірювання цього показника якості теоретично можливо, однак зараз немає точних

давачів спирту в розчинах, які містять, поряд з етанолом, багато різних вищих спиртів. Тому замість вимірювання концентрації етанолу в бражному дистилляті використовується непрямий параметр – температура зверху колони. Однак, тільки при відхиленні температури від номіналу на ± 0.5 , температура зверху є сильно корельованою з концентрацією етанолу. При більшому відхиленні кореляція стає неточною. І хоча в деяких промислових децентралізованих системах керування БК реалізують канал «витрата бражки–температура зверху», однак в них потрібне відхилення температури не дотримується [11, 12, 13].

В роботах [9, 14, 15, 16, 17] показано, що використання лінійно-квадратичних регуляторів стану і модельно-прогнозуючих регуляторів стану з наглядом й моделлю збурень в вигляді стрибка дозволяє досягти якісних перехідних процесів в системах керування ректифікаційними установками. Однак проблема синтезу наглядача в роботах розглядалась з точки зору стійкості системи чи врахування характеру шумів, однак не розглядалось питання оптимальної структури астатичної системи керування з наглядом. Крім того, не достатньо розглянуто питання оптимальної процедури синтезу цифрових систем керування ректифікаційними колонами з використанням дискретного лінійно-квадратичного регулятора.

Цифрова аперіодична система керування з лінійно-квадратичним регулятором має включати нагляд стану й модель збурень в вигляді стрибку (інтегратор). В літературі описані дві структури систем автоматичного керування [7]: з одним й двома наглядом стану. Перший інтегратор відновлює поточні стани об'єкту, а другий дозволяє відновити стани інтегратору. Принципові структурні схеми моделей замкнених систем автоматичного керування (САК) з одним й двома наглядом показані на рис. 1.

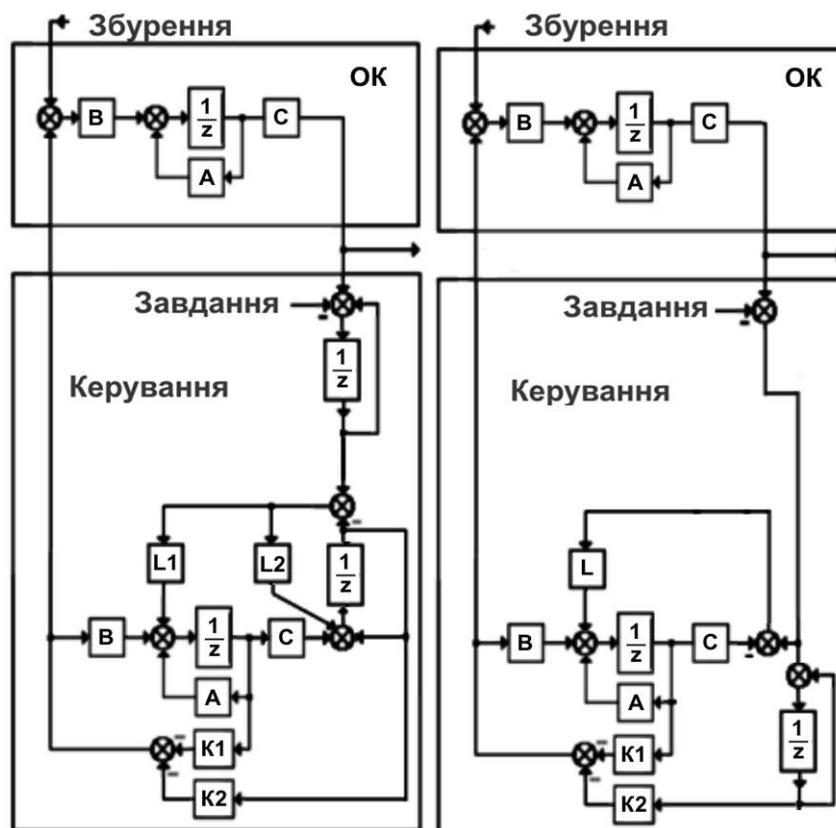


Рис. 1. Структурні схеми моделей систем керування з лінійно-квадратичними регуляторами ($K1$, $K2$) з одним і двома наглядом ($L1$, $L2$).

Розв'язок задачі синтезу систем керування з використанням модного наглядача розглянуто в літературі й може бути реалізований за допомогою стандартних функцій

Matlab. Водночас порівняльний аналіз САК з одним й двома наглядачами з результатів аналізу літератури не проводився. Недостатня увага також присвячена проблемі робастності цифрової системи керування ректифікаційною колоною, яка реалізується на базі лінійно-квадратичного регулятора.

Мета та задачі дослідження

Метою роботи є синтез оптимального астатичного багатовимірної цифрового лінійно-квадратичного регулятора ректифікаційної колони (бражної колони спиртового виробництва).

Задачі дослідження наступні: сформулювати загальні вимоги до цифрової системи керування; провести вибір каналів керування; провести вибір оптимальної форми представлення математичної моделі динаміки; провести вибір методу представлення запізнення; сформулювати алгоритм синтезу систем керування з одним й двома наглядачами; провести вибір кроку дискретності цифрової системи керування; провести дослідження впливу вагових коефіцієнтів на якість керування регуляторів; провести імітаційне моделювання розроблених систем керування й провести їх порівняльний аналіз.

Основна частина

Формулювання загальних вимог до цифрової системи керування

Технологічні вимоги до відхилення температури зверху БК від заданого значення доволі жорсткі: довгострокові $\pm 0.5^\circ\text{C}$, короткострокові $\pm 1^\circ\text{C}$. Вимоги до відхилення тиску довгострокові ± 0.5 кПа, короткострокові – ± 1.5 кПа. Вимоги до відхилення температури води після дефлегматора часто не ставляться, однак орієнтовно прийемо їх такими: довгострокові $\pm 3-5^\circ\text{C}$, короткострокові $\pm 10^\circ\text{C}$.

Запас керуючого впливу в відсотках є обмежений. Звичайно він становить $\pm 20-30\%$ від максимальної витрати. Працездатність системи керування при дії збурень будемо досліджувати при найгіршому типі збурень – збуренні стрибком по всім вхідним каналам величиною 10%. Практика показує, що якщо система керування витримує таке збурення, то вона витримує й стохастичні, імпульсні й експериментально зняті тренди збурень з виробництва.

В термінах параметричної робастності сформулюємо вимоги для моделі каналів в вигляді інерційної ланки першого порядку з запізненням (FOPDT). Прийемо, згідно з рекомендаціями, приведеними в [18], для всіх каналів припустимо відхилення постійної часу $\pm 40\%$, часу запізнення $\pm 20\%$, коефіцієнту передачі $\pm 10\%$.

Вибір каналів системи керування

Проблема вибору оптимальної конфігурації системи керування бражної колони для лінійно-квадратичного регулятора розглянута в роботі [17]. Зазвичай, для БК розглядаються системи керування з двома та трьома керуючими впливами. В задачі з двома керуючими впливами багатовимірний регулятор значно не покращить якість керування і не дозволить досягнути поставленої мети керування при дії збурень. Включення в якості керуючого впливу витрати бражки додає значні перехресні впливи в систему керування. Отже, тільки при постановці задачі керування з трьома керуючими впливами застосування багатовимірної регулятора має сенс і дозволяє досягти мету керування. Тому для лінійно-квадратичного регулятора бражної колони доцільно обрати конфігурацію з трьома впливами.

Вибір оптимальної форми побудови математичної моделі динаміки

Експериментальна математична модель динаміки об'єкту керування (ОК) в вигляді матриці передатних функцій представлена в табл. 1

Таблиця 1.

Параметри, що вимірюються	Експериментальна математична модель		
	Керуючі впливи, %		
	Витрата бражки F	Витрата пари V	Витрата хол. води G
Тиск зверху P_B (Па)	$\frac{-173}{370s+1}$	$\frac{287}{73s+1}$	$\frac{-10.8}{220s+1}$
Температура зверху T_B (C)	$\frac{-0.15}{450s+1}e^{-72s}$	$\frac{0.05}{220s+1}e^{-60s}$	$\frac{-0.009}{190s+1}e^{-100s}$
Температура води, що відходить $T_{отх}$ (C)	$\frac{0.9}{423s+1}e^{-160s}$	$\frac{0.1}{200s+1}e^{-150s}$	$\frac{-0.285}{268s+1}e^{-74s}$

Бачимо, що коливання температури проходить в десятих долях градуса Цельсія, коливання тиску в сотнях Паскалів. Досвід дослідження [17] показує, що оптимальним варіантом є синтез регулятора без застосування специфічних для окремих каналів вагових коефіцієнтів інтегрального критерію якості. Для цього коефіцієнти математичної моделі треба масштабувати з використанням нормалізуючих множників $y_s = [57.4; 0.03; 0.18]$, а постійні часу перерахувати в хвилини. Математична модель після нормалізації приведена в табл. 2.

Таблиця 2.

Параметри, що вимірюються	Нормалізована математична модель		
	Керуючі впливи, %		
	Витрата бражки F	Витрата пари V	Витрата хол. води G
Тиск зверху $P_{B(n)}$	$\frac{-3.01}{6.17s+1}$	$\frac{5}{1.22s+1}$	$\frac{-0.19}{3.67s+1}$
Температура зверху $T_{B(n)}$	$\frac{-5}{7.5s+1}e^{-1.2s}$	$\frac{1.67}{3.67s+1}e^{-1.0s}$	$\frac{-0.3}{3.17s+1}e^{-1.67s}$
Температура води, що відходить $T_{отх(n)}$	$\frac{5}{7.05s+1}e^{-2.67s}$	$\frac{0.56}{3.33s+1}e^{-2.5s}$	$\frac{-1.58}{4.47s+1}e^{-1.23s}$

Проведемо аналіз нормалізованої моделі за допомогою матриці RRA [19].

$$RRA = \begin{bmatrix} -0.15 & 1.19 & -0.04 \\ 1.01 & -0.19 & 0.18 \\ 0.14 & -0.00 & 0.86 \end{bmatrix}$$

Бачимо, що значна частина матриці має від'ємні й далекі від одиниці значення, що вказує на високий ступінь взаємозв'язку й підтверджує вибір каналів.

Вибір методу представлення запізнення

Відомо, що в неперервному часі математична форма запису в вигляді простору станів не дозволяє представити чисте запізнення без апроксимації – частіше за все обирають апроксимацію Паде. В дискретній формі представлення запізнення можливе, однак необхідна кількість станів для представлення ланки чистого запізнення з часом τ дорівнює $n = \tau / \Delta t$. Таке представлення доцільно не для синтезу, а для моделювання об'єкту керування (назвемо таку дискретну модель P_{d1}) в моделі системи автоматичного керування (САК). Для синтезу регулятора використаємо апроксимацію запізнення ланкою Паде першого порядку (назвемо таку дискретну модель P_{d2}). Використання різних моделей для розрахунку й моделювання САК є додатковим індикатором робастності отриманого регулятора.

Синтез системи керування С1 з одним наглядачем

- 1) Сформуємо дискретну систему P_{d2} в просторі станів з використанням апроксимації Паде 1 порядку (за допомогою функцій `pade`, `ss`, `c2d` системи Matlab).
- 2) Введемо значення вагових коефіцієнтів Q_{1K1} , Q_{1K2} , Q_{1L} , R_{1K} , R_{1L} . Для початку доцільно їх прийняти одиничними.
- 3) Сформуємо вагові матриці $Q_1 = \begin{bmatrix} C^T \cdot Q_{1K1} \cdot C & 0 \\ 0 & Q_{1K2} \end{bmatrix}$, $R_1 = R_{1K}$, C – матриця з P_{d2} .
- 4) Розрахуємо регулятор стану з інтегральною складовою за допомогою функції `lqi` (P_{d2}, Q_1, R_1). Ця функція використовує розширену матрицю моделі виду $A_1 = \begin{bmatrix} A & 0 \\ -C \cdot \Delta t & I \end{bmatrix}$, $B_1 = \begin{bmatrix} B \\ -D \cdot \Delta t \end{bmatrix}$, де A , B , C , D – матриці системи P_{d2} , I – одинична матриця.
- 5) Сформуємо наглядач стану за допомогою функції `dlqr` для матриць системи P_{d2} $L = \text{dlqr}(A^T, C^T, Q_{1L}, R_{1L})^T$.
- 6) Сформуємо регулятор C_1 як систему в дискретному просторі станів з наглядачем за допомогою команд $L = \text{estim}(P_{d2}, L, [1:m], [1:m])$; $C_1 = \text{lgtrack}(L, K)$; де $m=3$ – кількість виходів й виходів.

Синтез системи керування С2 з двома наглядачами

- 1) Сформуємо дискретну систему P_{d2} в просторі станів з використанням апроксимації Паде першого порядку (за допомогою функцій `pade`, `ss`, `c2d`).
- 2) Введемо значення вагових коефіцієнтів Q_{2K1} , Q_{2K2} , Q_{2L} , R_{2K} , R_{2L} . Для початку доцільно їх прийняти одиничними.

- 3) Сформуємо вагові матриці $Q_2 = \begin{bmatrix} C^T \cdot Q_{2K1} \cdot C & 0 \\ 0 & Q_{2K2} \end{bmatrix}$, $R_2 = R_{2K}$.
- 4) За матрицями A, B, C системи P_{d2} сформуємо розширені матриці

$$A_1 = \begin{bmatrix} A & 0 \\ C & I \end{bmatrix}, B_1 = \begin{bmatrix} B \\ 0 \end{bmatrix}, C_1 = [0 \quad I].$$

- 5) Використовуючи функцію `dlqr` розрахуємо параметри наглядача й регулятора стану

$$K = [K_1, K_2] = \text{dlqr}(A_1, B_1, Q_2, R_2); L = \begin{bmatrix} L_1 \\ L_2 \end{bmatrix} = \text{dlqr}(A_1^T, C_1^T, Q_{2L}, Q_{2R})^T.$$

- 6) Сформуємо регулятор C_2 як систему $(A_R, B_R, C_R, 0)$

$$A_R = \begin{bmatrix} A - B \cdot K_1 & -B \cdot K_2 - L_1 & L_1 \\ C & I - L_2 & L_2 \\ 0 & 0 & I \end{bmatrix}, B_R = \begin{bmatrix} 0 \\ 0 \\ I \end{bmatrix}, C_R = [K_1 \quad K_2 \quad 0],$$

Моделювання перехідних процесів в системі керування

Моделювання перехідних процесів може проводитись як програмно, так і за допомогою пакетів візуального імітаційного моделювання, таких як Simulink. Використання дискретної реалізації систем та масштабування часу на сучасному комп'ютері дозволяє досягти достатньо високої швидкості моделювання. Це робить зручною процедуру емпіричного вибору параметрів.

Особливості процедури моделювання САК, що застосовувалась при дослідженні: 1) моделі об'єкта і регулятора представляються в дискретному просторі станів з однаковим кроком Δt ;

- 2) моделюється система керування з нормованою моделлю ОК, вихідні й вхідні значення керованих змінних масштабуються за допомогою по елементного ділення й множення на вектор us ;
- 3) модель об'єкта $Pd1$ реалізується з чистим запізненням;
- 4) для моделювання різних типів невизначеностей модель $Pd1$ перераховується (виходячи зі зміни коефіцієнтів, каналів, тощо);
- 5) модель $Pd2$ (дискретна модель в просторі станів, отримана з нормованої матриці передатної функції з використанням апроксимації ланки запізнення ланкою Паде першого порядку) при всіх експериментах залишається незмінною, але безпосередньо не входить до моделі САК;
- 6) перед запуском процедури імітаційного моделювання параметри регуляторів $C1$ і $C2$ та їх наглядців при всіх експериментах розраховуються за незмінною моделлю $Pd2$, настроювання проводиться шляхом зміни вагових коефіцієнтів.
- 7) при імітаційному моделюванні збурення у вигляді вектору фдодається до вектору виходів регулятора u , який реалізує закон керування, виходячи з різниці між вектором завдання та вектором керованих змінних.

Загальні принципи вибору параметрів інтегрального квадратичного критерію при синтезі цифрової системи керування

В задачі керування з нормованою моделлю визначальним є крок дискретності Δt . Від нього залежить як стійкість системи, так й основні прямі показники якості. У системі з інтегральним критерієм виду $J = \sum_{i=1}^{\infty} y^T \cdot Q \cdot y + \Delta u^T \cdot R \cdot \Delta u$ параметри $Q_{1K1}, R_{1K} / Q_{2K1}, R_{2K}$ впливають на базовий запас стійкості системи керування. Параметр Q_{1K2} дозволяє покращити стійкість системи до параметричної невизначеності. Настроювання параметрів наглядача не сильно впливає на якість перехідних процесів, але можуть впливати на швидкість перехідних процесів й на чутливість до шумів вимірювання. В роботі описувати задачу настроювання наглядача не будемо, оскільки зміна коефіцієнтів $Q_{1L}, R_{1L} / Q_{2L}, R_{2L}$ не покращує якість процесів керування в сенсі поставлених задач.

Вибір кроку дискретності цифрової системи керування

Оскільки перехідні процеси в ректифікаційних колонах достатньо тривалі, то крок дискретності може бути рівним десяткам секунд чи хвилинам, тому технічні обмеження, пов'язані з часом збору інформації як правило не викликають проблем. Вибір величини кроку дискретності як правило робиться напівемпірично, однак для орієнтації рекомендується використовувати власні значення системи.

Розглянемо два практичних правила для визначення кроку дискретності системи.

Перше правило [7] може бути сформовано наступним чином: $dt_1 = 1 / \max(|\lambda(A)|)$.

Друге правило має наступний вигляд: $dt_2 = (0.2 \cdot \pi) / \max(|\lambda(A)|) \approx 0.6283 / \max(|\lambda(A)|)$.

При розрахунку кроку дискретності час запізнення для неважко керованих об'єктів можна не враховувати. Розрахувавши $\max(|\lambda(A)|)$ для Pd_2 , що дорівнює 0.8189, одержимо $dt_1 = 1.2200$, $dt_2 = 0.7665$. Крім того, використаємо емпіричне правило – крок дискретності замкненої системи керування має бути в 2..10 разів меншим, ніж оптимальний крок дискретності для моделі об'єкту. Отже, перевіримо якість керування в системі з регулятором C_1 з кроками $dt_1, dt_2, dt_1 / 10, dt_2 / 10$

$$\Delta t \in [0.0767, 0.1000, 0.1220, 0.5000, 0.7665, 1.0000, 1.2200].$$

Об'єкт будемо моделювати при номінальних параметрах об'єкта й збуренні $f = [10; 10; 10]$. В якості критеріїв якості виберемо такі прямі показники якості, як модуль максимальних відхилень керуючих впливів, модуль максимальних відхилень керованих змінних, час регулювання.

Графік залежності прямих показників якості від Δt показаний на рис. 1.

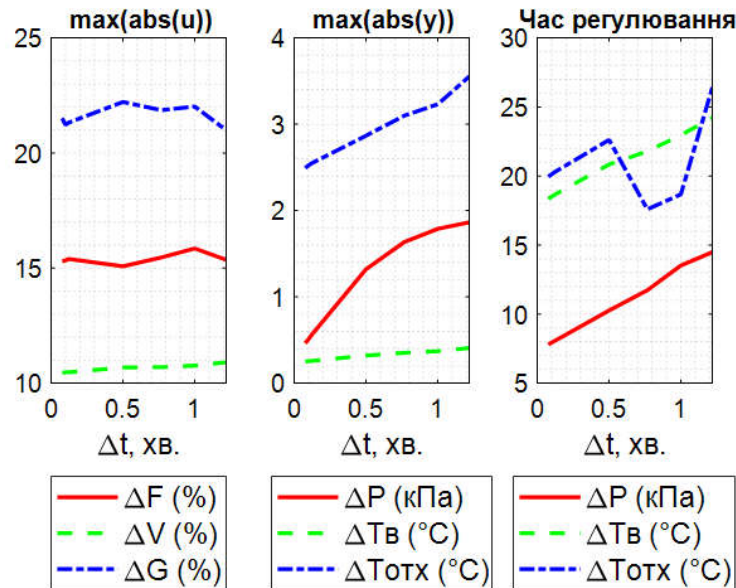


Рис. 1. Залежність прямих показників якості від кроку дискретності при стандартних вагових коефіцієнтах (система з регулятором С1)

Бачимо, що максимум відхилення керуючого впливу майже не залежить від кроку дискретності, а максимальне відхилення й час регулювання зі збільшенням кроку дискретності збільшуються. Крім того, бачимо що правило зменшення кроку дискретності в 2..10 раз працює. Вибір між $\Delta t_1 / 10$ і $\Delta t_2 / 10$ не дуже суттєвий, однак, якщо використовувати критерій максимуму відхилення, то доцільно обрати перший, тобто $\Delta t = 0.122$ хв., так як різниця між показниками не однозначна (наприклад, максимум керування при $\Delta t_2 / 10$ більший), а швидкість моделювання з більшим кроком прискориться. Якщо ж орієнтуватись на час регулювання, то деякий оптимум буде на точці $\Delta t = 0.55$ хв. Отже, виберемо $\Delta t = 0.122$ хв.

