

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

УДК 004.4

Т. Б. Мартинюк, О. В. Войцеховська, О. С. Городецька, А. К. Рижков
МОДУЛЬ ІНТЕГРАЦІЇ ВЕБЗАСТОСУНКІВ ІЗ ШТУЧНИМ
ІНТЕЛЕКТОМ

Вінницький національний технічний університет, Вінниця

Анотація. В роботі досконалено метод інтеграції серверної частини вебзастосунок для організації дієти та системи тренувань зі штучним інтелектом ChatGpt, що дало змогу покращити User Experience при використанні серверної частини вебзастосунок та збільшити швидкість обробки запитів штучним інтелектом та пришвидшити роботу користувача зі штучним інтелектом. Проаналізовано сучасні технології для зв'язку серверної частини веб-додатку із базою даних, реалізації авторизації з метою впровадження захисту серверної частини від злоумисників, а також методи інтеграції веб-застосунок з штучним інтелектом. За результатами аналізу обрано стек технологій, зокрема для розробки серверної частини використано Web-API, для зв'язку серверної частини вебзастосунок із базою даних було використано технологію Entity Framework, авторизацію забезпечено за допомогою JWT Tokens. Розроблено серверну частину веб-застосунок для організації тренувань та дієти мовою програмування C#, з урахуванням принципів об'єктно-орієнтованого програмування SOLID. Під час розробки використано багаторівневу архітектуру для розподілення різних функціональних можливостей між різними модулями серверної частини. Налаштовано зв'язок серверної частини вебзастосунок з базою даних для отримання та збереження інформації. Реалізовано механізм авторизації на JWT-Токенах, що дозволило захистити методи для інтеграції з штучним інтелектом від злоумисників та дало можливість тільки авторизованим користувачам використовувати штучний інтелект для побудови тренувань та дієти. Спроектовано базу даних MSSQL, в якій зберігаються персональні дані користувача, що використовуються для побудови дієти та системи тренувань штучним інтелектом ChatGpt. Запити до бази даних оптимізовані за рахунок використання техніки Eager Loading та запитів Deferred Execution.

Ключові слова: вебзастосунок, модуль інтеграції, штучний інтелект, ChatGpt, багаторівнева архітектура, .NET, Access Token.

Abstract. The method of integrating the server part of the web application for organizing a diet and workouts with artificial intelligence ChatGpt was improved in the work, which made it possible to improve the User Experience when using the server part of the web application and increase the speed of processing requests by artificial intelligence and speed up the user's work with artificial intelligence. Modern technologies for the connection of the server part of the web application with the database, the implementation of authorization in order to implement the protection of the server part from intruders and the methods of integrating the web application with artificial intelligence are analyzed. Based on the results of the analysis, a stack of technologies was chosen, in particular, Web-API was used to develop the server part, Entity Framework technology was used to connect the server part of the web application with the database, and authorization was provided using JWT Tokens. The server part of the web application for workouts and diet organization was developed in the C# programming language, taking into account the principles of SOLID object-oriented programming. During the development, a multi-level architecture was used to distribute various functionalities between different modules of the server part. The connection of the server part of the web application with the database for receiving and saving information is configured. An authorization mechanism on JWT-Tokens was implemented, which made it possible to protect the methods for integration with artificial intelligence from attackers and gave the opportunity to only authorized users to use artificial intelligence to build workouts and diets. An MSSQL database that stores personal user data used to build the ChatGpt AI diet and workouts is designed. Database queries are optimized by using the Eager Loading technique and Deferred Execution queries.

Key words: web application, integration module, artificial intelligence, ChatGpt, multi-tier architecture, .NET, Access Token.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-5-12>.

Вступ

Вебзастосунки вже давно стали невід'ємною частиною нашого життя. Вони використовуються в різних сферах, включаючи освіту, бізнес, розваги, соціальні мережі та багато інших. Широке розповсюдження вебзастосунків пояснюється їх зручністю, доступністю та гнучкістю. Вони дозволяють користувачам виконувати різноманітні завдання, не виходячи з браузера.

Актуальність

Незважаючи на широке розповсюдження, вебзастосунки постійно потребують вдосконалення. Одним з напрямків цього вдосконалення є інтеграція з чатом GPT, яка може значно покращити функціональність вебзастосунків, додаючи можливості для більш ефективної взаємодії з користувачами.

Чат GPT може використовуватися для виконання різноманітних завдань, таких як відповідь на запитання користувачів, надання рекомендацій, автоматизація процесів та багато іншого [1]. Це може зробити вебзастосунки більш інтерактивними, зручними та корисними для користувачів. Таким чином, інтеграція вебзастосунків з чатом GPT є важливим кроком на шляху до створення більш інтелектуальних та корисних вебзастосунків.

Постановка задачі

В даній роботі інтеграцію із чатом GPT реалізовано на прикладі розробки модулю інтеграції, що використовується у вебзастосунку для організації тренувань та дієти. Більшість спортивних сайтів та застосунків можуть запропонувати користувачам лише статті на тему харчування, тренування та розра-

хунок денної норми калорій, в залежності від даних користувача, але на сьогодні жоден із сайтів не може побудувати повноцінну персоналізовану дієту та тренувальну програму, виходячи із індивідуальної інформації, що надав користувач. Тому розробка вебзастосунку для організації планування дієти та тренувань з використанням чату GPT є актуальною та перспективною задачею.

Мета

Метою роботи є розширення функціональних можливостей вебзастосунку завдяки його інтеграції із чатом GPT, що дасть можливість покращити User Experience (UX) та збільшити швидкість обробки запитів чатом GPT.

Основна частина

При розробці вебзастосунку для організації тренувань та дієти було вирішено використовувати ChatGpt, оскільки штучний інтелект має змогу проаналізувати інформацію про користувача, а саме індивідуальні характеристики, його мету та медичні обмеження, і, враховуючи її, побудувати найкращий денний раціон, розрахувати калорії, вказати, які вправи повинен робити користувач для досягнення результату. При цьому необхідно налаштувати ChatGpt так, щоб він спілкувався з користувачем, наче він персональний дієтолог чи тренер, який надає рекомендації щодо дієти та тренувань.

Для розробки вебзастосунку було обрано клієнт-серверну архітектуру, оскільки клієнт-серверний розподіл допомагає забезпечити ефективну обробку запитів, підвищити масштабованість та краще керувати ресурсами.

Проведено аналіз та вибір технологій для розробки клієнтської та серверної частини вебзастосунку. Клієнтську частину розроблено із використанням технології Qwik, оскільки вона орієнтована на досягнення максимальної продуктивності та оптимізації роботи веб-застосунку та зосереджується на уникненні надмірного завантаження коду JavaScript, що призводить до швидкого завантаження сторінок та поліпшення інтерактивності для користувача [2].

При проектуванні серверної частини обрано багаторівневу архітектуру, яка розділяє рівень доступу до даних, рівень бізнес логіки та рівень представлення на окремі шари [3, 4]. Для розробки API було обрано платформу ASP.Net Core та мову програмування C#. Для взаємодії з базою даних обрано Entity Framework Core, який відповідає за зручну маніпуляцію над даними через об'єктно-орієнтований підхід платформи .Net [5]. Окрім цього потрібно забезпечити авторизацію користувачів, для того щоб захистити методи інтеграції з штучним інтелектом. Для цього було обрано авторизацію на JWT-токенах [6-9].

В роботі вдосконалено метод інтеграції серверної частини з штучним інтелектом, в якому реалізовано побудову та надсилання запитів, створених на основі персональної інформації користувача, до штучного інтелекту ChatGpt з використанням його API. UML-діаграму діяльності методу інтеграції наведено на рис. 1. Коли клієнт надсилає запит, серверна частина перевіряє чи користувач, який запитав дієту існує, і при позитивному результаті відбувається перевірка чи користувач додав усю необхідну інформацію для побудови запиту.