Вибір вагових коефіцієнтів для забезпечення параметричної робастності регулятора С1

Як було сформульовано в підрозділі 4.1, в термінах FOPDT моделі доцільно розглядати відхилення постійної часу $\pm 40\%$, часу запізнення $\pm 20\%$, коефіцієнту передачі $\pm 10\%$. Для ректифікаційної колони встановлено, що з трьох приведених типів відхилень найгіршим є відхилення постійної часу в меншу сторону. Таким чином, будемо шукати кращі вагові коефіцієнти спочатку саме для цього найгіршого випадку $T_R = 0.6 \cdot T_0$. Зменшувати постійну часу будемо за всіма каналами об'єкта. В якості критерію працездатності системи при зміні вагового коефіцієнту виберемо максимум відхилення керуючого впливу. Збільшення порядку коефіцієнту Q_{IKI} призводить до втрати стійкості системи. Збільшення порядку коефіцієнту R_{IK} в діапазоні 1..1000 майже не впливає на максимум відхилення керуючих впливів. Збільшення порядку коефіцієнтів Q_{IL} і R_{IL} призводить до значного погіршення критерію (до сотень відсотків). Таким чином, бачимо, що єдиним параметром, що можливо змінювати для досягнення параметричної робастності є параметр R_{IK} . Отже, встановимо значення $R_{IK} = 10$ й дослідимо прямі показники якості при зміні параметрів моделі об'єкта.

Змінювати параметри будемо за всіма каналами об'єкта. Результати моделювання замкнених САК, підключених для об'єкта зі зміненими параметрами показані на рис. 4.

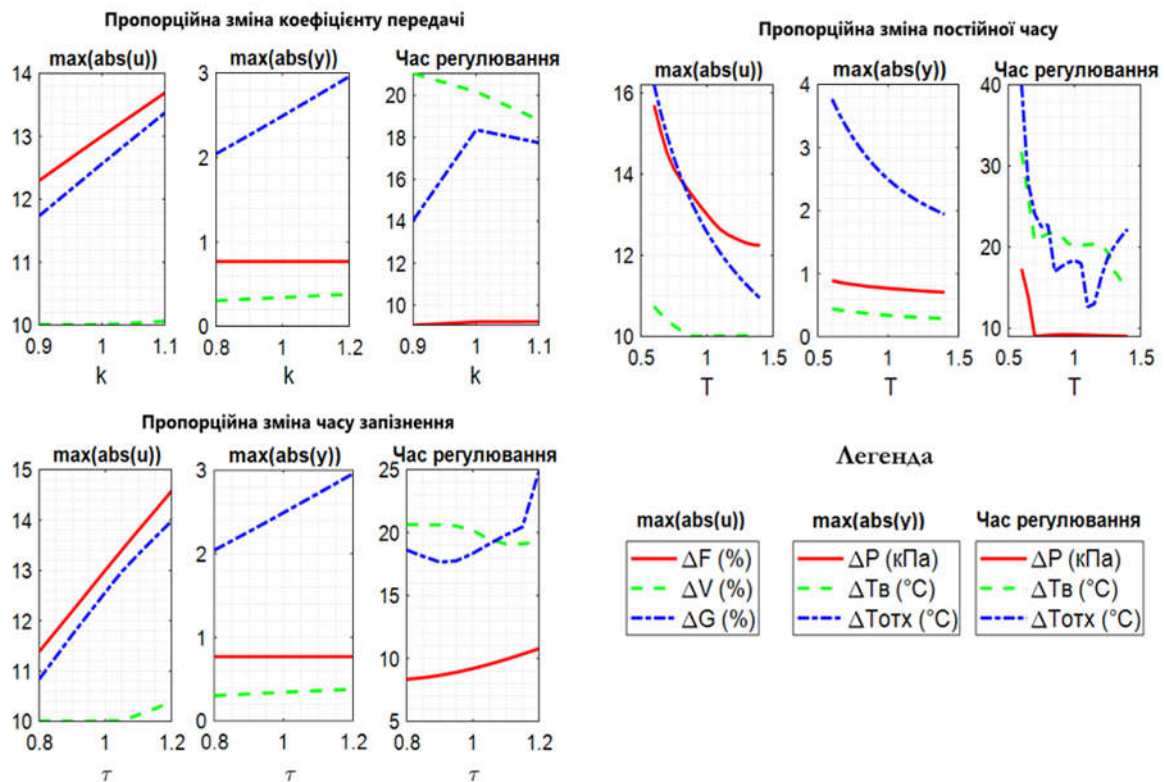


Рис. 2. Залежність прямих показників якості перехідних процесів від множника зміни номінальних параметрів об'єкта керування при $R1K.=10$ (система з регулятором С1)

Графіки, що показані на рис. 2, демонструють, що розроблена система керування має параметричну робастність відповідно до поставлених вимог. Відхилення всіх параметрів в заданих діапазонах не є критичним.

Вибір вагових коефіцієнтів для забезпечення структурної робастності регулятора С1

Відомо, що математичні моделі каналів БК, які пов'язані з температурою зверху колони, можна апроксимувати не лише першим порядком з запізненням, але й другим порядком з запізненням. В випадку БК це не дуже збільшує точність моделювання, однак представляє інтерес для нашого дослідження. Температурним параметром БК є температура зверху. Параметри моделі другого порядку за цією змінною приведені в табл.3. Розгінні характеристики, моделей каналів першої і другого порядків з запізненням показані на рис. 3.

Таблиця 3.

Моделі каналів нормалізованої моделі другого порядку (SOPDT) для температури зверху

Параметр	Витрата бражки F, %	Витрата пари V, %	Витрата хол. води G, %
Температура зверху, T_v (н)	$\frac{-5}{(4.5s + 1)^2} e^{-1.2s}$	$\frac{1.67}{(2.2s + 1)^2} e^{-1.0s}$	$\frac{-0.3}{(1.9s + 1)^2} e^{-1.67s}$

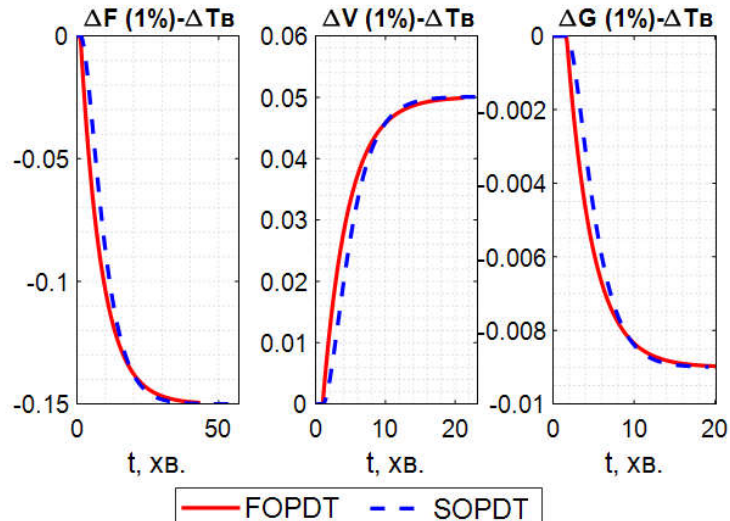


Рис. 3. Розгінні характеристики не нормалізованих моделей каналів FOPDT(див. табл. 1) і SOPDT(див. табл. 3 з урахуванням нормалізації).

Як бачимо, розгінні характеристики каналів відрізняються незначно, однак підключення регулятора С1 при $R1K=10$ до моделі об'єкта Pd1 зі зміненими моделями каналів призводить до втрати стійкості САК при заданих обмеженнях відхилення моделі. Для збільшення запасу стійкості САК відносно структурної невідповідності необхідно змінювати параметр $Q1K2$. Для розглянутого випадку система стає стійкою до зазначеної структурної невідповідності моделі при значенні $Q1K2=0.1$.

Вибір вагових коефіцієнтів для забезпечення параметричної й структурної робастності регулятора С2

Настроювання системи керування з регулятором С2 виконується за аналогічними правилами. Для системи керування оптимальний крок дискретності є таким самим. Для забезпечення параметричної робастності величину $R2K$ необхідно встановити рівною 100. Аналогічно для забезпечення структурної робастності необхідно встановити $Q2K2=0.1$. На відміну від системи з регулятором С1 система з регулятором С2 більше реагує на зміну вагових коефіцієнтів наглядача. З точки зору прямих показників якості істотного покращення зміною вагових коефіцієнтів наглядача регулятора С2 досягнуто не було, однак характер коливальності процесу можливо дещо змінювати.

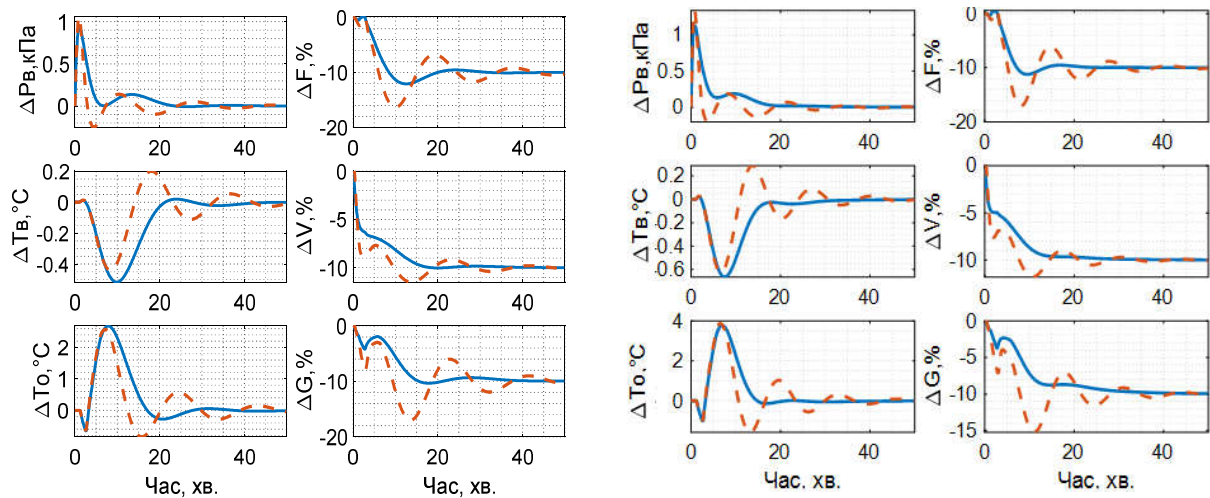
Порівняльний аналіз систем керування з регуляторами С1 і С2

Проведемо 4 імітаційні експерименти:

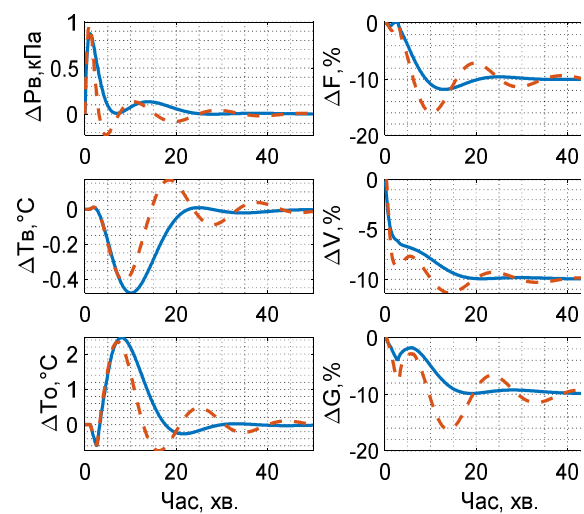
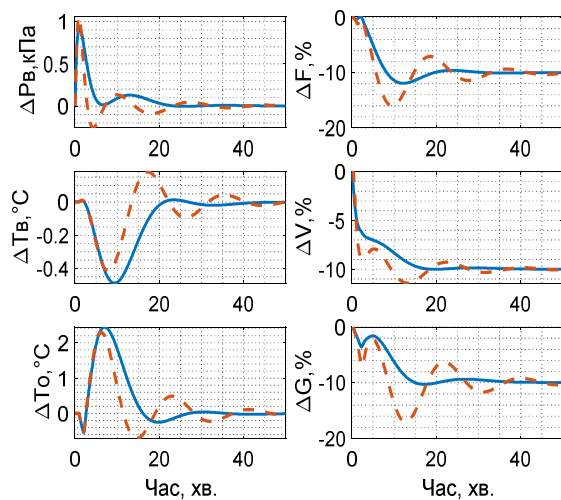
- 1) Збурення $f=[10;10;10]$, параметри ОК не змінюються
- 2) Збурення $f=[10;10;10]$, параметри ОК змінюються в сторону $T=0.6T$
- 3) Збурення $f=[10;10;10]$, параметри ОК змінюються в сторону $\tau=0.8\tau$
- 4) Збурення $f=[10;10;10]$, параметри ОК змінюються в сторону $k=0.9k$

В усіх експериментах регулятор розраховується за моделлю з каналами виключно в вигляді ланок першого порядку, а об'єкт моделюється з каналами по температурі верху з ланками 2 порядку.

Перехідні процеси при проведенні експериментів показані на рис. 4.



1) Номінальні параметри ОК

2) $T=0.6T$ 3) $\tau=0.8\tau$ 4) $k=0.9k$ — Регулятор C_1 — Регулятор C_2 **Рис. 4.** Порівняльний аналіз перехідних процесів в системах керування при проведених експериментах

Бачимо, що обидва регулятори при запропоновані процедурі налаштування справляються з поставленими вимогами. В цілому, якщо проведено масштабування моделі, застосування наглядча з відновленням інтегрованих станів не покращує якості перехідних процесів, але збільшує ступінь їх коливальності.

Висновки

Проблема синтезу оптимальних цифрових багатовимірних систем керування ректифікаційними установками є актуальною. Для того, щоб досягнути з використанням методів сучасної теорії керування більш якісних перехідних процесів треба зважати на значну кількість факторів, на яку часто в науковій літературі не звертають увагу.

В статті розроблена процедура синтезу астатичного регулятора на базі лінійно-квадратичного регулятора, особливістю якої є масштабування математичної моделі, що спрощує процедуру налаштування регулятора. З використанням запропонованої процедури показано як розв'язати проблеми вибору оптимального кроку дискретності, досягти параметричної й структурної робастності, проаналізована проблема

необхідності відновлення інтегральних станів в нагляді з лінійно-квадратичним регулятором. На простому прикладі продемонстровано, що підходи робастного синтезу можуть не гарантувати практичний результат, оскільки обмежуються структурою моделі об'єкту керування.

Список літератури

1. Кишенько В.Д., Смітюх Я.В. Модель брагоректифікаційної установки як об'єкта керування. Збірник наукових праць Кіровоградського національного технічного університету "Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація". 2004. Вип. 15. С. 229–234.
2. Ульянов Н.И., Кузьмицкий И.Ф. Аппроксимация аналитических моделей динамики тепло- и массообменного процесса ректификации. Труды Белорусского гос. технологического ун-та. Физико-математические науки и информатика. 2011. № 6 (144). С. 85–89.
3. Луцька Н.М., Гриценко Н.Г. Розробка моделей системи керування бражною колони. Наукові праці Нац. Університету харчових технологій, 2016. № 6. Т. 22. С. 22–27.
4. Стопакевич А.А. Многомерная модель брагоректификационной установки косвенного действия. Наукові праці ОНАХТ, 2010. №38. Т. 1. С. 360–365.
5. ТОВАЖНЯНСКИЙ Л.Л., УЛЬЕВ, Л.М., СТАВРОВА, К.И. Экстракция данных для теплоэнергетической интеграции пятиколонного агрегата производства спирта. Вестник Нац. техн. ун-та "ХПИ", 2012.
6. Смітюх Я.В., Кишенько В.Д. Ідентифікація брагоректифікаційної установки на основі нейронечіткої мережі. Східно-Європейський журнал передових технологій, 2011. № 1/3 (49). С. 22–25.
7. Стопакевич А.А. Системный анализ и теория сложных систем управления. Одесса: Астропринт, 2013.
8. Ладанюк А.П., Луцька Н.М., Кишенько В.Д., Власенко Л.О., Іващук В.В. Сучасна теорія управління. Київ: Ліра-К, 2019
9. Стопакевич А. А. Разработка робастной системы управления колонной атмосферной перегонки нефти. Восточно-Европейский журнал передовых технологий, 2015. № 5(2). С. 49–57.
10. Маринченко В.О., Домарецький В.А., Шиян П.Л., Швець В.М., Циганков П.С., Жолднер І.Д. Технологія спирту. Вінниця: Поділля–2000, 2003.
11. Смітюх Я.В., Кишенько В.Д. Відновлення та оцінка трактора на основі часових рядів роботи брагоректифікаційної установки. Східно-Європейський журнал передових технологій, 2006. № 3/3(21). С. 55–57.
12. Novakovska N., Kyshenko V. Fractal analysis of distillation unit time series in prediction and control problems. Ukrainian Journal of Food Science, 2015. V. 3.# 2. P. 243–253.
13. Гриценко Н.Г., Ладанюк Л.П., Луцька Н.М., Смітюх Я.В., Кириленко Р.Г. Сучасні методи керування брагоректифікаційними установками. Енергетика і автоматика, 2016. № 3 (29). С. 68–78.
14. Пастушенко В.С., Стопакевич А.А., Стопакевич А.А. Модельно-прогнозирующее управление ректификационной колонной в технологическом процессе утилизации углекислого газа в производство метанола. Технологический аудит и резервы производства, 2016. №6/2 (32). С. 36–40.
15. Стопакевич А.А. Цифровая многомерная система управления технологической установкой. Цифрові технології, 2011. №9.

16. Стопакевич А.А. Синтез и исследование цифровых систем супервизорного управления колонной ректификации нефти. Автоматизация технологических и бизнес-процессов, 2015. Т. 7, № 4. С. 24–33.
17. Стопакевич А.А., Стопакевич А.А. Разработка живучих систем управления технологическими установками. Проблемы региональной энергетики, 2021. Т. 3. № 2. С. 243–253.
18. Аксельрод Л.А., Мандельштейн М.Л. К исследованию динамики брагоректификационных установок. Сборник научных трудов НПО «Пищепромавтоматика», 1974. С. 38–48.
19. Amit J., Babu B.V. Relative Response Array: A New Tool for Control Configuration Selection. International Journal of Chemical Engineering and Applications, 2015. Vol. 6. No. 5. P. 356–362.

SYNTHESIS AND RESEARCH OF AN ASTATIC OPTIMAL DIGITAL CONTROL SYSTEMS OF A DISTILLATION COLUMN

Andrii Stopakevych, Oleksii Stopakevych

National University of Intellectual Technologies and Communications,
1, Kuznechna street, Odessa, 65029, Ukraine, stopakevich@gmail.com
National University "Odessa Polytechnic", 1,
Shevchenko Ave., Odessa, 65044, Ukraine, stopakevich@opu.ua

The problem of distillation columns control systems synthesis is an actual topic for many years. But the research aim of most publications is not to develop an optimal control system, but to develop decentralized control systems with autonomous continuous-time controllers. Although such control systems almost a priori do not allow to reach the theoretical optimum in the sense of classical integral performance index in the problem of control of complex technological plants, such as distillation columns, they have practical advantages in their digital implementation. One of the reasons for less attention of researchers to the problem of optimal multivariable control of distillation columns is the greater complexity of the problem of commercially suitable control systems development. The problem of digital implementation of such systems, their stability under different types of uncertainties, such as their suitability for use in conditions of structural and parametric uncertainties of the plant model, is often not studied in the works that consider this problem. The problem of synthesis of the optimal digital linear-quadratic multivariable controller for a distillation column with the use of an observer and a disturbance model is considered in the article. The problem of the optimal plant model structure for simple choice of weight matrices in solving the Riccati equation is investigated. A clear relationship between the sample time and the control quality is found. The problem of synthesis of the control system with one and with two observers (the second is for observing the integrated states) is formulated. The simple approach of weight matrices selection is suggested, which needs to specify only weight coefficients and can take into account a parametric and structural uncertainty of the plant. The mash distillation column control problem is researched. To improve the quality of control processes for all major types of disturbances, we use multivariable controllers which take into account the influence of cross-links between channels. The application of both formulated synthesis problems allowed obtaining digital control systems that meet the requirements of production and have the properties of parametric and structural robustness.

Keywords: Discrete automatic control system, linear-quadratic controller, distillation column, mash column, alcohol, robustness, parametric uncertainty, structural uncertainty.

**ДОСЛІДЖЕННЯ МЕТОДУ СТАБІЛІЗАЦІЇ ДИСПЕРСІЇ ВИПАДКОВИХ
ВЕЛИЧИН НА ОСНОВІ СТЕПЕНЕВИХ ПЕРЕТВОРЕНЬ ДЛЯ МОДЕЛЕЙ
МАШИННОГО НАВЧАННЯ****О.О. Фомін¹, М.М. Масрі², О.А. Туманов², О.В. Сєрбова², В.В. Ткаченко²**¹Одеський національний політехнічний університет,
пр. Шевченка, 1, Одеса, 65044; Україна; fomin@onu.ua²Приватний заклад вищої освіти «Одеський технологічний університет «Шаг»»,
вул. Садова, 3, Одеса, 65023; Україна; dr.mohanadmasri@gmail.com

В роботі розв'язується завдання побудови моделей машинного навчання. Метою роботи є підвищення точності моделей машинного навчання для випадку розподілу даних навчальної вибірки відмінного від нормального. Поставлена мета досягається шляхом застосування статистичних перетворень до ознак навчальної вибірки для стабілізації дисперсії випадкових величин. Найбільш суттєві результати: досліджено ефективність методу статистичної класифікації на основі баєсова підходу для побудови моделей у вигляді поліномів другого порядку, що дозволяє підвищити точність моделювання у випадку розподілу даних навчальної вибірки відмінного від нормального, проведені експериментальні дослідження і сформульовані рекомендації щодо ефективності застосування статистичних перетворень даних навчальної вибірки при різних розподілах даних навчальної вибірки для наступних законів розподілу випадкових величин: рівномірний, біноміальний, експоненціальне. Значимість отриманих результатів: застосування сформульованих рекомендацій дозволяє забезпечити підвищення точності моделей машинного навчання в умовах розподілу даних навчальної вибірки відмінного від нормального. Запропоновані рекомендації апробовані на даних тестового завдання. Завдання демонструє підвищення точності моделей машинного навчання для більшості розглянутих законів розподілу випадкових величин.

Ключові слова: статистичні характеристики, випадкова величина, степеневі перетворення, моделі машинного навчання.

Вступ

Великі обсяги даних та значні успіхи в області Data Science і Big Data забезпечують нові можливості при рішенні прикладних задач, пов'язані з підвищенням точності побудови моделей машинного навчання [1, 2]. Ефективне функціонування сучасних інформаційних систем в таких умовах забезпечується зростаючими вимогами до процесів обробки вихідної інформації, в тому числі, до методів статистичної обробки даних.

Одними з поширених в теоретичних розробках є задачі, пов'язані з використанням теорії перевірки статистичних гіпотез. Незважаючи на те, що в загальному випадку теорія перевірки статистичних гіпотез розроблена без накладення обмежень на щільності розподілу розглянутих випадкових величин, на практиці, у зв'язку зі спостереженням нормального закону розподілу випадкових величин в багатьох природних процесах, зручністю використання математичного апарату і наявністю ефективних інструментальних засобів комп'ютерного моделювання найбільш широко використовуються гаусові моделі випадкових величин, що складають навчальну вибірку. Це не завжди адекватно відображає реальні природні процеси, що, в загальному випадку, призводить до зниження точності побудови моделей машинного навчання [3].

Проблема подальшого розвитку даного напрямку полягає в тому, що обробка негауссовских процесів не в повній мірі досліджена і потребує подальшого своєму вивченні. Тому, подальший розвиток моделей машинного навчання та методів їх побудови, в разі розподілу даних навчальної вибірки відмінного від нормального, є актуальним напрямком досліджень.

Мета роботи

Метою роботи є підвищення точності моделей машинного навчання у випадку розподілу даних навчальної вибірки відмінного від нормального шляхом застосування степеневих перетворень до ознак навчальної вибірки для стабілізації дисперсії випадкових величин.

Аналіз останніх досліджень і публікацій

Развитие теории и методов машинного обучения при работе с негауссовскими процессами характеризуется несколькими научными школами и направлениями, в частности применением марковских процессов и использованием полигауссовских моделей [4, 5].

Были разработаны общие подходы статистических методов обработки данных, нашедшие отражение в работах [6–9]. Ці наукові напрямки отримали свій розвиток, що відображено в безлічі публікацій і послужило основою для створення методів побудови моделей об'єктів у випадку розподілу даних навчальної вибірки відмінного від нормального і самих технічних систем їх реалізації. Незважаючи на те, що зазначені напрями принципово відрізняються один від одного, їх об'єднує те, що в їх основі лежить імовірнісний підхід до опису випадкових процесів, що ґрунтується на використанні щільності ймовірності розподілу для опису випадкових величин. Однак такі підходи характеризуються рядом проблем, пов'язаних з необхідністю оперування самими щільностями ймовірностей розподілу, що не завжди є можливим, а також складністю практичної реалізації.

Іншим напрямком процесу побудови моделей машинного навчання у випадку розподілу даних навчальної вибірки відмінного від нормального є вибір ознак навчальної вибірки і визначення способу їх виділення (вимірювання) [10–13]. Згідно цьому підходу після накопичення статистичних даних необхідно розглянути можливість виключення частини ознак, задовольняючи при цьому існуючим вимогам до точності моделювання.

Рішення задачі вибору сукупності ознак може бути досягнуто двома шляхами.

Перший з них заснований на зважуванні тим або іншим способом різних систем ознак з метою оцінки їх інформативності при моделюванні, наприклад, за результатами рішення задачі класифікації об'єктів екзаменаційної вибірки за допомогою побудованого одним з алгоритмів навчання вирішального правила [14, 15]. Набори ознак, для яких критерій оцінки точності малий, відкидаються, і в якості системи ознак обирається набір, для якого додавання будь-якої нової ознаки не збільшує або збільшує небагато його інформативність. Якщо параметри статистично незалежні, то систему ознак можна сформувати шляхом оцінки інформативності кожного параметра і відкидання деякої кількості найменш інформативних з них. При такій процедурі формування простору ознак значення самих ознак не змінюються, а тільки зменшується їх кількість.

Для вирішення різноманітних завдань математичної статистики отримав свій подальший розвиток інший підхід, де в якості апіорного опису випадкових величин використовується не щільність ймовірності розподілу випадкових величин, а деякий перетворення вихідних даних з метою отримання щільності розподілу випадкової

величини, близької до нормальної, що дозволяє істотно спростити рішення конкретних практичних завдань при досягненні високої ефективності обробки.

Цей шлях вирішення задачі скорочення інформації при моделюванні об'єкту полягає в знаходженні оптимального, в деякому сенсі, перетворення A вихідного простору векторів вимірювань x розмірністю n в простір зображень меншої розмірності Y (розмірністю $m < n$) [16, 17]. В якості такого перетворення може використовуватися вейвлет-перетворення і розкладання Карунена-Лоєва [18]. Однак на відміну від описаного вище методу вибору діагностичних ознак цей метод не передбачає скорочення кількості вимірювань. В цьому випадку нові ознаки виявляються відірваними від конкретного фізичного змісту і мають тільки абстрактне інформаційне значення.

Ця актуальна та перспективна задача може бути вирішена за рахунок побудови моделей істотно меншої розмірності, що забезпечує зниження вимог до вимірювань і зберігання даних, зменшення обчислювального навантаження при комп'ютерній реалізації моделей машинного навчання, підвищення оперативності моделювання при збереженні високої його точності.

Незважаючи на великий інтерес до цього напрямку і достатня кількість публікацій, до сьогоднішнього дня не в повній мірі не вирішеною залишається завдання проведення систематизованих досліджень ефективності подібних перетворень на випадки найбільш поширених розподілів випадкових величин. Вирішенню цього завдання присвячена дана робота.

Дана робота присвячена вирішенню цього завдання, а саме: дослідженню методів стабілізації дисперсії Випадкове величин на основі степеневих Перетворення для моделей машинного навчання.

Основна частина

Ефективність застосування методів машинного навчання для розв'язання задач регресії, класифікації, кластеризації тощо у великій мірі залежить від інформативності ознак навчальної вибірки. Якщо обрані ознаки досить повно характеризують внутрішню структуру об'єкта контролю, то ідентичні за структурою об'єкти з'являються в просторі цих ознак у вигляді щільної множини точок. Об'єктам з особливостями структури – дефектним – будуть відповідати точки, що відхиляються від цієї щільної безлічі.

Вибір сукупності ознак навчальної вибірки робить вирішальний вплив на точність моделі машинного навчання. Визначення точності моделі машинного навчання передбачає використання конкретної моделі, оскільки тільки в її рамках має сенс точність моделювання.

Алгоритм машинного навчання

Як показав огляд, для задач моделювання об'єктів навколишнього світу більшість традиційних методів побудови моделей машинного навчання, що базуються на припущенні про нормальний закон розподілення даних в навчальній вибірці, є мало ефективні внаслідок наявності у вибірці негаусівських розподілів випадкових величин [19, 20].

В даній роботі використано метод статистичної класифікації на основі баєсова підходу (максимальної правдоподібності) для побудови діагностичних моделей у вигляді поліномів другого порядку.

Діагностичні моделі $d(x)$ на основі методу максимальної правдоподібності будуються за виразом (1). Запис діагностичні моделі у векторній формі має вигляд:

$$d(x) = -\frac{1}{2}(x-m_1)^T S_1^{-1}(x-m_1) + \frac{1}{2}(x-m_2)^T S_2^{-1}(x-m_2) + \frac{1}{2} \ln \frac{|S_2|}{|S_1|} \quad (1)$$

де S_i – коваріаційна матриця розмірності $n \times n$ вимірюваних параметрів стану для i -го класу; $|S_i|$ – визначник матриці S_i ; S_i^{-1} – матриця, зворотна матриці S_i .

У випадку незалежних p ознак $S_i = \sigma_i E_0$, де E_0 – одинична матриця розміру $p \times p$, σ_i – дисперсія ознак у i -му класі навчальної вибірки, вираз (2) для діагностичних моделей спрощується:

$$d(x) = -\frac{1}{2}(x-m_1)^T (x-m_1) / \sigma_1^2 + \frac{1}{2}(x-m_2)^T (x-m_2) / \sigma_2^2 + \frac{1}{2} \ln \frac{|S_2|}{|S_1|} \quad (2)$$

Така модель дає оптимальний за кількістю помилок результат у випадку нормального розподілу даних навчальної вибірки та добре працює при дотриманні вимог симетричного і унімодального розподілу даних, що не завжди забезпечується реальним світом. Для усунення зазначеного недоліку можна використовувати два шляхи: адаптація метода побудови моделі на випадок негаусівського розподілу ознак навчальної вибірки або адаптація навчальної вибірки під вимоги алгоритма.

Критерій точності моделювання

В якості критерія точності моделювання об'єкту використовуються експериментальні оцінки: помилки класифікації та ймовірності правильного розпізнавання.

Помилки класифікації визначаються за виразом:

$$\Delta_{ij} = \frac{L_{ij}}{N_i}, \quad (3)$$

де L_{ij} – кількість об'єктів i -го класу в екзаменаційній вибірці, помилково віднесених до іншого класу $j (j \neq i)$; N_i – кількість елементів i -го класу в екзаменаційній вибірці $i=1, 2, \dots, M$; M – кількість класів станів ОД.

Ймовірність правильного розпізнавання P , середня по всіх класах:

$$P = 1 - \frac{\sum_{i=1}^M \sum_{j \neq i} L_{ij}}{\sum_{i=1}^M N_i} \quad (4)$$

На практиці частіше використовують перетворення випадкової величини, які наближають її функції щільності розподілу до нормального закону (процес нормалізації випадкової величини). Використання такого підходу може забезпечити високу точність машинного моделювання, навіть, при використанні математичного апарату та інструментальних средств комп'ютерного моделювання, що розраховано на випадки гаусівських моделей випадкових величин. Це важливо, так як алгоритми машинного навчання працюють значно краще з нормалізованими даними.

Постановка експерименту

Для підвищення якості моделювання в задачі класифікації в разі розподілу ознак в навчальній вибірці відмінного від нормального пропонується використання перетворень, спрямованих на усунення зв'язку між дисперсією і математичним очікуванням. Таким чином, дисперсія стає постійною по відношенню до середнього. Таку стабілізацію пропонується здійснювати шляхом застосування степеневих

перетворень випадкової величини $x=(x_1, \dots, x_n)$, зокрема логарифмування зі стабілізацією:

$$x_j^0 = \log_a(x_j + b) \quad (5)$$

де a – основа логарифма; b – стабілізуючий коефіцієнт.

Для дослідження ефективності такого перетворення при використанні різноманітних розподілів ознак навчальної вибірки поставленої виконано тестовий експеримент.

Не зважаючи на те, що існує багато різноманітних законів розподілу випадкових величин, на практиці частіше за інші використовуються наступні випадки: рівномірний, біноміальний та експоненціальний закон (Таблиця 1).

Таблиця 1.

Розповсюджені закони розподілу випадкових величин

№.	Закон розподілу	Формальний опис
1	Рівномірний	$f(x) = \begin{cases} 1/(b-a), & a \leq x \leq b \\ 0, & x \notin [a, b] \end{cases}$
2	Біноміальний	$f(x) = C_n^k p^k (1-p)^{n-k}, k=0, \dots, n$
3	Експоненціальний	$f(x) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$

Навчальна вибірка для експерименту являє собою матрицю розмірністю $m \times 2$ (m – кількість вимірювань). Кожна строка матриці є вектором $x=(x_1, x_2)$, має при різних законах розподілу випадкової величини (рівномірному, біноміальному, експоненціальному) та розділена на 2 класи.

Для кожного випадку вирішуються задачі побудови моделі (вирішального правила) об'єктів методом статистичної класифікації на основі баєсова підходу:

- на основі початкової навчальної вибірки;
- на основі навчальної вибірки, отриманої шляхом степеневих (5) перетворень її ознак;

Випадок рівномірного розподілу випадкової величини

На рис. 1 та 2 представлено результати розв'язання задачі класифікації для рівномірного закону розподілу даних навчальної вибірки. Експериментально збудована функція розподілу ймовірностей для рівномірного закону розподілу ознаки x_1 наведено на рис. 1, а. Скоригована за допомогою степеневих перетворень навчальної вибірки функція розподілу ймовірностей ознаки x_1 наведено на рис. 1, б. На рис. 2 наведено вирішальні правила класифікації для рівномірного закону розподілу ознак (x_1, x_2) : для початкової навчальної вибірки (рис. 2, а) та скоригованої за допомогою степеневих перетворень навчальної вибірки (рис. 2, б).

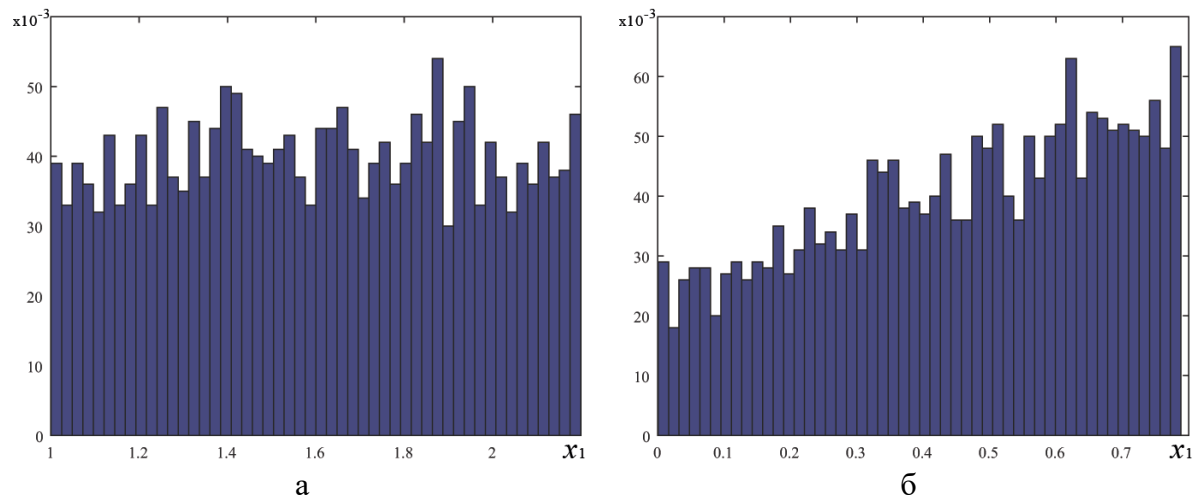


Рис. 1. Функції розподілу ймовірностей ознаки x_1 : а – рівномірний закон розподілу, б – скоригований за допомогою степеневих перетворень навчальної вибірки закон розподілу

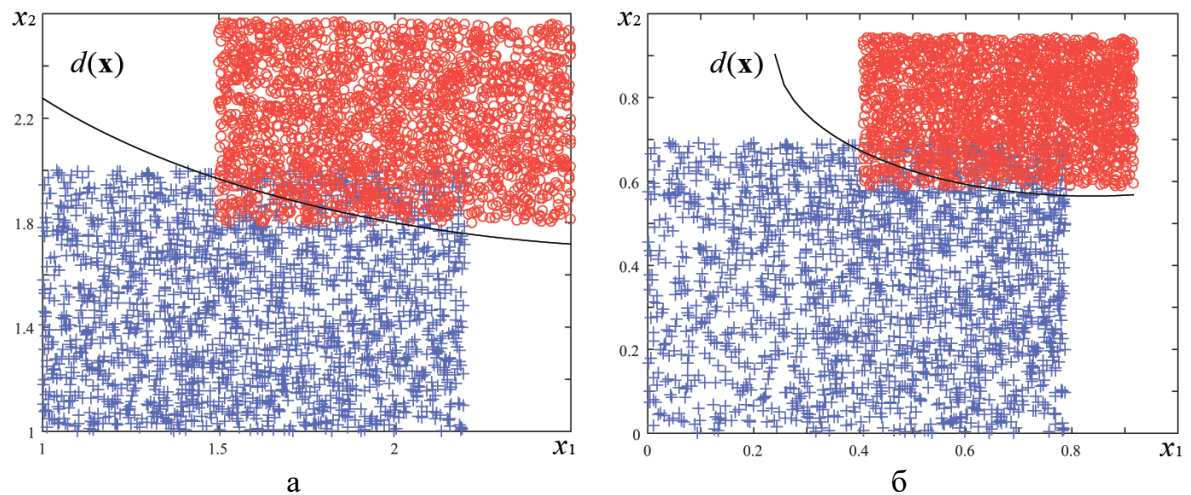


Рис. 2. Вирішальні правила $d(x)$ класифікації в просторі ознак (x_1, x_2) : а – початкова навчальна вибірка з рівномірним законом розподілу, б – скоригований за допомогою степеневих перетворень навчальна вибірка

Випадок біноміального розподілу випадкової величини

На рис. 3 та 4 представлено результати розв'язання задачі класифікації для рівномірного закону розподілу даних навчальної вибірки. Експериментально збудована функція розподілу ймовірностей для рівномірного закону розподілу ознаки x_1 наведено на рис. 3, а. Скоригована за допомогою степеневих перетворень навчальної вибірки функція розподілу ймовірностей ознаки x_1 наведено на рис. 3, б. На рис. 4 наведено вирішальні правила класифікації для рівномірного закону розподілу ознак (x_1, x_2) : для початкової навчальної вибірки (рис. 4, а) та скоригованої за допомогою степеневих перетворень навчальної вибірки (рис. 4, б).