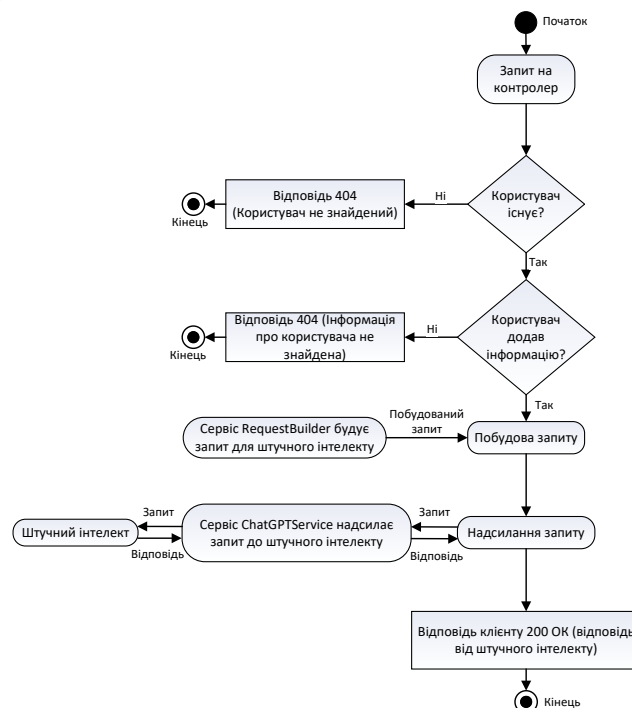


Рисунок 1 – UML-діаграма діяльності методу інтеграції серверної частини з штучним інтелектом

Якщо верифікація пройшла успішно, сервіс серверної частини буде запит до ChatGPT. При цьому, запит повинен містити усю необхідну інформацію про користувача, зокрема вік, стать, зріст та вагу. Також штучному інтелекту важливо розуміти рівень фізичної активності користувача, оскільки це напряму впливає на кількість калорій, які користувач може споживати за добу. Важливо, щоб ChatGPT розумів ціль користувача, якою може бути: втрата зайвої ваги, збереження своєї форми, набір м'язової ваги тощо. Користувач, за бажанням, може вказати свої вподобання у їжі та будь-які алергії чи непереносимість продуктів. Це допоможе штучному інтелекту сформулювати індивідуальні поради, рекомендації та плани на основі унікальних потреб користувача.

Згенерований запит надсилається до ChatGPT і серверна частина очікує на опрацювання запиту. При отриманні відповіді на запит, вона буде надіслана на клієнтську частину для відображення на рівні представлення.

Запропонований метод дозволяє заповнити просту форму на клієнтській частині, і з цієї інформації серверна частина побудує запит. В свою чергу, інші веб-застосунки, що інтегровані з штучним інтелектом, змушують користувача самому будувати запит до штучного інтелекту, через що користувач може забути вказати важливу інформацію або побудувати запит неправильно, з точки зору prompt engineering [10, 11].

У вебзастосунку використано ChatGPT версії 3.5-turbo. Приклад згенерованого серверною частиною запиту наведено на рис. 2. Запит у JSON-форматі буде надісланий на API ChatGPT.

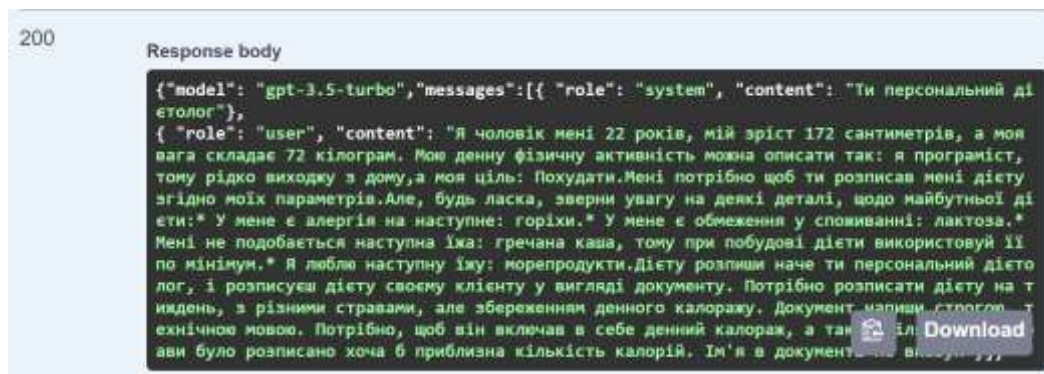


Рисунок 2 – Скріншот запиту, сформованого серверною частиною у JSON-форматі

В запиті вказано необхідну інформацію про користувача, наявність алергії та обмеження в їжі, харчові вподобання. Окрім цього вказано, що дієта повинна мати вигляд документа, в якому буде розписано денну допустиму кількість калорій для користувача, а також приблизний калораж кожної страви.

У відповідь на запит, що наведено на рис. 2, ChatGPT згенерує відповідь клієнту, в якій буде вказано раціон харчування на тиждень, кількість калорій в кожній страві, а також скільки всього калорій потрібно отримувати користувачу в день, щоб досягти своєї мети.

Аналогічно формується запит для побудови тренування для користувача, відповідно до його цілей. У цьому випадку штучний інтелект налаштовуємо на те, щоб він був персональним тренером, замість персонального дієтолога. Інформація, що вводиться, подібна до тієї, яка використовувалась при побудові запиту на дієту.

Для реалізації описаного вище методу інтеграції було розроблено програмний модуль інтеграції з штучним інтелектом, UML-діаграма класів якого наведена на рис. 3.

Модуль інтеграції вебзастосунку для організації тренувань та дієти зі штучним інтелектом складається з двох класів та двох інтерфейсів для забезпечення перевикористання та гнучкості коду:

- інтерфейс `IChatRequestBuilder`, в якому визначені публічні функції, що необхідні для отримання запиту для побудови дієти та тренувань;
- інтерфейс `IChatGptService`, в якому визначені усі публічні методи, необхідні для інтеграції зі штучним інтелектом;
- клас `ChatRequestBuilder`, в якому реалізовано методи для побудови запиту для отримання дієти та тренувань, а також приватні методи, в яких винесено базові елементи повідомлення штучному інтелекту та додавання харчових звичок відповідно до їх наявності;
- клас `ChatGptService`, в якому реалізовано метод, що ініціалізує клієнта та метод, що надсилає запит штучному інтелекту і отримує відповідь.

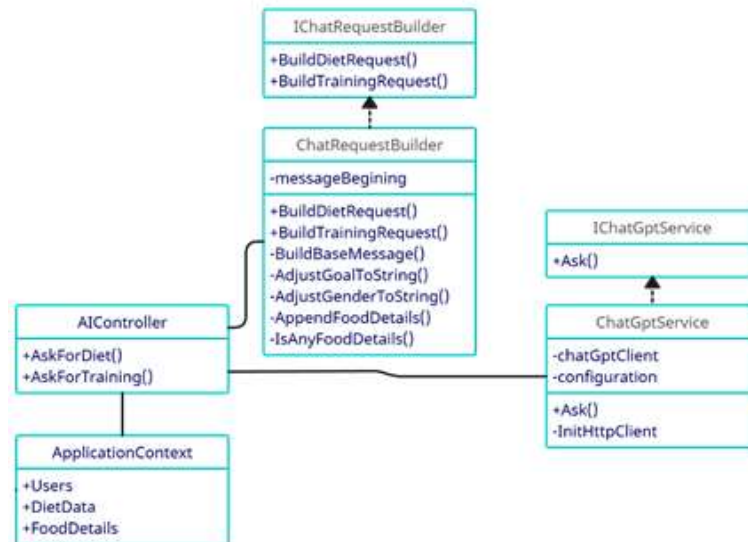


Рисунок 3 – UML-діаграма класів модулю інтеграції вебзастосунку із ChatGPT

Тригером до запуску усього процесу є контролер `AIController`, який приймає запит від клієнтської частини. Після отримання запиту контролер отримує інформацію про користувача із бази даних, передає її у клас `ChatRequestBuilder` для побудови запиту на дієту або тренування та надсилає цей запит до `ChatGpt`. Після отримання відповіді, клас контролеру відповідає на клієнтський запит та пересилає відповідь штучного інтелекту.

Тестування вебзастосунку

Для генерації системи тренувань та дієти користувач повинен зареєструватись та авторизуватись за електронною поштою і паролем, вказати антропометричні дані та за бажанням харчові звички, наявність алергії тощо. Зареєстрований користувач буде зберігатись в базі даних. Приклад додавання інформації, необхідної для побудови запиту наведено на рис. 4. Приклад додавання інформації про харчові звички наведено на рис. 5.