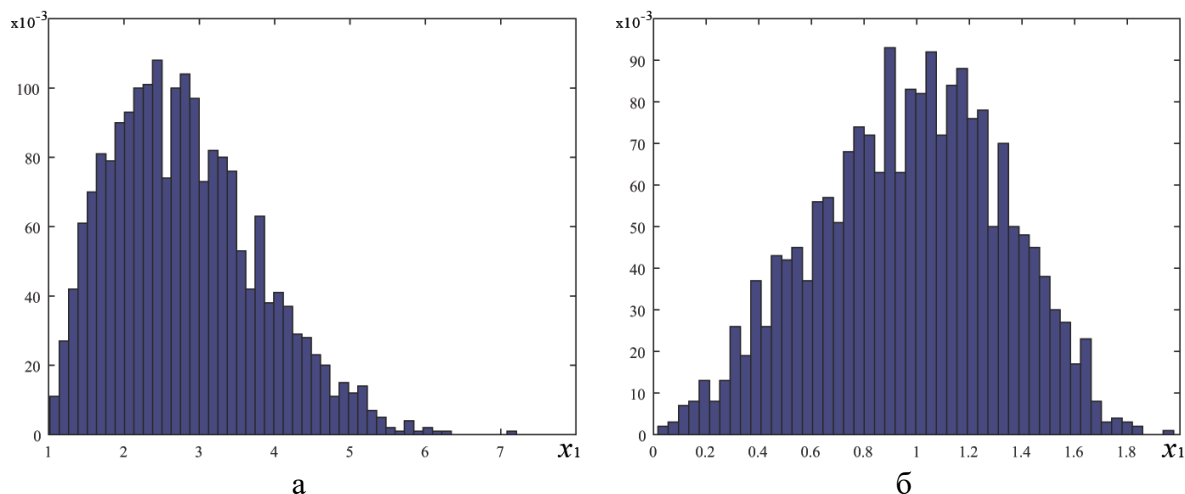


Рис. 3. Функції розподілу ймовірностей ознаки x_1 : а – біноміальний закон розподілу, б – скоригований за допомогою степеневих перетворень навчальної вибірки закон розподілу

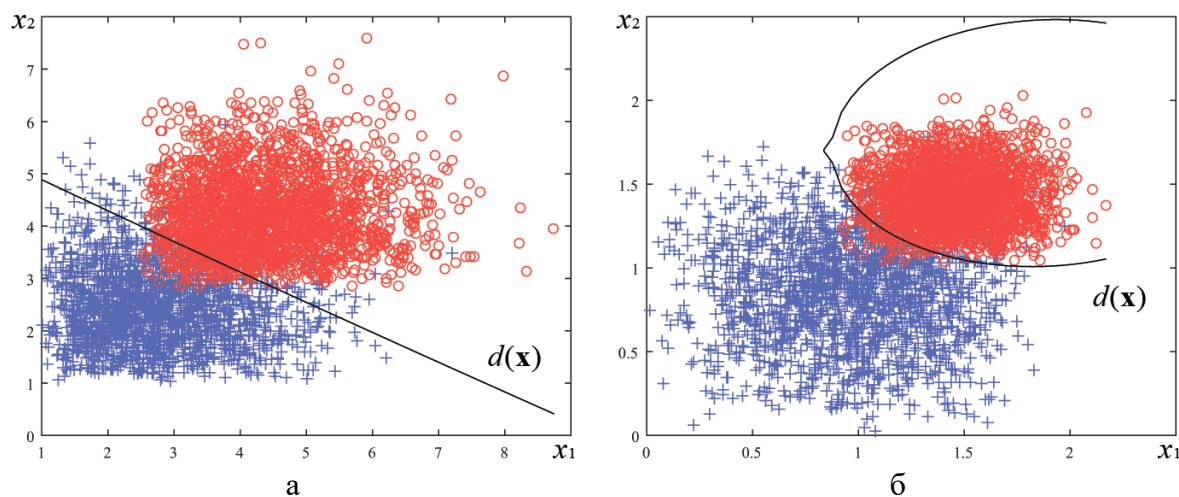


Рис. 4. Вирішальні правила $d(x)$ класифікації в просторі ознак (x_1, x_2) : а – початкова навчальна вибірка з біноміальним законом розподілу, б – скоригований за допомогою степеневих перетворень навчальна вибірка

Випадок експоненціального розподілу випадкової величини

На рис. 5 та 6 представлено результати розв'язання задачі класифікації для рівномірного закону розподілу даних навчальної вибірки. Експериментально збудована функція розподілу ймовірностей для рівномірного закону розподілу ознаки x_1 наведено на рис. 5, а. Скоригована за допомогою степеневих перетворень навчальної вибірки функція розподілу ймовірностей ознаки x_1 наведено на рис. 5, б. На рис. 6 наведено вирішальні правила класифікації для рівномірного закону розподілу ознак (x_1, x_2) : для початкової навчальної вибірки (рис. 6, а) та скоригованої за допомогою степеневих перетворень навчальної вибірки (рис. 6, б).

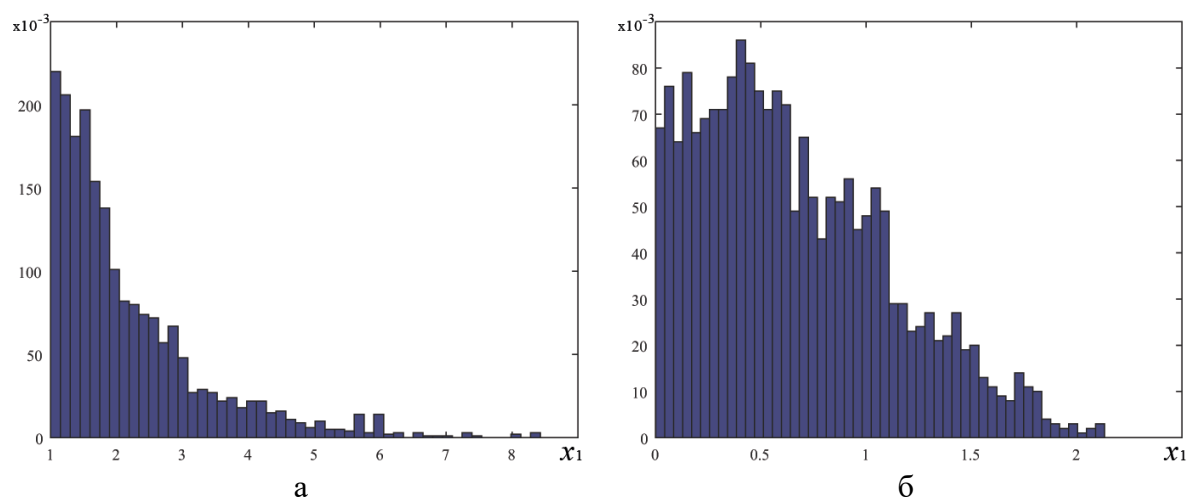


Рис. 5. Функції розподілу ймовірностей ознаки x_1 : а – експоненціальний закон розподілу, б – скоригований за допомогою степеневих перетворень навчальної вибірки закон розподілу.

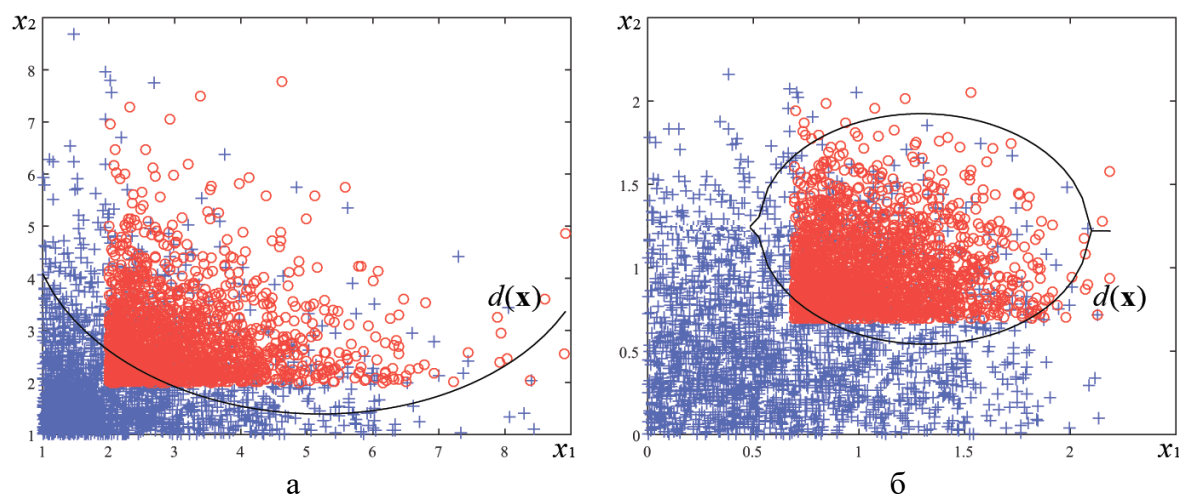


Рис. 6. Вирішальні правила $d(x)$ класифікації в просторі ознак (x_1, x_2) : а – початкова навчальна вибірка з експоненціальним законом розподілу, б – скоригований за допомогою степеневих перетворень навчальна вибірка.

Отримані результати оцінки якості моделювання з використанням степеневих перетворень для нормалізації законів розподілу ознак навчальної вибірки, а саме, помилки класифікації Δ_{ij} (3) та ймовірності правильного розпізнавання P (4) зведені в Таблицю 2.

Таблиця 2.

Результати оцінки якості моделювання з використанням степеневих перетворень для нормалізації законів розподілу ознак навчальної вибірки

№	Закон розподілу	Якість моделювання						Відносна помилка $\delta(P)$
		Без корегування			З корегуванням			
		Δ_1	Δ_2	P	Δ_1	Δ_2	P	
1	Рівномірний	0.079	0.060	0.86	0.061	0.060	0.88	2.02
2	Біноміальний	0.093	0.038	0.87	0.034	0.036	0.93	5.85
3	Експоненціальний	0.129	0.051	0.82	0.095	0.34	0.86	4.11

Аналіз даних Таблиці 2 демонструє переваги степеневих перетворень для біноміального та експоненціального законів розподілу даних навчальної вибірки. Для

рівномірного закону розподілу даних навчальної вибірки ефективність степеневих перетворень не є досить переконливою: перевага методу проявляється на рівні статистичної помилки. Тому, в якості рекомендації, можна стверджувати, що степеневі перетворення ознак навчальної вибірки доцільно використовувати при законах розподілу ознак біноміальному (та таких, що походять від нього: Пуассона, логнормального, хі-квадратного) та експоненціальному (та таких, що походять від нього: геометричного, Вейбула).

Висновки

В роботі успішно вирішена задача підвищення точності моделей машинного навчання для випадку розподілу даних навчальної вибірки відмінного від нормального шляхом застосування статистичних перетворень до ознак навчальної вибірки для стабілізації дисперсії випадкових величин.

Досліджено ефективність методу статистичної класифікації на основі баєсова підходу для побудови діагностичних моделей у вигляді поліномів другого порядку шляхом застосування степеневих перетворень ознак навчальної вибірки для стабілізації їх дисперсії та подальшого використання методу максимальної правдоподібності, що дозволяє підвищити достовірність діагностування у випадку розподілу даних навчальної вибірки відмінного від нормального.

Розглянутий метод стабілізації дисперсії випадкових величин на основі степеневих перетворень апробовано на тестових даних. На основі проведених експериментальних досліджень отримано результати ефективності застосування степеневих перетворень даних навчальної вибірки при різноманітних розподілах її ознак. Сформульовано рекомендації по застосуванню степенного перетворення для розглянутих законів розподілення ознак навчальної вибірки: степеневі перетворення доцільно використовувати при законах розподілу ознак біноміальному (та таких, що походять від нього: Пуассона, логнормального, хі-квадратного) та експоненціальному (та таких, що походять від нього: геометричного, Вейбула).

Застосування запропонованих рекомендацій дозволяє забезпечити підвищення достовірності моделей машинного навчання в умовах розподілу даних навчальної вибірки відмінного від нормального.

Список літератури

1. Yan H., Wan J., Zhang C., Tang S., Hua Q., Wang Z. Industrial big data analytics for prediction of remaining useful life based on deep learning. *IEEE Access*. 2018. Vol. 6. P.17190–17197.
2. Zhao R., Yan R., Chen Z., Mao K., Wang P., Gao R. X. Deep learning and its applications to machine health monitoring. *Mechanical Systems and Signal Processing*. 2019. Vol. 115. P. 213–237.
3. Шелухин О.И., Беляков И.В. Негауссовские процессы. СПб: Политехника, 1992. 312 с.
4. Кунченко Ю.П., Палагин В.В. Синтез алгоритмов проверки простых статистических гипотез, основанных на использовании стохастических полиномов, оптимальных по критерию асимптотической нормальности. Труды 51-й научной сессии, посвященной дню радио. Москва, 1996. Т.2, С.128-129.

5. ЧабдаровШ.М., СафиуллинН.З., ФеоктистовА.Ю. Основы статистической теории радиосвязи: Полигауссовы модели и методы. Казань: КАИ, 1983. 87 с.
6. Guyon I., Elisseeff A. An introduction to variable and feature selection. *Journal of Machine Learning Research*. 2003. No 3. P. 1157–1182.
7. Gantz J., E. Reinsel. Extracting Value from Chaos.*IDC's Digital Universe Study*, 2011. 12 p.
8. Кунченко Ю.П., Палагін В.В. Розробка теорії нелінійних методів опрацювання негауссівських сигналів на основі застосування стохастичних поліномів. *Труды IX Международной научно-практической конференции «Системы и средства передачи и обработки информации» (ССПОИ-2005)*. Черкассы: ЧГТУ, 2005. С. 9-11.
9. Fainzilberg L.S. Mathematical methods for evaluating the usefulness of diagnostic features. Kiev: Osvita Ukrainy, 2010. 152 p. [in Russian].
10. Tang, J., Alelyani, S., Liu, H. Feature selection for classification: A review. *Data Classification: Algorithms and Applications*. CRC Press, 2014. P. 37–64.
11. Shahana A.H., Preeja V. Survey on feature subset selection for high dimensional data. *International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, India, 2016. P. 1–4.
12. Jain D., Singh V. Feature selection and classification systems for chronic disease prediction: A review. *Egyptian Informatics Journal*. 2018. Vol. 19, Issue 3. P. 179–189.
13. Liu H., Hiroshi M. Feature Selection for Knowledge Discovery and Data Mining. *The Springer International Series in Engineering and Computer Science*. 1998. 214 p.
14. Kohavi R., John G. Wrappers for feature selection. *Artificial Intelligence*. 1997. Vol. 97, Issues 1–2. P. 273–324.
15. Gopika N., Meena kowshalaya M.E. Correlation Based Feature Selection Algorithm for Machine Learning Proceedings. *International Conference on Communication and Electronics Systems (ICCES)*, 2018. P. 692–695.
16. Medvedew A., Fomin, O., Pavlenko, V., Speransky, V. Diagnostic features space construction using Volterra kernels wavelet transforms. *Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017. P. 1077–1081.
17. Derevianchenko O., Fomin O., Skrypnyk N. Improvement of the Quality for Cutting Tool Monitoring by Optimizing the Features of the State Space. In: Tonkonogyi V. et al. (eds) *Advanced Manufacturing Processes II. Lecture Notes in Mechanical Engineering*. Springer, InterPartner, 2020.
18. Dumas S. Karhunen-Loeve transform and digital signal processing – part 1. SETI League, 2016. 39 p.
19. Вагис Г.А., Гупал А.М., Сергиенко И.В. Эффективность байесовской процедуры распознавания. *Кибернетика и системный анализ*. 2001. №1. С. 71-77.
20. Bernard C. Picinbono. Measurements of Second-Order Properties of Point Processes. *IEEE Trans. Instrumentation and Measurement*. Vol. 57, №3, 2008. P. 548-555.

**ANALYSIS OF A METHOD FOR STABILIZING THE VARIANCE OF
RANDOM VARIABLES BASED ON POWER TRANSFORMATIONS
FOR MACHINE LEARNING MODELS**

O.O. Fomin¹, M.M. Masri², O.A. Tumanov², O.V. Serbova², V.V. Tkachenko²

¹Odesa national polytechnic university,

Shevchenko ave., 1, Odesa, 65044; Ukraine; fomin@opu.ua

²Private Higher Educational Institution «Odesa Technological University «STEP»»,
вул. Садова, 3, Одеса, 65023; Україна; dr.mohanadmasri@gmail.com

In the work the task of creating machine learning models is solved. The aim of the work is to increase the accuracy of machine learning models for the case of a distribution of data of the educational selection other than normal. This goal is achieved by using statistical rearrangements to the features of the educational selection for stabilization of dispersion of incidental values. The most significant results: The efficacy of the method of statistical classification on the basis of the basis of the basic approach for creating models in the form of polynomials of another order, which allows increasing the accuracy of modeling in the case of distribution of data of the educational sample different from the normal one, was investigated, Experimental studies and recommendations on the efficiency of using statistical transformations of the educational selection data at different distributions of the educational selection data for the following laws of distribution of incidental values were made: Equinomial, Binomial, Exponential. Significance of the results: the application of the formulated recommendations allows us to improve the accuracy of machine learning models under conditions of a distribution of educational selection data different from the normal. The provided recommendations were tested on the test assignment data. The task demonstrates an increase in the accuracy of machine learning models for most of the considered laws of distribution of incidental quantities.

Keywords: statistical characteristics, random variable, power transformations, models of machine learning.

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ЗА ДАНИМИ АЙТРЕКІНГУ**Т.В. Шаманіна, В.Д. Павленко**

Державний університет «Одеська політехніка»,
пр. Шевченка, 1, Одеса, 65044, Україна; e-mail: tatanatv8@gmail.com
pavlenko_vitalij@ukr.net

Управління та розмежування доступу до комп'ютерних систем і до їх ресурсів є одним з важливих аспектів інформаційної безпеки, що може бути реалізовано за рахунок ідентифікації користувачів. Останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до інформаційних систем. В роботі пропонується новий метод біометричної ідентифікації користувачів комп'ютерних систем на основі визначення інтегральних моделей Вольтерри окуло-моторної системи (ОМС) людини за даними експериментальних досліджень «вхід-вихід» із застосуванням інноваційної технології айтрекінга. *Метою* роботи є підвищення ефективності (надійності) захисту інформації в комп'ютерних системах за рахунок розробки апаратно-програмних засобів ідентифікації ОМС людини на основі нелінійної динамічної моделі та експериментальних даних айтрекінгу з використанням тестових візуальних стимулів. *Об'єкт дослідження* – процес біометричної ідентифікації користувача комп'ютерної системи на основі даних відстеження руху очей в динаміці – відгуків на задані тестові візуальні стимули (процес айтрекінгу). *Предмет дослідження* – інструментальні алгоритмічні та програмні засоби побудови моделі Вольтерри – оцінки багатовимірних перехідних функцій ОМС за даними айтрекінгу. Розроблено в середовищі програмування PythonIDLE програмні засоби ідентифікації ОМС. Використовуються тестові візуальні стимули у вигляді яскравих точок, які послідовно відображаються на екрані дисплея на різних відстанях від стартової позиції, що формально відповідає різним амплітудам тестових ступінчатих сигналів. Здійснено експериментальні дослідження ОМС у двох індивідів. На основі даних, отриманих за допомогою айтрекера TOBII PROTX300, визначено перехідні функції першого, другого та третього порядків ОМС. Виявлено значну відмінність у двох індивідів діагональних перетинів перехідних функцій другого та третього порядків. Таким чином, їх можна використовувати для формування простору інформативних ознак і побудови за допомогою засобів машинного навчання статистичних класифікаторів особистостей, що реалізують запропонований метод захисту інформації в комп'ютерних системах на основі біометричної ідентифікації користувачів за даними айтрекінга. Запропонований метод біометричної ідентифікації і розглянуті засоби впровадження механізмів захисту в комп'ютерних інформаційних системах мають можливість гнучкого управління безпекою в залежності від висунутих вимог, допустимого ризику та оптимальних витрат ресурсів.

Ключові слова: захист комп'ютерної інформації, біометрична ідентифікація, окуло-моторна система людини, модель Вольтерри, багатовимірні перехідні функції, тестові візуальні стимули, айтрекінг.

Вступ

Управління та розмежування доступу до комп'ютерних систем і до їх ресурсів є одним з важливих аспектів інформаційної безпеки, що може бути реалізовано за рахунок ідентифікації користувачів. Про це свідчить значне збільшення досліджень та публікацій, які присвячені цій проблемі [1-6]. Але значна більшість наукових статей

присвячується докладному розгляданню лише одного з можливих способів ідентифікації користувачів – паролній ідентифікації [7-10].

Останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до інформаційних систем [6]. На практиці використовуються такі біометричні методи: розпізнавання за відбитком пальця, за зображенням людини, по райдужній оболонці, по сітківці ока. Біометричні технології високонадійні і зручні. Але найчастіше розглядаються лише окремі біометричні ознаки, що використовуються для визначення особи користувача. Відбиток пальця, райдужна оболонка ока – всього цього може виявитися недостатньо для надійного захисту. Тому запропоновано біометричну технологію яка ідентифікує людину за індивідуальними рухами ока[11-13].

При відстеженні рухів ока пропонується знімати дві характеристики ока. Перша - фіксація ока на певній точці дисплея. Друга – момент руху ока при переміщенні погляду з однієї точки на іншу. Комп'ютер оцінює отримані дані, і визначає унікальні характеристики для кожного випадку, тобто для кожної людини, включаючи роботу м'язів очного яблука. Система ідентифікації на основі оцінки руху очного яблука має великий відсоток помилок, але об'єднаний комплекс з недорогим сканером райдужки працює вже набагато більш точно, з 5% -ою вірогідністю появи помилки [14, 15].

Таким чином, можна стверджувати, що надійність та стійкість існуючих систем біометричного захисту доступу до ресурсів інформаційних систем недостатня для сьогоденних потреб. Наразі системи безпеки стають все більш складними, і біометричні системи безпеки, що засновані на біометричній ідентифікації, повинні постійно еволюціонувати та ставатимуть більш надійними [16, 17].

В даній роботі пропонується новий метод біометричної ідентифікації користувачів комп'ютерних систем на основі визначення інтегральних моделей Вольтерри окуло-моторної системи (ОМС) людини за даними експериментальних досліджень «вхід-вихід» із застосуванням інноваційної технології айтрекінга [18]. Отримані при цьому багатовимірні перехідні функції (БПФ) використовуються для побудови системи біометричної ідентифікації фізичних осіб [19].

Метою роботи є підвищення ефективності (надійності) захисту інформації в комп'ютерних системах за рахунок розробки апаратно-програмних засобів ідентифікації окуло-моторної системи людини на основі нелінійної динамічної моделі та даних айтрекінгу.

Об'єкт дослідження – процес біометричної ідентифікації користувача комп'ютерної системи на основі даних відстеження руху очей в динаміці – відгуків на задані тестові візуальні стимули (процес айтрекінгу).

Предмет дослідження – інструментальні алгоритмічні та програмні засоби побудови моделі Вольтерри – оцінки багатовимірних перехідних функцій ОМС за даними айтрекінгу.

Модель Вольтерри

Для опису об'єктів невідомої структури (типу «чорний ящик») доцільно використовувати найбільш універсальні нелінійні непараметричні динамічні моделі – моделі Вольтерри [20, 21]. При цьому нелінійні і динамічні властивості досліджуваного об'єкта однозначно описуються послідовністю інваріантних щодо виду вхідного сигналу багатовимірних вагових функцій.

Для неперервної нелінійної динамічної системи (НДС) зв'язок між вхідним (стимулом) $x(t)$ і вихідним (відгуком) $y(t)$ сигналами при нульових початкових умовах може бути представлена рядом Вольтерри у вигляді

$$y(t) = \sum_{n=1}^{\infty} y_n(t) = \int_0^t w_1(\tau) x(t-\tau) d\tau + \int_0^t \int_0^t w_2(\tau_1, \tau_2) x(t-\tau_1) x(t-\tau_2) d\tau_1 d\tau_2 + \int_0^t \int_0^t \int_0^t w_3(\tau_1, \tau_2, \tau_3) x(t-\tau_1) x(t-\tau_2) x(t-\tau_3) d\tau_1 d\tau_2 d\tau_3 + \dots \quad (1)$$

де

$$y_n[x(t)] = \int_0^t \dots \int_0^t w_n(\tau_1, \dots, \tau_n) \prod_{i=1}^n x(t-\tau_i) d\tau_i, \quad (2)$$

$y_n(t)$ – n -на парціальна складова (ПС) відгуку НДС (n -вимірний інтеграл згортки); $w_n(\tau_1, \dots, \tau_n)$ – вагова функція (ядро Вольтерри) n -го порядку – симетрична функція щодо дійсних змінних $\tau_1, \dots, \tau_n$; t – поточний час.

На практиці як правило обмежуються кількома першими членами ряду (1). Ряд замінюється поліномом Вольтерри ступеня N . В даному дослідженні обмежилися першими трьома членами ряду (вибрали ступінь поліноміальної моделі Вольтерри $N=3$). Структурна схема моделі Вольтерри наведена на рис. 1.

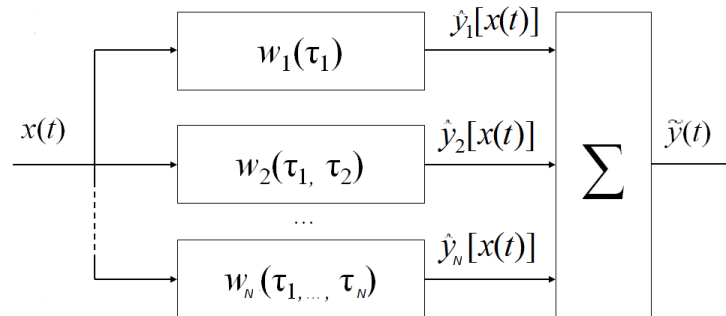


Рис. 1. Структурна схема моделі Вольтерри.

Побудова моделі Вольтерри ОМС на основі даних експериментів «вхід-вихід»

Задача ідентифікації (побудови моделі) у вигляді ряду (1) полягає у визначенні ядер Вольтерри на основі експериментальних даних «вхід-вихід» ОМС. Побудова моделі – це вибір тестових сигналів $x(t)$ і розробка алгоритму, який дозволяє по вимірюваному відгуку $y(t)$ визначати парціальні компоненти $y_n(t)$, що знаходяться на основі ядер Вольтерри $w_n(\tau_1, \dots, \tau_n)$. При цьому обмежуємось значеннями $n=1, 2, 3$ ($N=3$) [19].

З урахуванням специфіки досліджуваного об'єкта ОМС для ідентифікації використовуються тестові багатоступінчасті сигнали [21]. Якщо тестовий сигнал $x(t)$ являє собою одиничну функцію (функцію Гевісайда) – $\theta(t)$, то результатом ідентифікації є ПС $\hat{y}_n(t)$, причому при $n=1$: $\hat{y}_1(t) = \hat{h}_1(t)$ – оцінка перехідної функції першого порядку $h_1(t)$, а при $2 \leq n \leq N$: $\hat{y}_n(t) = \hat{h}_n(t, \dots, t)$ – оцінки діагональних перетинів перехідних функцій n -го порядку $h_n(t_1, \dots, t_n)$, які представляють собою n -вимірні інтеграли від ядер n -го порядку $w_n(\tau_1, \dots, \tau_n)$:

$$h_n(t, \dots, t) = \int_0^\infty \dots \int_0^\infty w_n(t - \tau_1, \dots, t - \tau_n) d\tau_1 \dots d\tau_n. \quad (3)$$

Для $n=1, 2, 3$, відповідно, маємо

$$\begin{aligned} h_1(t) &= \int_0^\infty w_1(t - \tau) d\tau. \\ h_2(t, t) &= \int_0^\infty \int_0^\infty w_2(t - \tau_1, t - \tau_2) d\tau_1 d\tau_2. \\ h_2(t, t, t) &= \int_0^\infty \int_0^\infty \int_0^\infty w_3(t - \tau_1, t - \tau_2, t - \tau_3) d\tau_1 d\tau_2 d\tau_3. \end{aligned} \quad (4)$$

Відгуки поліноміальної моделі Вольтерри ОМС ступеня N на вхідну ступінчасту функцію амплітудою a обчислюються за формулою:

$$\tilde{y}(t) = a\hat{y}_1(t) + a^2\hat{y}_2(t) + a^3\hat{y}_3(t), \quad i = \overline{1, N}, \quad (5)$$

де $\hat{y}_1(t) = \hat{h}_1(t)$, $\hat{y}_2(t) = \hat{h}_2(t, t)$, $\hat{y}_3(t) = \hat{h}_3(t, t, t)$ – отримані оцінки ПС 1-го, 2-го та 3-го порядку відгуку моделі ОМС.

В даному дослідженні використовується апроксимаційний метод ідентифікації [21]. Апроксимаційний метод ідентифікації НДС у часовій області ґрунтується на виділенні з відгуку НДС n -ої ПС за допомогою побудови лінійних комбінацій відгуків на тестові сигнали з різними амплітудами [21].

Справедливе наступне твердження, доведення якого дається в [22].

Нехай на вхід системи по черзі подаються тестові сигнали $a_1x(t)$, $a_2x(t), \dots, a_Nx(t)$ (N – порядок апроксимаційної моделі; $a_1, a_2, \dots, a_N$ – різні дійсні числа, які задовольняють умові $|a_i| \leq 1$ для $\forall i=1, 2, \dots, N$; $x(t)$ – довільна функція), тоді лінійна комбінація відгуків НДС на ці впливи дорівнює n -ої ПС відгуку на вхідний сигнал $x(t)$. При цьому виникає методична похибка через ПС відгуку ОМС вищих порядків $n > N$:

$$\sum_{i=1}^N c_i y[a_i x(t)] = y_n[x(t)] + \sum_{i=1}^N c_i \sum_{n=N+1}^{\infty} y_n[a_i x(t)], \quad (6)$$

де

$$\begin{aligned} y_n[x(t)] &= y_n(t); \\ y[a_i x(t)] &= \sum_{n=1}^{\infty} a_i^n \int_0^t \dots \int_0^t w_n(\tau_1, \dots, \tau_n) \prod_{i=1}^n x(t - \tau_i) d\tau_1 \dots d\tau_n. \end{aligned}$$

Якщо c_j – дійсні коефіцієнти, такі що

$$A_N c = b, \quad (7)$$

Де

$$A_N = \begin{bmatrix} a_1 & a_2 & \dots & a_N \\ a_1^2 & a_2^2 & \dots & a_N^2 \\ \dots & \dots & \dots & \dots \\ a_1^N & a_2^N & \dots & a_N^N \end{bmatrix}, \quad c = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_N \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_N \end{bmatrix},$$

та $b_l = 1$ при $l = n$, $b_l = 0$ при $l \neq n$, $\forall l \in \{1, 2, \dots, N\}$.

В окремих випадках, маємо:

для $N=2$

$$\begin{bmatrix} a_1 & a_2 \\ a_1^2 & a_2^2 \end{bmatrix} \cdot \begin{bmatrix} c_1^{(1)} \\ c_2^{(1)} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} a_1 & a_2 \\ a_1^2 & a_2^2 \end{bmatrix} \cdot \begin{bmatrix} c_1^{(2)} \\ c_2^{(2)} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix};$$

для $N=3$

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^3 & a_2^3 & a_3^3 \end{bmatrix} \cdot \begin{bmatrix} c_1^{(1)} \\ c_2^{(1)} \\ c_3^{(1)} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^3 & a_2^3 & a_3^3 \end{bmatrix} \cdot \begin{bmatrix} c_1^{(2)} \\ c_2^{(2)} \\ c_3^{(2)} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^3 & a_2^3 & a_3^3 \end{bmatrix} \cdot \begin{bmatrix} c_1^{(3)} \\ c_2^{(3)} \\ c_3^{(3)} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Система (7) завжди має розв'язок, причому єдиний, оскільки її детермінант тільки множителем $a_1 a_2 \dots a_N$ відрізняється від детермінанта Вандермонда. Таким чином, при будь-яких дійсних числах a_i , відмінних від нуля і попарно різних, можна знайти числа c_i , за яких лінійна комбінація (6) з відгуків НДС дорівнює n -му члену ряду Вольтерри з точністю до відкинутих членів ряду порядку $N+1$ й вище. При виконанні вказаних умов формування СЛАР (7), отримуємо співвідношення (6).

Оцінки перехідних функцій отримуємо наступним чином:

$$\begin{aligned} \hat{h}_n^{(N)}(t, \dots, t) &= \hat{y}_n(t) = \sum_{i=1}^N c_i^{(n)} y[a_i \theta(t)] = \\ &= c_1^{(n)} y_{a_1}(t) + c_2^{(n)} y_{a_2}(t) + \dots + c_N^{(n)} y_{a_N}(t), \quad n = 1, 2, \dots, N. \end{aligned} \quad (8)$$

де $y_{a_i}(t) = y[a_i \theta(t)]$ – відгук ОМС на тестовий ступінчастий сигнал з амплітудою a_i .

В окремих випадках маємо:

для $N=2$

$$\hat{h}_1^{(2)}(t) = \hat{y}_1(t) = \sum_{i=1}^2 c_i^{(1)} y[a_i \theta(t)] = c_1^{(1)} y_{a_1}(t) + c_2^{(1)} y_{a_2}(t), \quad (9)$$

$$\hat{h}_2^{(2)}(t, t) = \hat{y}_2(t) = \sum_{i=1}^2 c_i^{(2)} y[a_i \theta(t)] = c_1^{(2)} y_{a_1}(t) + c_2^{(2)} y_{a_2}(t), \quad (10)$$

ля $N=3$

$$\hat{h}_1^{(3)}(t) = \hat{y}_1(t) = \sum_{i=1}^3 c_i^{(1)} y[a_i \theta(t)] = c_1^{(1)} y_{a_1}(t) + c_2^{(1)} y_{a_2}(t) + c_3^{(1)} y_{a_3}(t), \quad (11)$$

$$\hat{h}_2^{(3)}(t, t) = \hat{y}_2(t) = \sum_{i=1}^3 c_i^{(2)} y[a_i \theta(t)] = c_1^{(2)} y_{a_1}(t) + c_2^{(2)} y_{a_2}(t) + c_3^{(2)} y_{a_3}(t), \quad (12)$$

$$\hat{h}_1^{(3)}(t, t, t) = \hat{y}_3(t) = \sum_{i=1}^3 c_i^{(3)} y[a_i \theta(t)] = c_1^{(3)} y_{a_1}(t) + c_2^{(3)} y_{a_2}(t) + c_3^{(3)} y_{a_3}(t). \quad (13)$$

Результати досліджень

Питання організації та методика експериментальних досліджень із застосуванням технології айтрекінгу детально описані у [23].

Експерименти було організовано з метою виявити мінливість БПФ для різних індивідів. Дані для побудови моделі – відгуки ОМС на однакові тестові стимулю-ступінчасті сигнали з різними амплітудами a_1 , a_2 і a_3 для кожного з двох індивідів було отримано за допомогою айтрекера ТОВІПРОТХ300 (300 Hz) в Лабораторії аналізу руху та ергономіки інтерфейсів Люблінського технологічного університету (Люблін, Польща) [23].

У дослідженні кожного індивіда реалізовано цикли «Вправо по горизонталі». У кожному циклі послідовно виконуються 3 незалежних експериментів з амплітудами тестових сигналів $a_1=0.33$, $a_2=0.66$, $a_3=1.0$ (у відносних одиницях від ширини екрану монітора). Таким чином, реалізується наступна послідовність вхідних візуальних сигналів, координати яких (у відносних одиницях): експеримент #1: ($x=0$, $y=0.5$) та ($x=0.33$, $y=0.5$); експеримент #2: ($x=0$, $y=0.5$) та ($x=0.66$, $y=0.5$); експеримент #3: ($x=0$, $y=0.5$) та ($x=1.0$, $y=0.5$). Експериментальні дослідження індивідів проводились в різний час і в різні дні.

На рис. 2 представлено схему процесу айтрекінга.

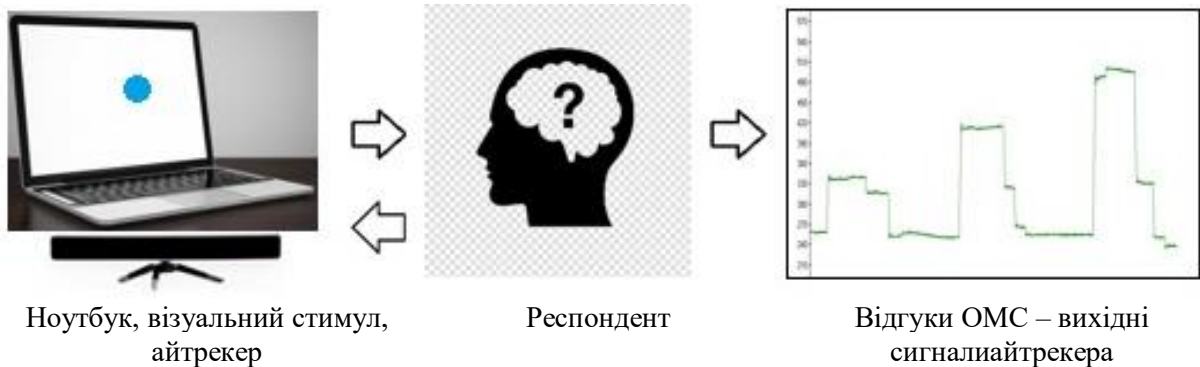


Рис. 2. Схема процесу айтрекінга.

Графіки відгуків ОМС, отриманих при різних амплітудах тестових сигналів для індивіда № 1 та індивіда № 2, наведені на рис. 3 і 4, відповідно.

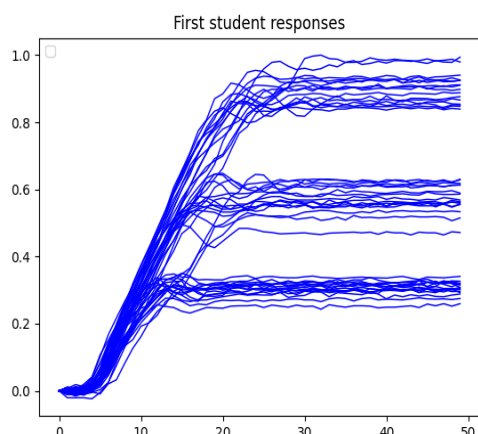


Рис. 3. Відгуки ОМС індивіда #1 на візуальні стимули з амплітудами a_1, a_2, a_3 .

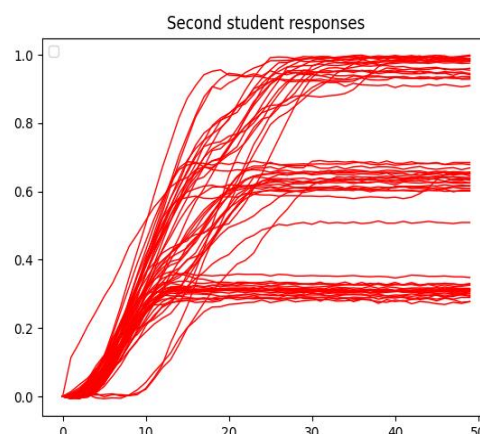


Рис. 4. Відгуки ОМС індивіда #2 на візуальні стимули з амплітудами a_1, a_2, a_3 .

За усередненими даними відгуків ОМС на візуальні стимули з різною відстанню від стартової позиції (формально це відповідає тестовим сигналам різної амплітуди), графіки яких наведено рис. 5, визначено перехідні функції ОМС при використанні апроксимаційних моделей різного ступеня N ($N = 1, 2, 3$). Графіки перехідних функцій для індивіда № 1 та індивіда № 2 при $N=1$ наведено на рис. 6; при $N = 2$ – на рис. 7 і при $N = 3$ – на рис. 8.

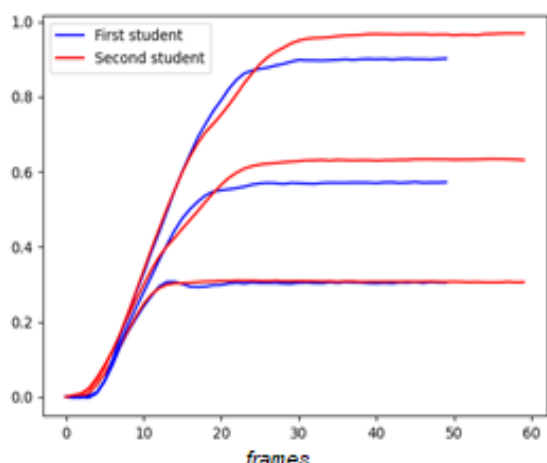


Рис. 5. Усереднені відгуки ОМС двох індивідів.

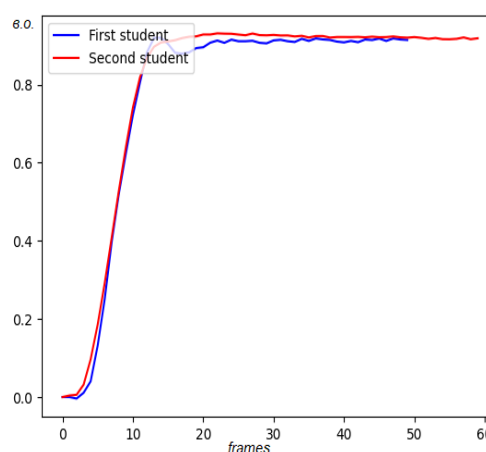


Рис. 6. Перехідні функції 1-го порядку двох індивідів.