Штучний інтелект обробляє запит і у відповіді надсилає дієту або систему тренувань у вигляді тексту та деяку службову інформацію про виконання запиту (`index` – індекс повідомлення від штучного інтелекту; `message` – відповідь чату GPT у вигляді тексту; `finish_reason` – причина закінчення генерації відповіді; `usage` – об'єкт, який містить інформацію про кількість використаних токенів на генерацію відповіді). Відповідь штучного інтелекту з наданою дієтою на тиждень наведено у лістингу 1.

```
Request body
{
  "userId": "4c2514b5-f648-44fb-b4d5-0fb996d7f341",
  "age": 22,
  "height": 173,
  "weight": 69,
  "gender": 1,
  "goal": 1,
  "physicalActivity": "програміст, сидячий образ життя"
}

Code    Details
200
Response headers
access-control-allow-credentials: true
access-control-allow-origin: http://localhost:5087
content-length: 0
date: Mon, 20 Nov 2023 18:40:05 GMT
server: Kestrel
vary: Origin
```

Рисунок 4 – Приклад додавання інформації про користувача

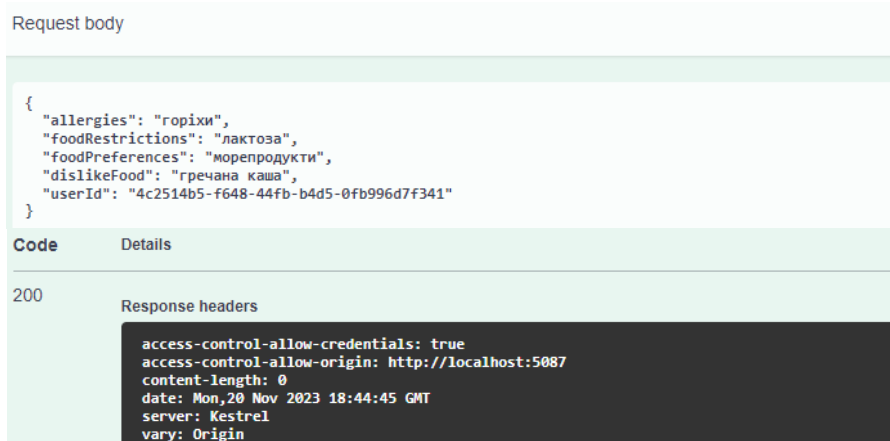


Рисунок 5 – Приклад додавання інформації про харчові звички користувача

Лістинг 1 – Відповідь штучного інтелекту на запит побудови дієти

```
{
  "id": "chatcmpl-8N3gu5xOZuLwmROAbSNaxx4GX811b",
  "object": "chat.completion",
  "created": 1700506424,
  "model": "gpt-3.5-turbo-0613",
  "choices": [
    {
      "index": 0,
      "message": {
        "role": "assistant",
        "content": "Дієтологічне розслідування N001\n\nЗгідно вимоги клієнта, вирішили скласти індивідуальну дієту з метою збереження маси, враховуючи її параметри та особливості. Враховуючи алергію на горіхи та обмеження щодо споживання лактози, були виключені відповідні продукти з раціону, замінені альтернативними варіантами задля забезпечення балансованого раціону. Також були враховані особисті вподобання клієнта щодо харчування і подані описи кожної страви з приблизною кількістю калорій.\n\nНагадуємо, що дана дієта розрахована на тиждень, з використанням різних страв для різноманітності, збереженням денного калоражу, а включення морепродуктів, що предпочитає клієнт, є обов'язковим.\n\n**План харчування**\n\n*День 1*\n\nСніданок: Омлет з двох яєць з додаванням цибулі та перцю - 240 ккал.\n\nСніданок №2: Нежирний йогурт з фруктами - 150 ккал.\n\nОбід: Грильована куряча грудка з овочами та рисом - 350 ккал.\n\nПолуденок: Яблуко - 80 ккал.\n\nПолуденок №2: Фруктовий салат із сезонних фруктів - 120 ккал.\n\nВечеря: Запечений лосось з пюре зі смаженими овочами - 400 ккал.\n\nПізна вечеря: Половина грейпфрута - 50 ккал.\n\n*День 2*\n\nСніданок: Нежирний йогурт з м'ясом та свіжими ягодами - 250 ккал.\n\nСніданок №2: Фруктовий смузі з молоком без лактози - 180 ккал.\n\nОбід: Тушкована свинина зі стевією та овочевим гарніром - 400 ккал.\n\nПолуденок: Груша - 60 ккал.\n\nПолуденок №2: Зелена салатна суміш з оливковою олією та орехами (без горіхів) - 150 ккал.\n\nВечеря: Печена тріска з лимона та овочевим гірчичним соусом - 350 ккал.\n\nПізна вечеря: Чашка чорного чаю - 0 ккал.\n\n*День 3*\n\nСніданок: Ржані оладки з лляним насінням та медом - 280 ккал.\n\nСніданок №2: М'яка моцарелла з томатами та базиліком - 200 ккал.\n\nОбід: Варений індича філе з квасолею та салатом зі свіжих овочів - 380 ккал.\n\nПолуденок: Мандарин - 40 ккал.\n\nПолуденок №2: Ароматизований йогурт без лактози - 120 ккал.\n\nВечеря: Гречані локшина з креветками та соєвим соусом - 450 ккал.\n\nПізна вечеря: Один шматочок чорного шоколаду (70% какао) - 60 ккал.\n\nІ так далі, розписуючи план харчування на тиждень із різними стравами, але зберігаючи денний калораж клієнту.\n\nЦей план харчування розроблено з урахуванням денного калоражу клієнта та її потреби в збереженні маси. Приблизна кількість калорій наведена для кожної страви, щоб забезпечити належний контроль над харчуванням.\n\nСупроводжуючи цей план харчування, радимо щодня споживати достатню кількість води, не менше 1,5-2 літрів, і займатися фізичною активністю для підтримання загальної фізичної форми.\n\nЦей план харчування підлягає регулярному оновленню та адаптації, в залежності від реакції клієнта та досягнення її цілей.\n\nПідпис: персональний дієтолог"
```

```
    },
    "finish_reason": "stop"
  ]
},
"usage": {
  "prompt_tokens": 588,
  "completion_tokens": 1559,
  "total_tokens": 2147
}
}
```

У дієті враховані обмеження користувача та його вподобання. Окрім цього кожна страва містить кількість калорій, необхідних користувачу. Видно, що штучний інтелект повертає текст із символами форматування, тому на рівні представлення розробники можуть відобразити дієту згідно UI/UX дизайну.

Аналогічно штучний інтелект надав програму тренувань для користувача. Відповідь штучного інтелекту з розписаною системою тренувань наведено у лістингу 2.