Визначено відгуки за допомогою розрахунків на моделях за формулою (5) при різних амплітудах тестових сигналів для індивіда № 1 та індивіда № 2, графіки яких наводяться у порівнянні з подібними відгуками ОМС, на рис. 9, 10 – при $N = 2$ і на рис. 11, 12 – при $N = 3$.

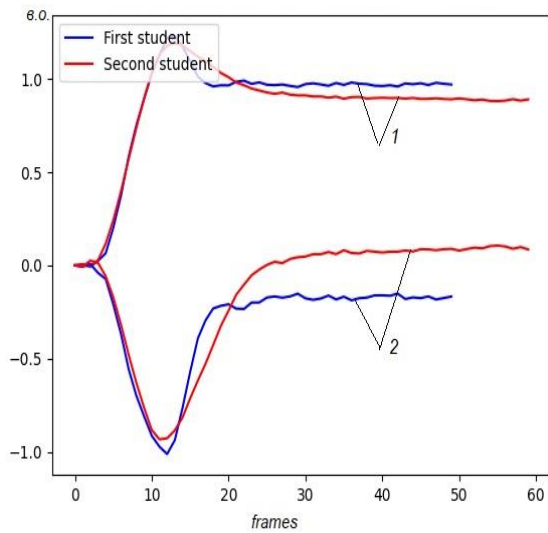


Рис. 7. Перехідні функції при $N=2$: 1 – 1-го; 2 – 2-го порядку двох індивідів.

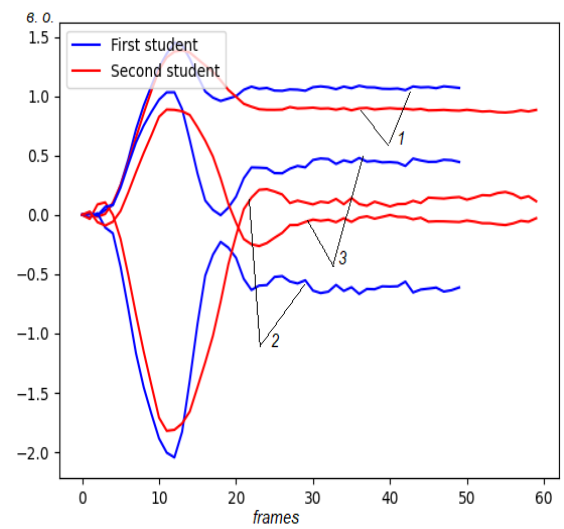


Рис. 8. Перехідні функції при $N=3$: 1 – 1-го; 2 – 2-го; 3 – 3-го порядку двох індивідів.

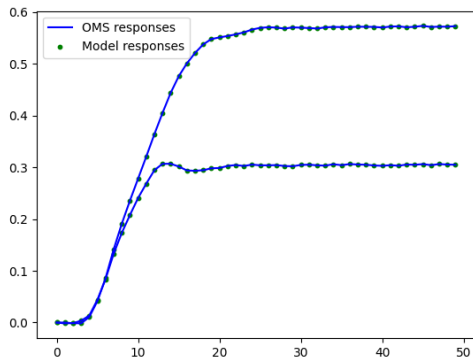


Рис. 9. Відгуки ОМС індивіда № 1 та моделі при $N=2$ на тестові сигнали з амплітудами a_1 , a_2 .

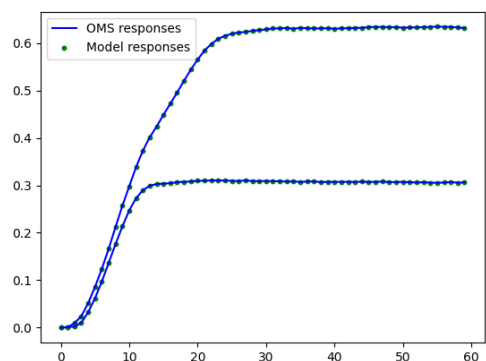


Рис. 10. Відгуки ОМС індивіда № 2 та моделі при $N=2$ на тестові сигнали з амплітудами a_1 , a_2 .

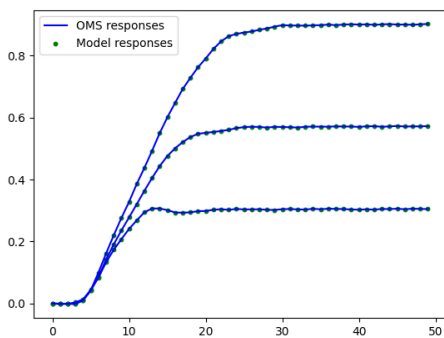


Рис. 11. Відгуки ОМС індивіда № 1 та моделі при $N=3$ на тестові сигнали з амплітудами a_1 , a_2 і a_3 .

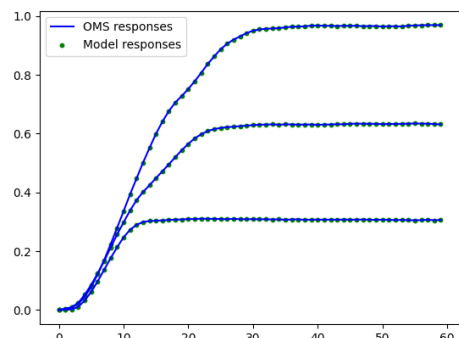


Рис. 12. Відгуки ОМС індивіда № 2 та моделі при $N=3$ на тестові сигнали з амплітудами a_1 , a_2 і a_3 .

Аналіз варіативності перехідних функцій

Аналіз мінливості (варіативності) перехідних функцій ОМС різних порядків, отриманих на основі обробки усереднених даних відгуків для двох

інформантів: індивіда № 1 – $\hat{y}_n^{(1)}(t)$ та індивіда № 2 – $\hat{y}_n^{(2)}(t)$, заснований на розрахунку наступних показників:

$$\sigma_{nN} = \max_{t \in [0, T]} |\hat{y}_n^{(1)}(t) - \hat{y}_n^{(2)}(t)|, \quad (14)$$

$$\varepsilon_{nN} = \left(\frac{1}{T} \int_0^T (\hat{y}_n^{(1)}(t) - \hat{y}_n^{(2)}(t))^2 dt \right)^{1/2}, \quad n = 1, 2, \dots, N. \quad (15)$$

де σ_{nN} , ε_{nN} – максимальне та стандартне відхилення відгуків ОМС, відповідно; T – час спостереження.

Результати розрахунку цих показників наведені в таблиці 1 і представлені діаграмами рис. 13 та 14.

Таблиця 1.

Показники варіативності перехідних функцій

N	ε_1	σ_1	ε_2	σ_2	ε_3	σ_3
1	0,025	0,056	-	-	-	-
2	0,066	0,118	0,489	0,264	-	-
3	0,158	0,22	0,83	0,808	1,182	0,66

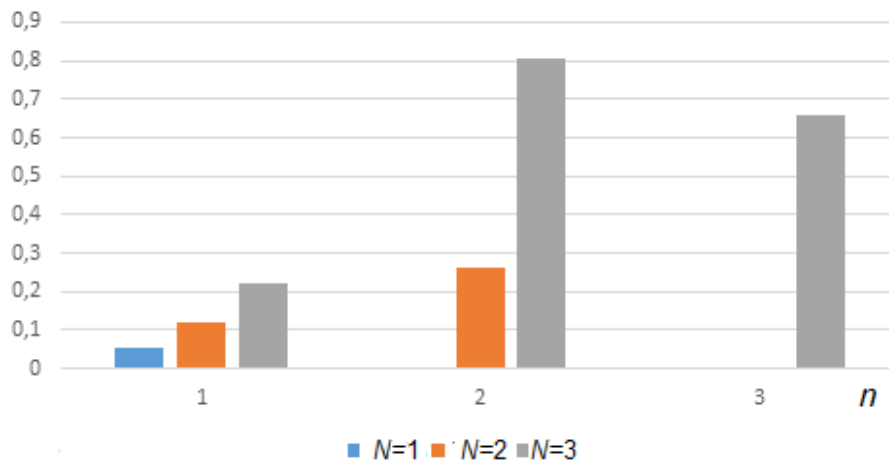


Рис. 13. Діаграма відхилень БПФ для двох індивідів за показником σ_{nN} .

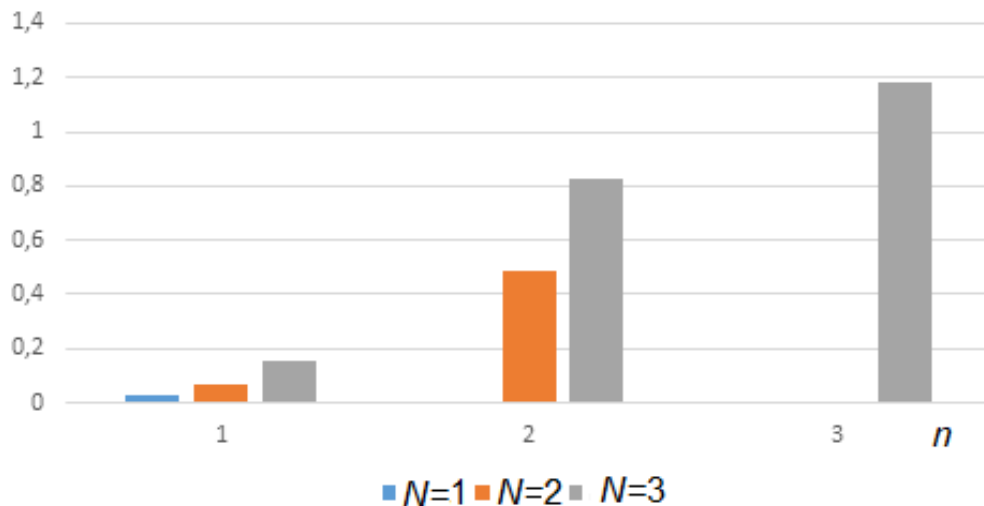


Рис. 14. Діаграма відхилень БПФ для двох індивідів за показником ε_{nN} .

Як можна бачити з рис.6-8, отримані перехідні функції першого порядку для індивідів № 1 та № 2 не суттєво змінюються. Проте, діагональні перетини перехідних функцій другого (рис. 7, 8) та третього (рис. 8) порядків істотно змінюються за величиною, отже, в подальшому можуть ефективно використовуватися, як джерело первинних даних, для побудови апаратно-програмних засобів біометричної ідентифікації користувачів комп'ютерних систем.

Висновки

Запропоновано новий метод біометричної ідентифікації користувачів інформаційних комп'ютерних систем на основі інтегральних динамічних моделей Вольтерри окуло-моторної системи, що визначаються на основі даних айтрекінга. Розроблено методику експериментальних досліджень ОМС «вхід-вихід» із застосуванням тестових візуальних стимулів і технології айтрекінгу та інструментальні програмні засоби побудови нелінійної динамічної моделі ОМС людини на основі отриманих експериментальних даних.

Здійснено експериментальні дослідження ОМС у двох індивідів. На основі даних, отриманих за допомогою айтрекера, визначено перехідні функції першого, другого та третього порядків ОМС. Виявлено значну відмінність у двох індивідів діагональних перетинів перехідних функцій другого та третього порядків. Таким чином, їх можна використовувати для формування простору інформативних ознак і побудови за допомогою засобів машинного навчання статистичних класифікаторів особистостей, що реалізують запропонований метод захисту інформації в комп'ютерних системах на основі біометричної ідентифікації користувачів за даними айтрекінга.

Запропонований метод біометричної ідентифікації і розглянуті засоби впровадження механізмів захисту в комп'ютерних інформаційних системах мають можливість гнучкого управління безпекою в залежності від висунутих вимог, допустимого ризику та оптимальних витрат ресурсів.

Список літератури

1. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів // Системи обробки інформації. –2013. – Вип. 6 (113). – С. 215-223.

2. Іванов В.Г., Кошева Н.А., Мазниченко Н.І. Біометричні технології в задачах ідентифікації користувачів інформаційних комп'ютерних систем // Системи обробки інформації. – 2012. – Том 1. – Вип. 4 (102).
3. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека – СПб.: Политехника, 2001. – 240 с.
4. Бекмурзин М.С., Захаров В.П., Зачек О.И. Биометрические технологии в антитеррористической деятельности правоохранительных органов: перспективы и проблемы использования // Вестник Московского университета МВД России. – 2014. – №10. – С. 44-49.
5. Десятчиков А.А., Лобанцов В.В., Матвеев И.А., Мурынин А.Б. Об объединении дистанционных биометрических методов распознавания человека // Современный экстремизм в Российской Федерации: особенности проявления и средства противодействия: Материалы Всероссийской научно-практической конференции в Академии Управления МВД России. – М.: Академия управления МВД РФ, 2006. – С. 374-379
6. Суомалайнен А. Биометрическая защита: обзор технологии. – ДМК-Пресс, 2019. – 99 с.
7. Воронова В.А., Тихонов В.А. Системы контроля и управления доступом – М.: «Горячая линия – Телеком», 2010. – 272 с.
8. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа – СПб.: Наука и техника, 2004. – 384 с.
9. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Изд-во Юниор, 2003. – 504 с.
10. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средств азащиты информации. В 2-х томах. Том 2. Информационная безопасность. – К.: Арий, 2008. – 344 с.
11. Quaia C., Optican L M. Dynamic Eye Plant Models and the Control of Eye Movements // Strabismus. – 2003. – Vol. 11. – P. 17-31, 2003.
12. Kasproski P. And Ober J. Eye Movementsin Biometrics // European Conferenceon Computer Vision, Prague, Czech Republic, 2004. – P. 248-258.
13. Silver D.L., Biggs A.J. Keystroke and EyeTracking Biometrics for User Identification // International Conference on Artificial Intelligence (ICAI), Las Vegas, NV, USA, 2006. – P. 344-348.
14. Holland C., Komogortsev O.V. Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus // IEEE Transactions on Information Forensicsand Security. – 2013. – 8(12), – P. 2115-2126.
15. Komogortsev O.V., Holland C., Jayarathna S., Karpov A. 2D Linear Oculomotor Plant Mathematical Model: Verification and Biometric Applications // ACM Transactions on Applied Perception. – 2013. – 10 (4) – P. 1-18.
16. Komogortsev O.V., Holland C.D., Karpov A., Price L.R. Biometricsvia Oculomotor Plant Characteristics: Impact of Parametersin Oculomotor Plant Model // ACM Transactions on Applied Perception. – 2015.– P. 1-14.
17. Rigas I., Komogortsev O., Shadmehr R. Biometric recognition via the complex eye movement behavior and the incorporation of saccadic vigor and acceleration cues // ACM Trans. On Applied Perception. – 2016. – Vol. 13 (2). – P. 1-21.
18. Pavlenko V., Salata D., Dombrovskiy M. and Maksymenko Yu. Estimation of the Multidimensional Transient Functions Oculo-Motor System of Human // MathematicalMethodsandComputationalTechniquesinScienceandEngineering: AIP Conf. Proc. MMCTSE'2017, Cambridge, UK. – 2017. – 1872. – Melville, NewYork. Publishedby AIP Publishing. – P. 110-117.
19. Pavlenko V., Salata D., Chaikovskiy H. Identificationof a oculo-moto rsystem human based on Voltterrakernels // International Journal of Biologyand

- Biomedical Engineering. – 2017. – 11. – P. 121-126.
20. Doyle F.J., Pearson R.K., Ogunnaike B.A. Identification and control using Volterra models. – Germany: Springer Publ. – 2002. – 314 p.
 21. Pavlenko V., Pavlenko S. Deterministic identification methods for nonlinear dynamical systems based on the Volterra model // Applied Aspects of Information Technology. – 2018. – Vol.01. – №01. – P. 9-29.
 22. Павленко С.В., Павленко В.Д., Положаєнко С.А. Вычислительные методы идентификации моделей Вольтерра: [монография]. – Одесса: Экология, 2017. – 124 с.
 23. Pavlenko V., Milosz M., Dzienkowski M. Identification of the oculomotor system based on the Volterra model using eye tracking technology // 4th Int. Conf. on Applied Physics, Simulation and Computing (APSAC 2020) 23-25 May, Rome, Italy. Journal of Physics: Conference Series. – 2020. – Vol. 1603. – IOP Publishing, 2020. – P. 1-8.

METHOD FOR THE PROTECTION OF INFORMATION IN COMPUTER SYSTEMS ON THE EYE TRACKING DATA

T.V. Shamanina, V.D. Pavlenko

State University "Odessa Polytechnic",
Av. Shevchenko, 1, Odessa, 65044, Ukraine; E-mail: tatanatv8@gmail.com,
pavlenko_vitalij@ukr.net

Management and differentiation of access to computer systems and their resources is one of the important aspects of information security, which can be implemented by identifying users. Recently, identification systems that use biometric characteristics of a person to solve the problem of access to information systems are becoming more and more widespread. The paper proposes a new method for biometric identification of users of computer systems based on the definition of the Volterra integral model of the human oculo-motor system (OMS) based on the data of experimental "input-output" studies using innovative eye tracking technology. *The aim of the work* is to increase the efficiency (reliability) of information protection in computer systems through the development of hardware and software tools for identifying human OMS based on a nonlinear dynamic model and experimental eye tracking data using test visual stimuli. *The object of the research* is the process of biometric identification of a computer system user based on eye tracking data in dynamics – responses to given test visual stimuli. *The subject of the research* is instrumental algorithmic and software tools for constructing the Volterra model – assessing the multidimensional transition functions of the OMS based on eye tracking data. OMS identification software was developed in the Python IDLE programming environment. Test visual stimuli are used in the form of bright dots, which are sequentially displayed on the display screen at different distances from the starting position, which formally corresponds to different amplitudes of test step signals. Experimental studies of OMS were carried out in two individuals. Based on the data obtained using the TOBII PRO TX300 eye tracker, the transition functions of the first, second and third orders of the OMS are determined. A significant difference in the diagonal sections of the transition functions of the second and third orders was revealed in two individuals. Consequently, they can be used to form a space of informative features and build statistical classifiers of individuals using machine learning tools that implement the proposed method for protecting information in computer systems based on biometric identification of users based on eye tracking data. The proposed method of biometric identification and the developed means of introducing information protection mechanisms in computer information systems have the ability to flexibly control security, depending on the requirements put forward, the permissible risks and optimal resource costs.

Keywords: protection of computer information, biometric identification, human oculo-motor system, Volterra model, multi-dimensional transient functions, test visual stimuli, eye tracking.

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ РЕЦЕНЗУВАННЯ СТАТЕЙ ДЛЯ НАУКОВОГО ЖУРНАЛУ

Г.О. Шеремет

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sheremet.heorhiy@gmail.com

На сьогоднішній день у світі відбувається цифрова трансформація суспільства. Більшість видів людської діяльності поступово переносяться в цифровий вимір. У зв'язку з цим діджиталізація процесу рецензування є досить актуальним завданням. Опис реалізації автоматизованих систем рецензування відсутній в відкритому доступі, оскільки такі системи є інтелектуальною власністю відповідних журналів. *Метою* роботи є розробка автоматизованої системи подвійного сліпого рецензування статей для фахового журналу «Інформатика та математичні методи в моделюванні» Державного університету «Одеська політехніка». В роботі розглядається процес рецензування в автоматизованій системі рецензування статей. Описані дії рецензента, редактора та авторів. Розглянута послідовність цих дій. Спроектowana база даних, яка забезпечує функціонування розробленої системи. Розроблено алгоритм, який видаляє особисту інформацію авторів з файлу. Алгоритм дозволяє видалити: особисту інформацію автора з першої сторінки, колонтитул парних сторінок, анотації російською та англійською мовами в кінці файлу. У статті розроблена автоматизована система подвійного сліпого рецензування статей, яка забезпечує подвійне сліпе рецензування, автоматизує робочий процес редактора журналу та рецензента, мінімізує можливість складання рецензії третьою стороною. За рахунок впровадження автоматизованої системи рецензування статей значно підвищиться швидкість рецензування та з'явиться єдина база рецензій. Розроблена автоматизована система рецензування використовується редакцією фахового журналу «Інформатика та математичні методи в моделюванні» Державного університету «Одеська політехніка» для підвищення ефективності процесу рецензування. Результати даної роботи можуть бути використані при побудові аналогічної системи рецензування статей.

Ключові слова: рецензування статей, система реєстрації, подвійне «сліпе» рецензування, база даних, MySQL.