Лістинг 2 – Відповідь штучного інтелекту на запит побудови системи тренувань

```
{
  "id": "chatcmpl-8N3rxSLkup3ArbwYFf4VGj1AtKSyz",
  "object": "chat.completion",
  "created": 1700507109,
  "model": "gpt-3.5-turbo-0613",
  "choices": [
    {
      "index": 0,
      "message": {
        "role": "assistant",
        "content": "Розклад тренувань для досягнення цілі -- збереження маси тіла:\n\nДень 1:
Нижня частина тіла\n\n1. Розминка (10 хвилин):\n - Швидка хода на біговій доріжці (5
хвилин)\n - Розтяжка ніг (5 хвилин)\n\n2. Силові вправи (3 набори по 10-12 повторень):\n -
Присідання з гантелями\n - Промовистий жим ніг\n - Випади з гантелями\n - Мостик\n\n3.
Кардіо-тренування (20-30 хвилин):\n - Велотренажер\n - Кросовер або еліптичний
тренажер\n\n4. Розтяжка (10 хвилин):\n - Статичні розтяжки для ніг та стегон\n\nДень 2:
Верхня частина тіла\n\n1. Розминка (10 хвилин):\n - Загальне розігрівання (5 хвилин)\n -
Розтяжка рук та плечей (5 хвилин)\n\n2. Силові вправи (3 набори по 10-12 повторень):\n - Жим
штанги на груди\n - Розведення гантелей на плечі\n - Тяга гантель до плеча\n - Вправи
для трапеції\n\n3. Кардіо-тренування (20-30 хвилин):\n - Біг на біговій доріжці\n - Верти-
кальний еліптичний тренажер\n\n4. Розтяжка (10 хвилин):\n - Розтяжка м'язів спини та
рук\n\nДень 3: Загальне зміцнення\n\n1. Розминка (10 хвилин):\n - Інтервальний біг на місці
(5 хвилин)\n - Розтяжка всього тіла (5 хвилин)\n\n2. Функціональні тренування (3-4 набори по
10-12 повторень):\n - Підйоми на боковій планці\n - Планка на передню та задню дельту\n
- Русская рулетка з гантелями\n - Супермени\n\n3. Кардіо-тренування (20-30 хвилин):\n -
Тренажер для бігу зі зростанням нахилу\n - Степ-платформа\n\n4. Розтяжка (10 хвилин):\n -
Інтервал розтяжок всіх м'язових груп тіла\n\nПримітка: Після кожної тренування, не забудьте
зайти на розтяжку зону, щоб розслабити м'язи та попрацювати над гнучкістю.\n\nЗверніть увагу,
що цей розклад є загальним і може бути змінений або адаптований відповідно до вашої фізичної
підготовки та ваших потреб. Рекомендую також проконсультуватися з особистим тренером, який
допоможе вам дещо продумати, зокрема, раціон харчування, тренувальний план тощо."
      },
      "finish_reason": "stop"
    }
  ],
  "usage": {
    "prompt_tokens": 256,
    "completion_tokens": 1078,
    "total_tokens": 1334
  }
}
```

Отримана система тренувань описує які вправи слід виконувати та в які дні. Також описано загальні рекомендації щодо занять спортом, щоб користувач міг коригувати систему тренувань під себе.

Висновки

1. Вдосконалено метод інтеграції веб-застосунку з штучним інтелектом ChatGPT 3.5-turbo за рахунок побудови та надсилання запиту до OpenAI API, сформованого на основі визначених в роботі вимог, що дало можливість покращити User Experience при використанні веб-застосунку.

2. Спроектовано багаторівневу архітектуру серверної частини веб-застосунку, що дозволило розділити різні функціональні можливості у різних модулях. Програмна реалізація серверної частини веб-застосунку для організації тренувань та дієти виконана на платформі ASP.Net Web-API, з дотриманням принципів об'єктно-орієнтованого програмування та принципів SOLID.

3. Реалізовано механізм авторизації на JWT-Токенах, що дозволило захистити методи для інтеграції з штучним інтелектом від злоумисників та дало можливість тільки авторизованим користувачам використовувати штучний інтелект для побудови тренувань та дієти.

4. Проведене тестування показало відсутність критичних помилок, стабільність роботи клієнтської і серверної частин та правильність виконання заданих функцій.

Список літератури

- [1] Introducing ChatGPT and Whisper APIs. [Електронний ресурс]. Режим доступу: <https://openai.com/blog/introducing-chatgpt-and-whisper-apis>.
- [2] Фреймворк Qwik. [Електронний ресурс]. Режим доступу: <https://qwik.builder.io/docs/concepts/think-qwik/>.
- [3] Understanding Multilayer Architecture. [Електронний ресурс]. Режим доступу: <https://www.c-sharpcorner.com/UploadFile/1492b1/understanding-multilayered-architecture-in-net/>
- [4] A Multi-Layer Back-End Application Architecture in .NET Core. [Електронний ресурс]. Режим доступу: <https://hamzaak.medium.com/a-multi-layer-back-end-application-architecture-in-net-core-c08898f2427e>
- [5] Introduction to Entity Framework. [Електронний ресурс]. Режим доступу: <https://www.partech.nl/nl/publicaties/2020/11/introduction-to-entity-framework>
- [6] Войцеховська О. В., Городецька О. С., та Рижков А. К., "Аналіз методів авторизації при проектуванні серверної частини веб-додатку" на Матеріали міжнародної науково-практичної інтернет-конференції "Електронні інформаційні ресурси: створення, використання, доступ", 2023 р. С. 225–227. Режим доступу: https://drive.google.com/file/d/1oVmxS3W_sEQPjes9S9AzWDaJxDxi6IOX/view.
- [7] Authentication and Authorization in Web API. [Електронний ресурс]. Режим доступу: <https://dotnettutorials.net/lesson/authentication-and-authorization-in-web-api/>
- [8] Introduction to authorization in ASP.NET Core. [Електронний ресурс]. Режим доступу: <https://learn.microsoft.com/en-us/aspnet/core/security/authorization/introduction?view=aspnetcore-7.0>
- [9] JSON Web Tokens. [Електронний ресурс]. Режим доступу: <https://auth0.com/docs/secure/tokens/json-web-tokens>
- [10] Prompt engineering. [Електронний ресурс]. Режим доступу: <https://platform.openai.com/docs/guides/prompt-engineering>.
- [11] Embeddings – OpenAI API. [Електронний ресурс]. Режим доступу: <https://platform.openai.com/docs/guides/embeddings>.

Стаття надійшла: 12.01.2024

References

- [1] Introducing ChatGPT and Whisper APIs. [Online]. Available: <https://openai.com/blog/introducing-chatgpt-and-whisper-apis>.
- [2] Framework Qwik. [Online]. Available: <https://qwik.builder.io/docs/concepts/think-qwik/>. Accessed on: 07. 01. 2024.
- [3] Understanding Multilayer Architecture. [Online]. Available: <https://www.c-sharpcorner.com/UploadFile/1492b1/understanding-multilayered-architecture-in-net/>. Accessed on: 07. 01. 2024.
- [4] A Multi-Layer Back-End Application Architecture in .NET Core. [Online]. Available: <https://hamzaak.medium.com/a-multi-layer-back-end-application-architecture-in-net-core-c08898f2427e>. Accessed on: 07. 01. 2024.
- [5] Introduction to Entity Framework. [Online]. Available: <https://www.partech.nl/nl/publicaties/2020/11/introduction-to-entity-framework>. Accessed on: 07. 01. 2024.
- [6] Voitsekhovska O. V., Horodetska O.S., Ryzhkov A. K., "Analiz metodiv avtoryzatsii pry proektuvanni servernoi chastyny veb-dodatku [Analysis of authorization methods when designing the server part of a web application]" on Materials of the international scientific and practical Internet conference: stvorennia, vykorystannia, dustup [Electronic information resources: creation, use, access]", 2023. P. 225–227 [Online].
- [7] Authentication and Authorization in Web API. [Online]. Available: <https://dotnettutorials.net/lesson/authentication-and-authorization-in-web-api/>. Accessed on: 07. 01. 2024.
- [8] Introduction to authorization in ASP.NET Core. [Online]. Available: <https://learn.microsoft.com/en-us/aspnet/core/security/authorization/introduction?view=aspnetcore-7.0>. Accessed on: 07. 01. 2024.
- [9] JSON Web Tokens. [Online]. Available: <https://auth0.com/docs/secure/tokens/json-web-tokens>. Accessed on: 07. 01. 2024.
- [10] Prompt engineering. [Online]. Available: <https://platform.openai.com/docs/guides/prompt-engineering>. Accessed on: 07. 01. 2024.
- [11] Embeddings – OpenAI API. [Online]. Available: <https://platform.openai.com/docs/guides/embeddings>. Accessed on: 07. 01. 2024.

Відомості про авторів

Мартинюк Тетяна Борисівна – д.т.н., професор, професор кафедри обчислювальної техніки.

Войцеховська Олена Валеріївна – к.т.н., доцент, доцент кафедри обчислювальної техніки.

Городецька Оксана Степанівна – к.т.н., доцент, доцент кафедри обчислювальної техніки.

Рижков Андрій Костянтинович – студент групи ІКІ-22м кафедри обчислювальної техніки, факультет інформаційних технологій та комп'ютерної інженерії.

T. B. Martyniuk, O. V. Voytsekhovska, O. S. Horodetska, A. K. Ryzhkov

**INTEGRATION MODULE OF WEB APPLICATIONS WITH
ARTIFICIAL INTELLIGENCE**

Vinnitsia National Technical University, Vinnitsia

УДК 004.932

Р. В. Маслій, В. В. Гармаш, П. П. Ковальчук, В. В. Кабачій

АНАЛІЗ МЕТОДІВ ЗНАХОДЖЕННЯ АНОМАЛІЙ У ЗОБРАЖЕННЯХ

Вінницький національний технічний університет, Вінниця

Анотація. Автоматичне виявлення аномалій має велике значення в промисловості, дистанційному зондуванні та медицині. Важливо мати можливість автоматично обробляти великі обсяги даних для виявлення, наприклад, хімічних об'єктів на багатоспектральних та гіперспектральних супутникових зображеннях, морських мін на сонарних зображеннях бічного зондування, або дефектів у виробничих моніторингових застосуваннях. Автоматичне виявлення аномальних структур на довільних зображеннях стосується задачі пошуку невідповідних шаблонів відносно нормального стану зображення. Це важка задача в комп'ютерному зорі, оскільки не існує чіткого і прямолінійного визначення того, що є нормальним чи не нормальним для даного довільного зображення. Практична важливість проявляється у розробці алгоритмів та моделей, які автоматично можуть виявляти незвичайні або аномальні образи у зображеннях. Проведено аналіз методів знаходження аномалій у зображеннях з точки зору можливості застосування до довільних зображень. Наведена класифікація методів виявлення аномалій за критеріями залучених підходів та моделей що використовуються для моделювання фону. Розглянуті методи, які використовують машинне навчання, такі як однокласовий метод опорних векторів та варіаційний автоенкодер, методи виявлення аномалій на основі найближчих сусідів, на основі кластеризації, статистичне виявлення аномалій, спектральне виявлення аномалій, виявлення аномалій за допомогою інформаційної теорії. Основна увага приділена методам, що класифікують за підходом до моделювання фону. Розглянуто п'ять категорій методів, що моделюють фон, базуючись на функції щільності ймовірності, глобальній та локальній однорідності, розрідженості та самоподібності. Для застосувань виявлення аномалій рекомендовано використовувати методи, у яких модель фону найкраще описує очікуваний фон, на якому відсутні аномалії, оскільки це, як правило, призводить до найкращої ефективності. На основі досліджень було встановлено, що ефективна універсальна модель виявлення аномалій у довільних зображеннях повинна: використовувати лише самоподібну чи розріджену модель фону; обробляти залишкове зображення як стохастичний процес для виявлення аномалій, як аномалій у кольоровому шумі; попередньо обробляти залишкове зображення перед виявленням аномалій.

Ключові слова: моделювання, обробка зображення, виявлення аномалій, фонові моделі, машинне навчання.

Abstract. Automatic anomaly detection is of great importance in industry, remote sensing, and medicine. It is important to be able to automatically process large amounts of data to detect, for example, chemical objects in multispectral and hyperspectral satellite images, sea mines in side-scan sonar images, or defects in industrial monitoring applications. Automatic detection of anomalous structures on arbitrary images refers to the task of finding inappropriate patterns relative to the normal state of the image. This is a difficult task in computer vision, since there is no clear and straightforward definition of what is normal or not normal for a given arbitrary image. The practical importance is manifested in the development of algorithms and models that can automatically detect unusual or anomalous patterns in images. An analysis of methods for finding anomalies in images from the point of view of the possibility of application to arbitrary images has been carried out. The classification of anomaly detection methods according to the criteria of the involved approaches and models used for modeling the background is presented. Methods that use machine learning, such as one-class support vector method and variational autoencoder, nearest neighbor-based anomaly detection, clustering-based anomaly detection, statistical anomaly detection, spectral anomaly detection, anomaly detection using information theory are discussed. The main attention is paid to the methods classified according to the background modeling approach. Five categories of background modeling methods based on probability density function, global and local homogeneity, sparsity, and self-similarity are considered. For anomaly detection applications, it is recommended to use methods in which the background model best describes the expected anomaly-free background, as this generally results in the best performance. On the basis of research, it was established that an effective universal model for detecting anomalies in arbitrary images should: use only a self-similar or sparse background model; process the residual image as a stochastic process to detect anomalies, such as anomalies in color noise; preprocess the residual image before detecting the anomaly.

Key words: modeling, image processing, anomaly detection, background model, machine learning.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-13-22>.

Вступ

У сучасному світі машинне навчання стає все більш важливою і перспективною галуззю, яка викликає значний інтерес серед дослідників і фахівців. Вже зараз його застосування суттєво змінює багато аспектів нашого повсякденного життя, включаючи медицину, фінанси, автономну навігацію, розпізнавання мови та інші галузі. Одним із важливих напрямків машинного навчання є виявлення аномалій у зображеннях.

Автоматичне виявлення аномальних структур на довільних зображеннях стосується задачі пошуку невідповідних шаблонів відносно нормального стану зображення. Це важка задача в комп'ютерному зорі, оскільки не існує чіткого і прямолінійного визначення того, що є нормальним чи не нормальним для даного довільного зображення.

Актуальність

Виявлення аномалій у зображеннях має велику практичну важливість та є досить актуальним. Практична важливість проявляється у розробці алгоритмів та моделей, які автоматично можуть виявляти незвичайні або аномальні образи у зображеннях. Серед таких аномалій можуть бути неочікувані об'єкти,

пошкодження зображень, помилки під час зйомки або будь-які інші зміни, які відхиляються від звичайного стану.

Автоматичне виявлення аномалій має велике значення в промисловості, дистанційному зондуванні та медицині. Важливо мати можливість автоматично обробляти великі обсяги даних для виявлення, наприклад, хімічних об'єктів на багатоспектральних та гіперспектральних супутникових зображеннях, морських мін на сонарних зображеннях бічного зондування, або дефектів у виробничих моніторингових застосуваннях [1]. Це виявлення може бути виконано за допомогою будь-якого пристрою для зображень, від камер до скануючих електронних мікроскопів.

Останнім часом методи виявлення аномалій у зображеннях стрімко розвиваються, тому у іноземних виданнях з'являється велика кількість статей присвячених цій задачі, зокрема і оглядових, наприклад робота [1], в україномовних же виданнях таких статей обмаль. Крім того, у оглядових статтях присвячених даній тематиці в переважній більшості розглядаються методи виявлення аномалій, які є залежними від конкретного застосування без врахування можливості використання кожного методу в інших застосуваннях, тобто без оцінки його універсальності. Наприклад, методи виявлення аномалій розроблені для медичних зображень, скоріш за все не будуть працювати достатньо надійно при їх використанні у промисловій інспекції якості продукції. Саме тому виникає потреба у проведенні аналізу методів виявлення аномалій, з акцентування уваги на довільних зображеннях для створення нового універсального методу, що може бути ефективно використаний у різних сферах застосування.

Мета

Метою дослідження є порівняння методів виявлення аномалій на довільних зображеннях та визначення більш універсального, для якого визначені основні параметри.

Задачі

1. Розглянути класифікацію методів виявлення аномалій за критеріями залучених підходів та моделей що використовуються для моделювання фону
2. Здійснити аналіз літературних джерел методів згідно класифікації до моделювання фону.
3. Здійснити аналіз розглянутих методів виявлення аномалій з точки зору можливості застосування до довільних зображень.

Розв'язання задач

У оглядовій статті [1] встановлюється розрізнення між точковими аномаліями, контекстуальними аномаліями, колективними аномаліями, в залежності від того, чи є фон сталим чи змінним і чи має аномалія більший масштаб, ніж початкові вибірки. Також робиться розрізнення між контрольованим, частково контрольованим та не контрольованим навчанням для виявлення аномалій. Крім того, автори пропонують таку класифікацію залучених підходів до виявлення аномалій у зображеннях:

1. Методи, які використовують машинне навчання. У цих методах класифікатор навчається відрізнити звичайні дані від аномальних у просторі ознак. Класифікація може бути багатокласовою (нормальні та аномальні дані) або однокласовою (класифікатор навчається визначити лише нормальні дані, тобто навчається знаходити межі навколо нормальних даних).