Вступ

Сучасний час є часом стрімкого розвитку суспільства, зокрема часом наукових досліджень в усіх сферах людської діяльності. Кожен день зусилля науковців світу з вирішення тої чи іншої конкретної проблеми завершуються отриманим вдалим результатом. Одним із традиційних шляхів доведення цих результатів до наукової спільноти є їх публікації в спеціалізованих виданнях. Але ніхто з людей, навіть відомих вчених, не може бути застрахованим від помилок, неточностей. Не можна також передбачити, що отримані результати будуть актуальними, значимими для відповідної галузі. Все це приводить до актуальності процесу рецензування визнаними фахівцями галузі результатів, що пропонуються авторами для публікації.

Системи рецензування, що існують в різних наукових виданнях, відрізняються між собою, але вимогою сьогодення є автоматизація відповідного процесу, актуальність чого зросла через карантинні міри, пов'язані з наявною в світі пандемією коронавірусу. Описи принципів реалізації існуючих автоматизованих систем рецензування, які використовуються в багатьох наукових журналах, включених до переліку фахових видань України, відсутні в відкритому доступі, оскільки такі системи є інтелектуальною

власністю відповідних журналів. Це не дає можливості скористатися готовим продуктом, а вимагає розробки особистого для кожного конкретного наукового видання.

Аналіз досліджень та публікацій

Рецензування залишається найдієвішим способом для оцінки значущості, актуальності, правильності отриманих авторами результатів на сьогодні, незважаючи на те, що деякі науковці виступають проти рецензування наукових публікацій.

Існує кілька видів рецензування [1,2,3].

Single-blindreview – одностороннє «сліпе». Цей вид рецензування вважається найпоширенішим[4]. У цьому випадку ім'я рецензента приховано від автора. Такий спосіб оцінки допомагає прийняти незалежне рішення, без будь-якого тиску з боку автора. Але деякі вчені висловлюють побоювання, що рецензенти, які працюють в тій же області, що і вони, можуть спеціально затримувати процес надання огляду роботи, дискредитувати автора або зовсім залишити за собою інформацію і видати її під своїм ім'ям.

Double-blindreview – подвійне «сліпе» [5]. У разі цього розгляду роботи анонімності дотримуються і автор, і рецензент. Такий стан речей дозволяє зберегти чесність і виключити будь-які упередження. Тут зовсім не буде відігравати роль біографія автора, його місце проживання або попередні роботи. Наукові статті розглядають незалежно від авторитету вченого. Багато дослідників виступають саме за цей вид рецензування.

Але є невеликий нюанс. Якщо автор працює в досить вузько спеціалізованій темі, рецензенти можуть впізнати його за специфікою предмета дослідження або за попередніми роботами.

Tripleblindpeerreview- тристороннє сліпе рецензування, є найбільш закритим методом оцінювання, оскільки всі учасники процесу (автори, рецензенти, редактори) є взаємно анонімними. Ця модель є сьогодні однією з найменш популярних, оскільки вимагає найбільше зусиль для реалізації[2].

Open review – відкрите рецензування[6]. Під час такого розгляду автор і рецензент знають один одного. Крім цього, в Інтернеті розміщують всю історію рецензування. Багато хто в науковому співтоваристві вважають, що саме таке рецензування є чесним і може убезпечити автора та експерта. Відкрите рецензування допомагає уникнути будь-яких передумов і жорстоких коментарів, а також плагіату. Рецензент більш тактовно і свідомо ставиться до роботи, швидше її виконує і надає чесну рецензію.

Але є й інша думка. Деякі вчені вважають, що відкритий розгляд може налякати експерта, і той напише рецензію без особливої критики, або мінімізує її кількість. Молоді рецензенти, через страх нашкодити своїй кар'єрі, можуть відмовитися об'єктивно критикувати роботу більш досвідченого і авторитетного вченого.

More Transparent Peer Review – прозоре рецензування. З часом все більше зростає потреба приймати більш відкриті моделі рецензування, і саме прозорий розгляд є інноваційним способом, допомагає пояснити ті чи інші рішення. Читачі можуть отримати доступ до історії експертного розгляду, звітів, висновків редакторів і відповідей авторів. За коментарями рецензентів можна зрозуміти, наскільки глибока робота була проведена, на що саме спиралися фахівці, нівелюючи можливості виникнення недостовірної інформації.

Collaborative Review – спільний розгляд[7]. Цей спосіб включає великий спектр підходів, під час якого співпрацює команда вчених. Двоє і більше рецензентів можуть працювати разом над роботою і в кінці надавати спільний звіт. Такий підхід передбачає співпрацю з автором для того, щоб поліпшити статтю, поки вона не буде відповідати

загальним критеріям. Спільне розгляд є більш конструктивним, тому що усуває бар'єри, з якими стикається вчені і експерти.

Postpublication review – огляд публікації після публікації. Рецензія зберігається або з'являється після публікації. Postpublication review може мати вигляд сторінки дискусійного форуму з коментарями разом з опублікованою статтею. Цей вид рецензування не виключає інші види експертного розгляду та йде більше як доповнення до основного способу.

Кожен зі способів рецензування має як свої переваги, так і недоліки. Вибір виду рецензування залежить від конкретного наукового видання, від його політики якості. В Україні, за аналізом процесів рецензування, що представлені на веб-сайтах українських наукових журналів, найпоширенішою є саме модель подвійного сліпого рецензування [2], яка і використовується далі.

Мета і задачі роботи

Мета роботи: розробка автоматизованої системи подвійного сліпого рецензування статей для фахового наукового журналу.

Для досягнення поставленої мети в роботі розв'язувалися наступні *задачі*:

- реалізувати реєстрацію, автентифікацію та авторизацію користувачів у системі рецензування;
- реалізувати процес безпосереднього рецензування статей;
- спроектувати базу даних.

Система розробляється з метою автоматизування процесу рецензування статей та покликана полегшити роботу редактора.

Основна частина

У системі необхідно реалізувати реєстрацію користувачів. За основу системи реєстрація була взята найпростіша реалізація, яка знаходиться у відкритому доступі [8]. Вона передбачає створення однієї таблиці в базі даних. З наступними полями «id», «login», «password» (рис.1).

Поле	Тип [Документація]	Длины/ Значения*	Атрибуты	Ноль	По умолчанию**	Дополнительно	Первичный	Индекс	Ун
id	INT			not null		auto_increment	☒	☐	☐
login	VARCHAR	15		not null			☐	☐	☐
password	VARCHAR	15		not null			☐	☐	☐

Рис. 1. Реалізація реєстрації користувачів.

Поле «id» забезпечує унікальність кожного запису у таблиці. Поля «login» та «password» користувач вказує при реєстрації і використовує їх при кожному вході у систему.

У розробленій системі процес рецензування відбувається згідно до рис. 2. Спочатку рецензенту необхідно зареєструватися у системі. При реєстрації рецензент надає свої особисті дані: ім'я, прізвище, по батькові, e-mail та вигадує пароль. На вказаний e-mail рецензент отримає код, який система відправляє після створення редактором запиту на рецензування. Отриманий код рецензент пред'являє, щоб отримати доступ до рецензування. Редактор, в свою чергу, додає авторів в базу даних системи. У формі додавання автора редактор вказує: ім'я автора, прізвище автора, по батькові автора, e-mail. Після рецензування на вказаний e-mail буде відправлена рецензія.

Наступним кроком, після реєстрації рецензента та занесення авторів до бази даних, буде створення запиту на рецензування редактором. У формі створення запиту

редактор залишає наступні дані: обирає одного рецензента серед зареєстрованих у системі; обирає до п'яти авторів, яких попередньо заніс до бази даних системи; завантажує файл статті. Після створення запиту на рецензування обраний рецензент отримає код, для доступу до рецензування, на його e-mail.

Отримавши код рецензент заходить в систему та пред'являє його. Система порівнює наданий рецензентом код з тим, що має у своїй базі даних. У випадку їх відповідності система надає рецензенту файл статті та шаблон рецензії. Рецензент завантажує статтю на свій пристрій, ознайомлюється з нею та заповнює наданий шаблон рецензії згідно своєї думки. По завершенню процесу рецензування рецензент підтверджує заповнений шаблон і він зберігається у базі даних системи.

На наступному кроці редактор має можливість ознайомитись зі складеною рецензією. Якщо рецензія складена некоректно він видаляє її з бази даних та створює новий запит на рецензування.

У випадку коли рецензію складено коректно, редактор надсилає рецензію авторам.

Автори, отримавши рецензію на свою поштову скриньку, ознайомлюються з нею і в залежності від змісту рецензії публікують або допрацьовують статтю.

Розглянемо структуру бази даних, яка забезпечує функціонування розробленої системи. У системі використовується СУБДМ у SQL [9].

База даних має наступні чотири таблиці:

- користувачі;
- автори;
- запити;
- рецензії.

До таблиці «користувачі» заносяться дані, які рецензент вказує при реєстрації (рис. 2).

#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐ 1	id	int			Нет	Нет		AUTO_INCREMENT	
☐ 2	name	varchar(30)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 3	surname	varchar(30)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 4	patronymic	varchar(30)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 5	email	varchar(320)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 6	password	varchar(60)	utf8mb4_0900_ai_ci		Нет	Нет			

Рис. 2. Структура таблиці «Користувачі».

До таблиці «автори» заносяться дані авторів, які редактор вказує при додаванні авторів (рис. 3).

#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐ 1	id	int			Нет	Нет		AUTO_INCREMENT	
☐ 2	name	varchar(15)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 3	surname	varchar(15)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 4	patronymic	varchar(15)	utf8mb4_0900_ai_ci		Нет	Нет			
☐ 5	email	varchar(320)	utf8mb4_0900_ai_ci		Нет	Нет			

Рис. 3. Структура таблиці «Автори».

До таблиці «запити» заносяться дані запиту, які редактор надає при створенні запиту на рецензування. У поле «article» заносяться шлях до файлу статті. Поля «email_author2- email_author5» є необов'язковими і заповнюються у випадку коли стаття має більше одного автора (рис. 4). У полі «condition_request» зберігається стан

запиту. Запит має два стани, «очікує» та «виконано». Одразу після створення запиту він має стан «очікує», поле «condition_request» має значення «0». Після складання рецензії за цим запитом його стан змінюється на «виконано», поле «condition_request» має значення «1».

#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐	1	id	int		Нет	Нем		AUTO_INCREMENT	
☐	2	email_reviewer	varchar(320)	utf8mb4_0900_ai_ci	Нет	Нем			
☐	3	article	varchar(100)	utf8mb4_0900_ai_ci	Нет	Нем			
☐	4	email_author1	varchar(320)	utf8mb4_0900_ai_ci	Да	NULL			
☐	5	email_author2	varchar(320)	utf8mb4_0900_ai_ci	Да	NULL			
☐	6	email_author3	varchar(320)	utf8mb4_0900_ai_ci	Да	NULL			
☐	7	email_author4	varchar(320)	utf8mb4_0900_ai_ci	Да	NULL			
☐	8	email_author5	varchar(320)	utf8mb4_0900_ai_ci	Да	NULL			
☐	9	code	int		Нет	Нем			
☐	10	condition_request	tinyint(1)		Нет	Нем			

Рис. 4. Структура таблиці «Запити».

До таблиці «рецензії» заноситься рецензія, яку склав рецензент (рис. 5). У поле «review» заноситься шлях до файлу рецензії, до поля «edited_review» заноситься id запиту за яким була складена рецензія. У полі «edited_review» зберігається стан рецензії. Поле має два стани, «складена» та «відправлена». Одразу після створення рецензії має стан «складена», поле «edited_review» має значення «0». Коли редактор відправляє рецензію її стан змінюється на «відправлена», поле «edited_review» має значення «1».

#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐	1	id	int		Нет	Нем		AUTO_INCREMENT	
☐	2	review	varchar(200)	utf8mb4_0900_ai_ci	Нет	Нем			
☐	3	id_request	int		Нет	Нем			
☐	4	edited_review	tinyint(1)		Нет	Нем			

Рис. 5. Структура таблиці «Рецензії»

Анонімність рецензента досягається шляхом приховування його особистості. Рецензія, яка відправляється авторам на поштову скриньку, не містить особистої інформації рецензента. До особистої інформації рецензента має доступ тільки редактор.

Для досягнення анонімності автора цього не достатньо, оскільки файл статті містить особисту інформацію автора. Отже було розроблено алгоритм, який видаляє з файлу особисту інформацію автора.

Розглянемо алгоритм, який видалятиме:

- особисту інформацію автора з першої сторінки;
- колонтитул парних сторінок;
- анотації російською та англійською мовами в кінці файлу.

Алгоритм, для редагування файлу статті згідно вимог, приведений нижче (рис. 6).

Розроблений алгоритм дозволяє видалити з файлу статті особисту інформацію авторів. Але слід бути обережним з його використанням, оскільки файл статті повинен відповідати чіткому стандарту. Якщо у файлі статті буде зайвий абзац або навпаки додатковий, алгоритм некоректно спрацює і є ймовірність витоку особистої інформації авторів.

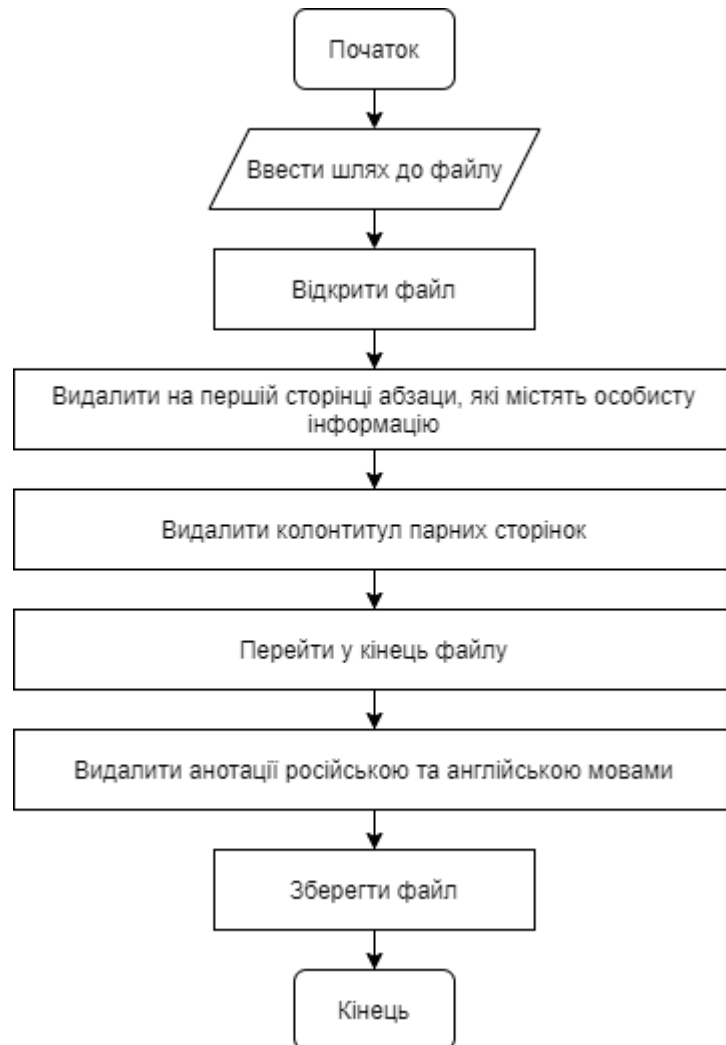


Рис. 6. Алгоритм видалення особистої інформації авторів з файлу статті

Висновки

У статті розроблена автоматизована система подвійного сліпого рецензування статей для фахового журналу.

Були розв’язані наступні задачі:

- реєстрація, аутентифікація та авторизація користувачів у системі рецензування;
- реалізований процес безпосереднього рецензування статей;
- спроектована база даних.

Всі перераховані вище завдання реалізовані повністю і в повній мірі покривають вимоги розробленої системи.

Розроблена система:

- автоматизує робочий процес редактора журналу та рецензентів;
- мінімізує можливість складання рецензії третьою стороною;
- забезпечує подвійне сліпе рецензування.

Розроблена автоматизована система рецензування використовується редакцією фахового журналу «Інформатика та математичні методи в моделюванні» для підвищення ефективності роботи.

Отримані в роботі результати можуть бути корисні не тільки для замовника, а й для інших наукових журналів. Результати роботи можуть служити основою для подальших розробок у цій галузі.

Список літератури

1. Наукове рецензування: його види та етапи.
URL: <https://ua.publ.science/uk/blog/retsenzirovaniye-ego-vidy-i-etapy>
2. О. Березко, Л. Ковалик. Аналіз алгоритму двостороннього сліпого рецензування в контексті впровадження принципів відкритої науки. *Вісник Національного університету «Львівська політехніка». Серія: Інформатизація вищого навчального закладу*. 2018. № 903. С. 58-66.
3. Jones L. What is peer review? URL: <https://editorresources.taylorandfrancisgroup.com/peer-review-introduction/>
4. Types of peer review. URL: <https://authorservices.wiley.com/Reviewers/journal-reviewers/what-is-peer-review/type/s-of-peer-review.html>
5. A. Etkin, T. Gaston, J. Roberts. PeerReview: Reform and Renewal in Scientific Publishing. URL: <https://www.fulcrum.org/concern/monographs/f4752j47p>
6. Березко О. Аналіз особливостей моделей рецензування в контексті побудови відкритих спільнот. *Інформація, комунікація, суспільство 2018*: матеріали VII Міжнародної наукової конференції ІКС-2018, Львів, 2018. С. 71-72.
7. Hayward A. 7 Common types of academic peer review. URL: <https://www.editage.com/insights/7-common-types-of-academic-peer-review>.
8. Шкурूपий М. Создание регистрации на сайте на PHP + MySQL. URL: <https://ruseller.com/lessons.php?id=347&rub=37>
9. Справочное руководство по MySQL.
URL: http://www.mysql.ru/docs/man/Database_use.html

DEVELOPMENT OF AN AUTOMATED ARTICLE REVIEW SYSTEM
FOR A SCIENTIFIC JOURNAL

Sheremet H.A.

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: sheremet.heorhiy@gmail.com

Today, the world is undergoing a digital transformation of society. Most of human activities are gradually being transferred to the digital dimension. In this regard, the digitalization of the peer review process is a very urgent task. The description of the implementation of automated peer review systems is not publicly available, because such systems are the intellectual property of the respective journals. The aim of the work is to develop an automated system for double-blind reviewing of articles for the professional Informatics and Mathematical Methods in Simulation journal. The paper discusses the process of reviewing in an automated system for reviewing articles. Described actions of reviewer, editor and authors. The sequence of these actions is considered. Designed the database that ensures the functioning of the developed system. An algorithm has been developed that removes the personal information of authors from the file. The algorithm allows you to delete: personal information of the author from the first page, headers of even pages, annotations in Russian and English at the end of the file. The article has developed an automated system for double-blind reviewing of articles, which provides double-blind reviewing, automates the workflow of the journal editor and reviewer, and minimizes the possibility of a third-party reviewing. Due to the introduction of an automated system for reviewing articles, the speed of reviewing will significantly increase and a single database of reviews will appear. The developed automated review system is used by the editors of the Informatics and Mathematical Methods in Simulation journal to improve the efficiency of the review process. The results of this work can be used to build a similar system for reviewing articles.

Keywords: article review, registration system, double blind review, database, MySQL.

**МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ДИНАМІЧНИХ СТАНІВ ПАРОРІДИННИХ
ДВОФАЗНИХ СИСТЕМ****С.А. Положаєнко, Д.А. Лись**Державний університет «Одеська політехніка»
просп. Шевченка, 1, Одеса, 65044; e-mail: sanp277@gmail.com

В межах хвильової динаміки двофазних середовищ — як розділу механіки неоднорідних систем та теплофізики, що інтенсивно розвивається, розглянуто можливості математичного опису (формалізації) процесів динаміки парорідинних двофазних систем. При цьому, на підставі врахування ефекту міжфазної взаємодії та використання концепції хвильових рухів, запропоновано гомогенну математичну модель динамічних станів парорідинних двофазних систем. Актуальність такої моделі полягає в тому, що двофазні потоки являють собою основне «робоче тіло», зокрема, в енергетичних установках та апаратах хімічної технології, а робочі процеси в металургійній, нафтодобувній та нафтопереробній (в т. ч. нафтохімічній) промисловості, в криогенних апаратах супроводжуються утворенням парорідинних систем. В зв'язку з цим, наявність адекватної гомогенної математичної моделі динаміки для середовищ, які розглядаються, заснованої на врахуванні законів збереження та придатної для застосування у інженерних розрахунках, слід розглядати як перевагу над емпіричними моделями, які забезпечують задовільну точність розрахунків лише в обмеженому діапазоні технологічних параметрів і абсолютно непридатних для позаштатних та аварійних режимів. Проведений аналіз розповсюдження нелінійних хвиль та формування ударних хвиль у парорідинному (або газорідинному) середовищі на основі гомогенного представлення останнього показує аналогічність традиційному газодинамічному підходу, але, тим не менш, парорідинна (або газорідинна) суміш має певні особливості. Перед усім це стосується ідеалізації гомогенної суміші як деякого газу — континууму, у якого густина рідини, а властивість стискання як у газового середовища. Наслідком останнього є низькі значення швидкості звука та висока нелінійність, спричинена залежністю від тиску, особливо на ділянках його зростання. Можна вважати, що гомогенна модель є достатньо інформативною, щоб дозволити робити висновки щодо можливих механізмів перебігу динамічних процесів для парорідинної (газорідинної) суміші та прогнозувати подальший їх розвиток за умови апріорної інформації про газодинамічні характеристики двофазної системи.