2. Виявлення аномалій на основі найближчих сусідів. Основне припущення цих методів полягає в тому, що нормальні екземпляри даних у просторі ознак знаходяться близько один до одного, тоді як аномалії знаходяться далеко від своїх найближчих сусідів. Це може бути виміряно за допомогою відстані до k -го найближчого сусіда або за відносною щільністю.

3. Виявлення аномалій на основі кластеризації. Ці методи припускають, що екземпляри нормальних даних належать до кластера у просторі ознак, тоді як аномалії визначаються як ті, що знаходяться далеко від центру їхнього найближчого кластера.

4. Статистичне виявлення аномалій. Аномалії визначаються як спостереження, ймовірно невірні для генерації стохастичною моделлю фону. Таким чином, аномалії знаходяться в областях з низькою ймовірністю моделі фону.

5. Спектральне виявлення аномалій. Основним інструментом цих методів є аналіз головних компонентів (АГК) та його узагальнення. Принцип полягає в тому, координати аномалій відхиляються відносно нормальних координат АГК.

6. Виявлення аномалій за допомогою інформаційної теорії. Ці підходи аналізують інформаційний зміст набору даних за допомогою мір інформаційної теорії, таких як колмогорова складність, ентропія, відносна ентропія та інші.

Більшість досліджень в галузі виявлення аномалій проводяться шляхом моделювання розподілів фонових даних для оцінки ймовірності того, що тестові дані не належать до таких розподілів [1]. Тому основні методи виявлення аномалій можна класифікувати за їхнім підходом до моделювання фону.

Кожен метод виявлення повинен виконувати три завдання:

а) моделювати "фон" без аномалій. Ця модель фону може бути створена з вибірок різного розміру, взятих з даного зображення (або бази даних зображень): пікселі (наприклад, у гіперспектральних зображеннях), фрагменти, локальні ознаки (наприклад, вейвлет коефіцієнти).

б) визначити вимір, який оцінює, наскільки віддалені вибірки спостережуваних даних від їхньої моделі фону. Зазвичай ця міра - це ймовірність помилкового спрацювання (або, очікування кількості помилкових спрацювань), пов'язане з кожною вибіркою.

в) визначити відповідне (емпірично або статистично обґрунтоване) значення порогу на вимірі, отриманому у пункті б.

Класифікація методів здійснюється за структурою їхньої моделі фону та способом обчислення відстані між вибірками та моделлю фону.

Розглянемо докладно п'ять загальних структур для фону:

1. Фон може бути моделюваний функцією щільності ймовірності, яка може бути параметричною, такою як гауссова, гауссова суміш, або отримана інтерполяцією з вибірок за допомогою методу оцінки щільності ядра; ця структура веде до виявлення аномалій шляхом перевірки статистичних гіпотез;

2. Фон глобально однорідний (використовується еталонне зображення, глобальна трансформація Фур'є або модель згорткової нейронної мережі, як правило, з наступним відніманням фону);

3. Фон локально просторово однорідний (методи "центру-околу");

4. Фон є розрідженим у визначеному словнику або базі (моделі варіаційного розкладання).

Фон є самоподібним (у нелокальному розумінні, що для кожної вибірки існують інші подібні вибірки у зображенні).

Стохастичні моделі фону

Принцип роботи цих методів виявлення аномалій полягає в тому, що аномалії виникають в областях з низькою ймовірністю за фонову моделлю.

Гауссова модель фону. Припущення про гаусівський фон може застосовуватися до фрагментів зображень. У [2] запропонували побудувати гауссову модель фону на основі випадкових 2×2 фрагментів зображення в гіперспектральному зображенні. Якщо отримано цю модель фону (μ ; Σ), то аномальні (2×2) фрагменти виявляються за допомогою порогового значення для їх відстані Махаланобіса до гауссової моделі фону. Вибір блоків зображень для оцінки гауссової моделі фрагмента (μ ; Σ) виконується за допомогою процедури RANSAC вибираючи випадкові фрагменти зображення і поступово виключаючи аномальні.

У роботі [3] виконується оцінка фону в локальному просторі ознак головних компонентів (це також передбачає побудову гауссової моделі). Потім для виявлення аномальних пікселів, а саме тих, що мають надзвичайно велику відстань Махаланобіса до нормального розподілу, використовується перевірка статистичних гіпотез. Це виявляє потенційно аномальні пікселі, які потім групуються і фільтруються морфологічними операторами. Використання цього фільтру вказує на те, що перший етап може давати багато помилкових спрацювань.

Оцінка щільності розподілу функції ймовірності.

У роботі [4] автори використовують моделі гауссових випадкових полів Маркова для виявлення дефектів у тканинах. У цих методах розраховують ймовірність наявності дефектів у фрагментах розміром 32×32 або 64×64 , використовуючи модель, навчену на даних без дефектів. Потім застосовують тест відношення ймовірностей для класифікації цих фрагментів як аномальних або таких, у яких відсутні дефекти.

Модель гауссової суміші. Ідея, яка була представлена в роботі [5], полягає у навчанні моделі текстур на основі теорії текстонів Джулеза. Текстони інтерпретуються як фрагменти зображень, які відповідають гауссовій моделі. Таким чином, випадковий фрагмент зображення розглядається як відповідний моделі гауссової суміші, яка оцінюється на основі зразкових зображень за допомогою алгоритму максимізації очікування. Метод функціонує на кількох масштабах у гауссовій піраміді з фіксованими розмірами фрагментів. Пороги для виявлення аномалій навчаються на зразках без дефектів: на кожному масштабі обчислюється мінімальна ймовірність в моделі гауссової суміші для всіх фрагментів, і ці значення служать порогами для виявлення аномалій. Фрагмент вважається аномальним, якщо ймовірність його наявності менше, ніж мінімальна ймовірність, яка була визначена на текстурах без аномалій на двох послідовних діапазонах масштабів у гауссовій піраміді. Карта помітності (saliency map) створюється шляхом підсумовування цих послідовних значень ймовірності. Цю модель можна перетворити з карти помітності в систему виявлення аномалій за допомогою гіпотетичного тестування на фоновій моделі гауссової суміші.

Моделювання гауссової суміші вже давно вважається класичним методом у гіперспектральних зображеннях для виявлення аномалій. У цьому випадку, не потрібно використовувати фрагменти, оскільки кожен гіперспектральний піксель вже містить багатовимірну інформацію [1].

Гауссовий процес. У роботі [6] пропонують метод, який моделює фонове зображення як гауссовий стаціонарний процес, який також може бути модельований як результат згортки моделі білого гауссового шуму з довільним ядром, іншими словами, кольоровим шумом. Ця модель фону є досить обмеженою, але точною і простою для оцінки.

Висновки. У методах, які ґрунтуються на стохастичних моделях фону, аномалії виявляються як неспільні з імовірнісним розподілом, оціненим на основі вхідного зображення. Поріг виявлення аномалій є статистичним тестом на ймовірність, побудованим на основі навченої фонові моделі. Цей тест надає p -значення для кожного виявлення. Таким чином, змінюючи пороги виявлення, можна легко контролювати кількість помилкових спрацювань.

Моделі фону однорідного типу

Ці методи оцінюють фон та зазвичай віднімають його від зображення, щоб отримати залишкове (residual) зображення, на якому в кінцевому підсумку виконується виявлення.

Модель фону Фур'є. Можливо, найбільш успішним методом на основі фону є виявлення аномалій в періодичних патернах текстилю [7], [8]. Це може бути зроблено, шляхом вирівнювання певних частот в області Фур'є та застосування порогового значення до залишкових зображень для виявлення дефектів. У роботі [8] пропонують автоматизований метод виявлення дефектів на поверхнях із випадковими текстурями, які зустрічаються в шліфованому папері, виробках із чавуну, шкірі та інших промислових матеріалах. Запропонований метод ґрунтується на відніманні фону в області Фур'є. Він передбачає, що розподіл частотних компонентів в просторі спектру є ізотропним і має форму, яка близька до кола. Знаходячи відповідний радіус в просторі спектру та встановлюючи на нуль частотні компоненти поза вибраним колом, відбираються періодичні, повторювані патерни статистичних текстур. У відновленому зображенні однорідні області у вихідному зображенні стають майже плоскими, але дефектна область залишається незмінною. За словами авторів, це перетворює виявлення дефектів в текстурах у просте завдання порогового вибору в нетекстурованих зображеннях. Цей поріг встановлюється за допомогою методу бінаризації статистичного керування процесами (SPC):

$$f_b(x, y) = \begin{cases} 255, & \text{if } \mu - k\sigma \leq f(x, y) \leq \mu + k\sigma \\ 0, & \text{otherwise} \end{cases}$$

де k – параметр керування, μ – середнє значення залишкового зображення, а σ^2 – його дисперсія. Области, встановлені на нуль, потім виявляються.