Ключові слова. Парорідинні суміші, двофазні системи, гомогенна модель, математична модель, нелінійні та ударні хвилі.

Вступ

Певне розповсюдження в літературі [1 — 4], як достатньо наглядний та зручний спосіб континуального представлення двофазного середовища, зокрема газо- або парорідинної суміші, віднайшло представлення у вигляді *гомогенної суміші*. Таке трактування парорідинних двофазних систем (ПРДС) коректне за умови перебування останніх у *бульбашковому режимі* [1 — 3, 5], що є достатньо характерним фізичним станом парорідинної суміші [6, 7]. Суміш рідини та газу (пару) в даному випадку розглядається як деяке однорідне середовище із середньою температурою T , густиною ρ та тиском P . Основним припущенням даного представлення є швидкий обмін імпульсом, теплою та масою між фазами. Внаслідок цього, температури та швидкості руху фаз вважаються такими, що дорівнюють одна одній. Вважається, що тиск у рідинній фазі P_1 або дорівнює тискові в газовій фазі P_2 , або відрізняється на величину лапласівського тиску $\Delta P = 2\sigma/R$, де R — радіус бульбашок (середній), σ — коефіцієнт поверхневого

напруження (тут, і подальшому, індекс 1 позначає рідку фазу, а індекс 2 — пар або газову фазу).

Складання гомогенної математичної моделі (ММ) динамічних станів ПРДС дає подальший розвиток теорії нестационарної гідро-(газо)динаміки і дає змогу, хоча б у першому наближенні, врахувати особливості двофазних парорідинних систем. Така ММ може бути спробою створення простих хвильових моделей, які відповідають законам збереження, притаманних динамічним режимам, в яких перебувають двофазні системи.

Мета роботи

Формування ММ стану парорідинної двофазної системи (суміші), яка забезпечує адекватну формалізацію динамічних властивостей системи (суміші) у всіх технологічних режимах її перебування.

Основна частина

Для складання гомогенної математичної моделі ПРДС будемо вважати, що парова (газова) фаза складається з бульбашок одного розміру, а кількість бульбашок N на 1 кг маси суміші не змінюється, то питомий об'єм пару (газу) в суміші буде складати $V = (3/4)\pi R^3 N$. Істинний об'ємний вміст пару (газу) ϕ очевидно зв'язаний з V та густиною середовища ρ наступним чином: $\phi = V\rho$. В літературі, присвяченій дослідженню ПРДС [6, 7], зустрічається інший вираз для визначення ϕ , а саме: $\phi = (3/4)\pi R^3 N\rho = (3/4)\pi R^3 n$, де $n = N\rho$ — кількість бульбашок в одиниці об'єму. При цьому слід зазначити, що на відміну від N , величина n не є постійною. Масовий паро-(газо-)вміст X визначимо через ϕ та густину пару (газу): $X = V\rho_2 = \phi\rho_2/\rho$. На відміну від об'ємного масовий паро-(газо-)вміст при відсутності фазових переходів не змінюється.

Середню густину суміші (двофазної системи) можна увести через об'ємний паро-(газо-)вміст ϕ співвідношенням

$$\rho = \rho_1(1 - \phi) + \rho_2\phi \quad (1)$$

або масовий паро-(газо-)вміст X , відповідно:

$$1/\rho = (1 - X)/\rho_1 + X/\rho_2 = (1 - X)/\rho_1 + V. \quad (2)$$

Використавши ρ з рівняння (1), можна віднайти зв'язок між ϕ та X :

$$X = \frac{\rho_2\phi}{\rho_2\phi + \rho_1(1 - \phi)}.$$

Далі можна отримати:

$$\delta V/V = \frac{\delta P(1 - \phi)^2(1 - X)}{c_1^2\rho\phi} - \frac{\delta P}{\rho\phi} = \frac{\delta P}{\rho\phi} \left[\frac{(1 - \phi)^2(1 - X)}{c_1^2} - 1 \right], \quad (3)$$

де c_1 — швидкість звуку у рідині. Тут використано акустичний зв'язок між збудженнями густини рідини та тиску в середовищі: $\delta\rho_1 = \delta P/c_1^2$.

Таким чином, суміш бульбашок з рідиною розглядається як деякий газ, густина якого близька до густини рідини, а стискання цього середовища визначається стисканням газової або парової фази. Можна визначити деякі основні термодинамічні характеристики цієї суміші:

— ентропію

$$s = s_1(1 - X) + s_2 X ;$$

— ентальпію

$$h = h_1(1 - X) + h_2 X .$$

Для гомогенної моделі важливою властивістю є рівновага парорідинної суміші, яку може бути порушено навіть незначними впливами та хвильовими збудженнями.

Поширення малих збуджень та нелінійних хвиль

Рівняння гомогенної моделі будується по аналогії з рівнянням гідрогазодинаміки однофазного середовища [8, 9] і можуть бути представлені у вигляді

$$\begin{cases} \partial\rho/\partial t + \partial(u\rho)/\partial x = 0; \\ \partial u/\partial t + u\partial u/\partial x = -(1/\rho)\partial P/\partial x; \end{cases} \quad (4)$$

$$\partial h/\partial t + u\partial h/\partial x = (1/\rho)(\partial P/\partial t + u\partial P/\partial x). \quad (5)$$

Тут u , ρ , P , h — відповідно швидкість, густина, тиск та ентальпія суміші.

Малі збудження представимо з урахуванням уявлення про *адіабатичність* процесу на основі лінійної моделі (4), (5):

$$\partial u/\partial t = -(1/\rho_0)\partial P/\partial x ; \quad \partial\rho/\partial t = -\rho_0 \partial u/\partial x$$

або

$$\begin{aligned} \partial^2\rho/\partial t^2 &= \partial^2 P/\partial x^2; \\ ds/dt &= 0. \end{aligned} \quad (6)$$

При математичному описі динаміки газорідинної суміші, як і в газодинаміці, нелінійними є не тільки рівняння руху суміші (4), (5), але і рівняння стану, тобто джерело нелінійності — залежність швидкості звуку c від поточних значень збуджень швидкості. Тому тільки при нелінійному аналізі розповсюдження хвиль в рідині з бульбашками можна користуватися значенням $c = (\partial P/\partial\rho)_s^{0,5}$ при $P = P_0$, $\rho = \rho_0$, $\varphi = \varphi_0$.

З вищеприведеного випливає, що

$$\left(\frac{\partial\rho}{\partial P}\right)_s \frac{\partial^2 P}{\partial t^2} - \frac{\partial^2 P}{\partial x^2} = 0$$

або

$$\frac{\partial^2 P}{\partial t^2} - \left(\frac{\partial \rho}{\partial P} \right)_s - \frac{\partial^2 P}{\partial x^2} = 0. \quad (7)$$

При розгляді газорідного середовища у випадку, коли в процесі розповсюдження рідини масовий газовміст X не змінюється і зміна густини відбувається за рахунок стискання бульбашок, для $(\partial \rho / \partial P)_s$ можна скористатися формулою Меллока [10]

$$c_m^2 = \frac{\rho_2}{\rho_1} \frac{c_2^2}{\varphi(1-\varphi)} = \frac{\gamma P}{\rho \varphi}$$

(де γ — показник адіабати газу)

з початковими значеннями параметрів $P = P_0$, $\rho = \rho_0$, $\varphi = \varphi_0$:

$$\left(\frac{\partial \rho}{\partial P} \right)_s = \frac{\gamma P_0}{\rho_0 \varphi_0}, \quad (8)$$

і (7) приймає вигляд лінійного хвильового рівняння

$$\frac{\partial^2 P}{\partial t^2} - \frac{\gamma P_0}{\rho_0 \varphi_0} \cdot \frac{\partial^2 P}{\partial x^2} = 0. \quad (9)$$

В іншому граничному випадку, коли розглядається парорідне середовище та при розповсюдженні хвилі зміна густини відбувається виключно за рахунок зміни паровмісту X , вираз $(\partial \rho / \partial P)_s$ може бути визначено за співвідношенням

$$\left(\frac{\partial \rho}{\partial P} \right)_s = c_2^2 = \frac{P_2^2 L^2}{\rho^2 C_p \bar{B}^2 T^3}, \quad (10)$$

де L — прихована теплота пароутворення, $P_2 = P$, $\bar{B}$ — питома газова постійна, T — поточна температура, а рівняння (7) набуде вигляду:

$$\frac{\partial^2 P}{\partial t^2} - \frac{P_0^2 L^2}{\rho_1^2 C_p \bar{B}^2 T^3} \frac{\partial^2 P}{\partial x^2} = 0. \quad (11)$$

Аналіз похідної $(\partial P / \partial \rho)_s$ можна провести на основі класичного методу переходу до нових термодинамічних змінних. Тиск P має власні змінні (параметри) ρ та s . Переходячи до нових змінних ρ та X і використовуючи властивість якобіанів та умову калібрування термодинамічних потенціалів [8], можна отримати:

$$\left(\frac{\partial \rho}{\partial P}\right)_s = \frac{\partial(P, s)}{\partial(\rho, s)} = \frac{\partial(P, s)}{\partial(\rho, X)} \cdot \frac{\partial(P, X)}{\partial(\rho, s)}; \quad (12)$$

$$\left(\frac{\partial \rho}{\partial P}\right)_s = \frac{(\partial s / \partial X)_P}{(\partial \rho / \partial P)_X (\partial s / \partial X)_P - (\partial s / \partial P)_X (\partial \rho / \partial X)_P}. \quad (13)$$

У парорідинному середовищі без фазових переходів $X = \text{const}$, і з (13) випливає

$$(\partial P / \partial \rho)_s = (\partial P / \partial \rho)_X = \gamma P / (\rho \varphi) = c_m^2. \quad (14)$$

Для парорідинного середовища, коли $(\partial P / \partial \rho)_X = 0$, тобто густина змінюється тільки за рахунок зміни X , можна записати

$$\left(\frac{\partial \rho}{\partial P}\right)_s = \frac{(\partial s / \partial X)_P}{-(\partial s / \partial P)_X (\partial \rho / \partial X)_P} = \frac{P^2 L^2}{\rho_1^2 C_{P_1} \bar{B}^2 T^3} = c_2^2. \quad (15)$$

У загальному випадку, коли зміна густини відбувається за рахунок властивості стискання та зміни X , також справедливою є формула (13), з якої випливає

$$c^{-2} = c_m^{-2} + c_2^{-2} \quad \text{або} \quad c^2 = \frac{c_m^2 c_2^2}{c_m^2 + c_2^2}, \quad (16)$$

де c_m та c_2 визначаються формулами (14) та (15).

Таким чином, якщо при розповсюдженні хвилі має місце фазовий перехід (тобто зміна X), то в рамках рівновагового підходу розповсюдження збудження відбувається зі швидкістю, близькою до c_2 . З урахуванням зробленого зауваження, вирази (12), (13) та (15) (з відповідними початковими та граничними умовами) можна розглядати як гомогенну ММ ПРДС для можливих обмежень щодо виникнення *бульбашкового режиму*.

Наслідками високого ступеню стискання парорідинної суміші є низькі значення швидкості звуку та висока нелінійність, які виникають через значну залежність $c = c(P)$ на початковій ділянці росту тиску.

На практиці поширенням станом перебування ПРДС є утворення ударних хвиль. Розглянемо особливості гомогенної ММ ПРДС за умови існування ударних хвиль.

Ударні хвилі

Через нелінійність хвилі в середовищі можливі «перехлест» та утворення ударних хвиль. Ударні хвилі у газовій динаміці розглядаються як розриви, на границях яких виконуються певні співвідношення, що є наслідками законів збереження.

Газодинамічний аналіз стрибків в рамках гомогенної моделі в уявленні того, що ударні хвилі в рідині з бульбашками газу існують і є ізотермічними, було виконано в роботі [11]. Відповідно до результатів роботи [11] можна записати закони збереження маси та імпульсу на границі розриву, а саме (для простоти запису не застосовуючи індекс «см» при позначенні паро-(газо-)рідинної суміші):

$$\rho_1 u_1 = \rho_2 u_2; \quad P_1 + \rho_1 u_1^2 = P_2 + \rho_2 u_2^2. \quad (17)$$

Тут індекс 1 відповідає стану паро-(газо-)рідинної суміші до розриву, а індекс 2 — після розриву. Вважаючи процес стискання бульбашок ізотермічним, очевидно що $P_1 V_1 = P_2 V_2$, а враховуючи, що $V = \varphi / \rho$, можна отримати

$$P_1 / P_2 = \varphi_2 \rho_1 / \varphi_1 \rho_2. \quad (18)$$

Замінюючи $u_2 = \rho_1 u_1 / \rho_2$ закон збереження імпульсу можна записати наступним чином:

$$u_1^2 = \frac{(P_1 - P_2) \rho_2}{\rho_1 (\rho_2 - \rho_1)}. \quad (19)$$

Вважаючи, що рідина є такою, що не стискається, можна записати

$$(\rho_2 - \rho_1) \approx \rho_1 (\varphi_1 - \varphi_2); \quad u_1^2 = \frac{(P_1 - P_2) \rho_2}{\rho_1^2 \varphi_2 (\varphi_1 / \varphi_2 - 1)}. \quad (20)$$

З рівняння ізотермічності видно, що $\varphi_1 / \varphi_2 = (1 - \varphi_1) P_2 / [(1 - \varphi_2) P_1]$. Підстановка останнього в (20), і беручи до уваги співвідношення $(1 - \varphi_1) / (1 - \varphi_2) \approx 1$, можна отримати $u_1^2 = (P_2 - P_1) \rho_2 P_1 / [(P_2 - P_1) \rho_1^2 \varphi_2]$. Оскільки $(1 - \varphi_2) \approx 1$, $(1 - \varphi_1) \approx 1$, то, виконавши заміну по (1.33), можна віднайти

$$u_1^2 = P_2 / \varphi_1 \rho_1, \quad (21)$$

де P_2 — повний тиск за ударною хвилею.

У випадку, коли амплітуду ударної хвилі спрямовано до нуля, формула (21) переходить у вираз для квадрата швидкості звуку $c_0^2 = \gamma P_0 / \rho \varphi_0$. Співвідношення (21), яке зв'язує швидкість ударної хвилі з інтенсивністю стрибка, добре узгоджується з формулою Кемпбела-Пітчера [11], яку часто використовують при газодинамічному аналізі ударних хвиль.

Висновок

Для поширених випадків існування ПРДС (малих збуджень та нелінійних хвиль) отримано їх ММ у вигляді гомогенної моделі. Актуальність розробки саме гомогенної моделі ПРДС пояснюється тим, що значна кількість двофазних систем мають властивість значного стискання (тобто швидкість звуку в таких системах мала), характеризуються нелінійністю і, тому для розрахунку динаміки таких середовищ, що рухаються з відносно невеликими швидкостями, необхідно застосування газодинамічних методів. Крім того, рух двофазних систем супроводжується процесами міжфазного теплообміну, які спричиняють сильну дисипацію середовища, а інерційні властивості газових включень породжують залежність швидкості звуку від частоти — дисперсію швидкості звуку. Тому методи традиційної газової динаміки не відповідають специфіці двофазних потоків і дають незадовільні результати при розрахунках.

Для частинного випадку утворення ударних хвиль, спричинених розривністю потоку, розглянуто особливості складання гомогенної моделі ПРДС за умови існування хвилі до та після розривів.

Список літератури

1. Айдагулов Р. Р., Хабеев Н.С., Шагапов В.Ш. Структура ударной волны в жидкости с пузырьками газа с учетом нестационарного межфазного теплообмена. *Журнал прикладной механики и технической физики*. 2005. № 3. С. 67 — 74.
2. Акуличев В.А., Алексеев В.Н., Бурлаков В.А. Акустические волны в жидкости с паровыми пузырьками. Нелинейные процессы в двухфазных средах. Новосибирск: Изд-во Новосибирского ун-та, 2007. С. 114 — 121.
3. Воинов О.В., Петров А. Г. Движение пузырей в жидкости. *Итоги науки и техники. Сер.: Мех. жидкости и газа*. 2006. Т. 10. С. 86 — 147.
4. Кутателадзе С.С. Анализ подобия и модели термодинамике газожидкостных систем *Журнал прикладной механики и технической физики*. 2000, № 5. С. 24 — 33.
5. Акуличев В.А., Алексеев В.Н. О динамике паровых пузырьков в жидководородных пузырьковых камерах. *Акустический журнал*. 2007. Т. 17. № 3. С. 356 — 364.
6. Багатуров С.А. Основы теории и расчета перегонки и ректификации. М.: Энергия, 2014. 440 с.
7. Прауэниц Дж.М., Эккерт К.А., О'Рай Р.В., О'Коннепп Дж.П. Машинный расчет парожидкостного равновесия многокомпонентных смесей. М.: Химия, 2007. 217 с.
8. Гарипов Р.М. Замкнутые уравнения движения жидкости с пузырьками. *Журнал прикладной механики и технической физики*. 2003. №6. С. 3 — 24.
9. Zwick S.A. Behaviour of small permanent gas bubbles in a liquid. *J. Math. and Phys.* 2008. V. 37, No 3. P. 36 — 52.
10. Кедринский В.К. Распространение возмущений в жидкости, содержащей пузырьки газа. *Журнал прикладной механики и технической физики*. 2008. № 4. С. 29 — 34.
11. Campbell I.J., Pitcher A.S. Shock waves in a liquid containing gas bubbles. *Proc. Roy. Soc. Ser. A*. 2008. V. 243, No 1235. P. 534 — 545.

**MATHEMATICAL FORMALIZATION OF DYNAMIC STATES OF
VAPOR-LIQUID TWO-PHASE SYSTEMS**

S.A. Polozhaenko, D.A. Lys

Odessa National Polytechnic University
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: sanp277@gmail.com

Within the framework of wave dynamics of two-phase media – as a section of mechanics of inhomogeneous systems and thermo physics, which is intensively developing, the possibilities of mathematical description (formalization) of the processes of dynamics of vapor-liquid two-phase systems are considered. In this case, based on the effect of interphase interaction and the use of the concept of wave motions, a homogeneous mathematical model of dynamic states of vapor-liquid two-phase systems is proposed. The relevance of this model is that two-phase flows are the main "working fluid", in particular, in power plants and chemical technology, and work processes in the metallurgical, oil and refining (including petrochemical) industry, in cryogenic devices accompanied by the formation of vapor-liquid systems. In this regard, the availability of an adequate homogeneous mathematical model of dynamics for the environments under consideration, based on conservation laws and suitable for use in engineering calculations, should be considered as an advantage over empirical models that provide satisfactory accuracy only in a limited range of technological parameters and completely unsuitable for emergency and emergency modes. The analysis of the propagation of nonlinear waves and the formation of shock waves in a vapor-liquid (or gas-liquid) medium based on a homogeneous representation of the latter shows similarity to the traditional gas-dynamic approach, but, nevertheless, vapor-liquid (or gas-liquid) mixture has certain features. First of all, this applies to the idealization of a homogeneous mixture as a gas - a continuum, which has a liquid density and the property of compressing the gaseous medium. The consequence of the latter is low values of the speed of sound and high nonlinearity caused by the dependence on pressure, especially in areas of its growth. We can assume that the homogeneous model is quite informative, which allows us to draw conclusions about possible mechanisms of dynamic processes for vapor-liquid (gas-liquid) mixture, and predict their further development provided a priori information about the gas-dynamic characteristics of a two-phase system.

Keywords: Vapor-liquid mixtures, two-phase systems, homogeneous model, mathematical model, nonlinear and shock waves.