У роботі [7] зосереджуються на виявленні аномалій під час виробництва болтів і гайок. Метод розпочинається зі створення 2D нормалізованого розгорнутого зображення виробу, отриманого з послідовності часткових зображень виробу. Перший крок полягає в видаленні «фону», встановлюючи на нуль деякі коефіцієнти Фур'є. Фоновий малюнок, будучи дуже періодичним, практично повністю видаляється, після видалення великих коефіцієнтів Фур'є. Потім обчислюють середнє значення μ та дисперсію σ^2 залишкового зображення і воно бінаризується за допомогою методу SPC.

Модель фону на основі нейронних мереж. Загальна ідея полягає в тому, щоб вивчити модель фону, використовуючи нейронну мережу, навчену на нормальних даних.

Можливо, найважливішим застосуванням виявлення аномалій у промисловості є виявлення дефектів на поверхні. У роботі [9] пропонується ефективна техніка для виявлення дефектів на поверхні. Самоорганізаційна карта Кохонена (SOM) навчається на даних без дефектів при використанні двох основаних на гістограмах методах текстурного аналізу - матриць співвідношення та локальних бінарних шаблонів. Потім SOM може виявити аномалії, які, ймовірно, мають відмінний від зображень без дефектів розподіл ознак. Автори зауважують, що обидва методи демонструють задовільні результати, але локальні бінарні шаблони видаються ефективнішими з точки зору обчислювальної швидкості. Багато з методів виявлення дефектів на поверхні працюють схожим чином, вони обирають текстурні ознаки, а дефекти визначаються як ті, які недостатньо пояснюються моделлю ознак [1].

Генеративні нейронні мережі, зокрема, варіаційний автокодуювальник (VAE) часто використовуються у методах виявлення аномалій [1]. VAE складається з кодувальника, декодувальника та латентного простору. Кодувальник бере вхідні дані, зазвичай позначені як x , і відображає їх у латентний простір. Виходом кодувальника є середнє значення μ та логарифм дисперсії $\log(\sigma^2)$ мультіваріативного гаусівського розподілу, що представляє латентний простір:

$$q_\phi(z | x) = N(\mu_\phi(x), \sigma_\phi^2(x)),$$

де z – це зразок з латентного простору, а ϕ представляє параметри мережі кодувальника.

Після отримання середнього значення та дисперсії від кодера, вибирається зразок z з вивченого розподілу. Це досягається за допомогою трюку репараметризації, де z вибирається зі стандартного нор-

мального розподілу $N(0, I)$ та потім трансформується для отримання бажаного середнього значення та дисперсії.

$$z = \mu_\phi(x) + e \cdot \sigma_\phi^2(x),$$

де e – це зразок з $N(0, I)$.

Декодуювальник бере вибіркового латентний вектор z та відображає його назад у простір даних з метою відтворення вхідних даних x .

$$p_\theta(x | z) = N(\mu_\theta(z), \sigma_\theta^2(z)),$$

$$L(\phi, \theta; x) = -E_{q_\phi(z|x)}[\log(p_\theta(x | z))] + KL[q_\phi(z | x) \| N(0, I)],$$

де θ представляє параметри мережі декодера.

Під час навчання VAE прагне мінімізувати помилку відтворення та регулювати латентний простір. Для цього використовується функція втрат, що складається з втрат відтворення (обчислюється різниця між вихідними даними та відтвореними даними) та розбіжності Кульбака-Лейблера між навченим розподілом та стандартним нормальним розподілом.

Після навчання VAE на нормальних даних його можна використовувати для виявлення аномалій, оцінюючи помилку відтворення. Високі помилки відтворення характерні для екземплярів, які відхиляються від навченого нормального розподілу. У роботі [10] запропоновано навчити VAE й обчислити на його основі середню ймовірність відновлення, яка використовується як оцінка аномалії

Модель гладкого або фіксованого фону. Багато методів виявлення дефектів на поверхні належать до цієї категорії. Наприклад, загальна процедура виявлення дефектів у напівпровідниках полягає у використанні фіксованого еталонного чистого зображення та застосуванні певної процедури для виявлення різниці між спостережуваним зображенням і еталонним зображенням. Оскільки для різних мікросхем ймовірність наявності дефектів у тому ж самому місці дуже низька, можна отримати стандартне еталонне зображення, об'єднавши принаймні три зображення (шляхом заміни пікселів, розташованих у області дефекту, на пікселі, розташовані у відповідному місці іншого зображення) [1].

Ефективним методом виявлення аномалій у гладких матеріалах є метод, запропонований у [11]. У цій статті автори розробляють метод для повністю автоматичного виявлення аномалій на поверхнях коліс. Спочатку зображення коліс ресструються в фіксованому положенні. Для кожної ділянки колеса в заданому положенні розробляється лінійна детермінована фоновіа модель. Основа моделі складається з кількох поліномів низького ступеня в поєднанні з невеликою кількістю базисних функцій, вивчених як перші власні вектори методу головних компонент, застосованого до еталонних даних. Шуми, що виникають під час зйомки, точно моделюються за допомогою двопараметричного пуассонівського шуму. Параметри легко оцінюються з даних. Оцінка фону є проекцією кожного спостережуваного фрагмента у фоновий підпростір. Залишкове зображення, обчислене як різниця між вхідними і проекційними даними, може містити лише шум та аномалії. Отже, класичне статистичне тестування на норму залишкових значень кожного фрагмента надасть автоматичний поріг виявлення.

Висновки. Методи виявлення аномалій на основі моделей однорідного фону показують гарні результати та використовуються в широкому спектрі застосувань. Вони уникнуть пропозиції стохастичної моделі для часто складного фону, розраховуючи відстань до фону або виконуючи віднімання фону. Однак ця спрощення має свою ціну: деякі алгоритми важко узагальнювати для нових застосувань, і механізм прийняття рішення про виявлення, як правило, не має статистичного обґрунтування, за винятком деяких методів, наприклад, як у роботі [11].

Моделі фону локальної однорідності

Методи моделювання локальної однорідності, такі як методи центр-околу (*centr-surround*), часто використовуються для створення карт помітності. Їх основна ідея полягає в тому, що аномалії (або об'єкти на картах помітності) виникають як локальні події, які контрастують з оточуючими об'єктами.

У роботі [12] представлений загальний метод, який призначений для роботи з усіма типами зображень. Основна ідея полягає в тому, що вони намагаються оцінити ймовірність для фрагментів у зображенні, зумовлену областями, що оточують ці фрагменти. Метод оцінки використовує аналіз незалежних компонентів та перетворення Кархунена-Лоева (KLT) для зменшення розмірності та пошуку компактного представлення простору фрагменту та його околу, де елементи є якнайбільш незалежними. Аномалія визначається як фрагмент з низькою умовною ймовірністю відносно свого околу.

У роботі [13] було розширено використання методу опорних векторів (SVM) для розв'язання проблеми однокласової класифікації. Загальний концепт методу, що отримав назву Support Vector Data Description (SVDD), полягає у тому, що за умови, що лише малий обсяг навчальних даних представляє собою аномалії, можна оптимізувати функцію класифікатора для визначення, чи належить точка нормальному класу чи ні. Більш детально метод можна описати так. Нехай $X \subseteq R$ – простір вхідних даних і $\phi_k(x_i) : X \rightarrow Hk$ – функція відображення з ядром $k : X \times X \rightarrow [0, +\infty)$. Hk – простір ознак. Нехай вхідний набір даних задано як $D = \{x_1, \dots, x_n\}$ з $x_i \in X$. Основною метою SVDD є знаходження гіперсфери мінімального розміру, так щоб містити більшість об'єктів даних у Hk . Задачу SVDD можна описати так:

$$\min R^2 + \frac{1}{\nu n} \sum_{i=1}^n \xi_i,$$

$$s.t. \quad \|\phi_k(x_i) - a\|^2 \leq R^2 + \xi_i \quad \forall i, \xi_i \geq 0,$$

де R і a – відповідно радіус і центр сфери; ξ_i – змінна послаблення, яка дозволяє деяким зразкам даних бути за межами сфери; $\nu \in (0, 1]$ – це штрафний параметр, який контролює компроміс між обсягом сфери та кількістю відхилених зразків даних, таким чином забезпечуючи ефективний спосіб вимірювання частки аномальних даних для навчання.

У роботі [14] представлений підхід до виявлення аномалій з використанням глибокого навчання, який надихнувся тими ж ідеями. Метод, названий Deep SVDD, тренує глибоку нейронну мережу, щоб виділяти нормальні екземпляри даних та створювати навколо них найменшу можливу описову область. Аномаліями будуть вважатися точки що віддалені від цієї області Цей метод дозволяє ефективно виявляти аномалії у високорозмірних даних.

Зазвичай ці методи створюють карту помітності, оскільки такі карти мають простий і ефективний механізм для вимірювання рідкості. Однак вони не надають механізму визначення порогового значення виявлення аномалії. Декілька з оглянутих вище методів центр-околу намагаються виправити це, але це призводить до значного збільшення обчислювальної складності методу через потребу у визначенні локальної стохастичної моделі як для центру, так і для околу. Як наслідок, зазвичай доводиться використовувати двокласову класифікацію зі значно більшою складністю методології.

Моделі фону на основі розрідженості

Одним із недавніх не параметричних напрямків виявлення аномалій є навчання розрідженого словника, що представляє фон (тобто нормальність), та визначає аномалії за їхньою не розрідженістю. У роботі [15] запропонований метод побудови карт помітності за допомогою поєднання виразності образів та виразності кольорів при обчисленні статистичних характеристик фрагментів зображення. Таке поєднання дозволило покращити точність знаходження унікальних фрагментів зображення, забезпечуючи також високу швидкість обробки.

У роботі [16] автори представили низькорангове та розріджене тензорне представлення даних гіперспектральних зображень на основі спостереження того, що об'єм цих даних часто має низькорангову структуру через значні кореляції в спектрах сусідніх пікселів. У роботі [17] фонову моделлю є навчений словник фрагментів з бази даних без аномалій. Хоча метод виглядає загальним, автори розглянули задачу виявлення аномалій в складних однорідних текстурах, таких як мікрволокна. Модель фрагментів побудована як словник D , отриманий з усіх фрагментів p_i шляхом мінімізації

$$J_\lambda(X, D) = \|DX - P\|_F^2 + \lambda \|X\|_1,$$

де P – матриця, стовпцями якої є навчальні фрагменти; словник D представлений у вигляді матриці, де стовпці – це елементи словника; X – це матриця, де i -й стовпець представляє коефіцієнти фрагмента p_i у D . Помилка підгонки даних вимірюється нормою Фробеніуса першої складової формули. Норму l_1 матриці X слід розуміти як суму абсолютних значень усіх його коефіцієнтів.

Після отримання моделі фрагментів, той самий функціонал використовується для пошуку розрідженого представлення x для кожного тестового фрагмента p шляхом мінімізації

$$J_\lambda(X) = \left\| \hat{D}X - p \right\|^2 + \lambda \|X\|_1.$$

Для відповіді на питання, як з цієї мінімізації визначити, що тестовий фрагмент p є аномальним автори пропонують прив'язати до кожного фрагменту пару значень

$$\phi(p) = \left(\left\| \hat{D}X - p \right\|^2, \lambda \|X\|_1 \right).$$

Перший компонент визначає, наскільки добре фрагмент представлений у словнику D . Другий компонент вимірює розрідженість (і, отже, адекватність) цього представлення. Емпірична двовимірна гауссова модель (μ, Σ) отримується для всіх фрагментів навчального набору даних без аномалій. Відповідно до цього можна визначити область нормальності для моделі фрагментів шляхом встановлення порогу γ відстані Маханалобіса зразків до цієї гауссової моделі.

Великою перевагою моделей фону, які передбачають розрідженість, є те, що вони роблять дуже загальне структурне припущення щодо фону і створюють варіаційну модель, яка залежить лише від одного або двох параметрів, а саме від відносної ваги, яку вони надають термінам енергії, яку потрібно мінімізувати.

Моделі фону на основі нелокальної самоподібності

Принцип нелокальної самоподібності застосовується в багатьох методах відновлення зображень, зокрема в методах зменшення шуму у зображенні, таких як білатеральний фільтр або нелокальні середні.

Основне припущення цієї загальної моделі фону, яке застосовується до більшості зображень, полягає в тому, що в нормальних даних кожен фрагмент зображення належить до щільного кластеру в просторі фрагментів зображення. Аномалії, навпаки, знаходяться далеко від своїх найближчих сусідів. Це визначення аномалії може бути реалізоване шляхом кластеризації фрагментів зображення (аномалії виявляються, якщо вони знаходяться далеко від центроїда свого власного кластера) або за допомогою пошуку найближчих сусідів, що призводить до прямого вимірювання рідкості.

Модель, яка інспірується нелокальними середніми. У роботі [18] у детекторі аномалій, що базується на нелокальній самоподібній моделі фону, пропонується вимірювати рідкості як обернену функцію подібності. У кожному пікселі i дескриптор F_i вимірює схожість пікселя до свого околу. Потім цей дескриптор F_i порівнюється з відповідними дескрипторами пікселів у більш широкому околі. Помітність пікселя i вимірюється за допомогою

$$s_i = \frac{1}{\sum_{j=1}^N e^{\left(\frac{\rho(F_i, F_j) - 1}{h^2} \right)}}, \quad (1)$$

де $\rho(F_i, F_j)$ – косинусна відстань між двома дескрипторами, F_i – локальна ознака, а F_j для $j = 1, \dots, N$, N найближчих ознак до F_i в околі, та $0 < h < 1$ є параметром.

Якщо всі F_j не корелюються з F_i , всі експоненти в (1) будуть малими, а отже, помітність буде високою. Якщо натомість лише один F_j добре корелює з F_i , помітність буде близькою до одиниці, і якщо k різних F_j добре корелюють з F_i , помітність i -го пікселя S_i приблизно дорівнюватиме $1/k$. Недоліком методу є відсутність чіткого механізму встановлення порогу помітності для виявлення аномалій.

У роботі [19] наведений метод в значній мірі інспірований нелокальними середніми: для фрагменту зображення p , параметра схожості h^2 і набору n сусідніх фрагментів (p_j) , аномалія виявляється, коли

$$\sum_{j=1}^N e^{\left(\frac{-\|p - p_j\|_2^2}{h^2} \right)} \leq \tau,$$

де τ – емпіричний параметр.

У роботі [20] автори запропонували моделювання фону на залишковому зображенні, отриманому шляхом віднімання фону. Так як, згадані вище методи, що базуються на самоподібності, припускають, що фон є самоподібним, то для його видалення застосовується модифікація алгоритму нелокальних середніх. Моделювання фону полягає в заміні кожного фрагмента зображення середнім арифметичним з найбільш схожих фрагментів. Для запобігання збереженню аномалій із деякою самоподібною структурою в фоні ці схожі фрагменти шукають за межами «охоронної області зображення», центрованої на фрагменті, що розглядається.

Модель фону на основі ядра PCA. Метод ядра головних компонент (kernel PCA) зменшує обчислювальні витрати завдяки рівномірній випадковій вибірці невеликої частини даних, які з високою імовірністю не містять аномалій. Метод ядра головних компонент для виявлення аномалій, запропонований у роботі [21], визначає гауссове ядро на наборі даних x_i , $i = 1 \dots M$, встановлюючи

$$k(x_i, x_j) = e^{-\frac{1}{h^2} \|x_i - x_j\|^2}, \quad i, j = 1, \dots, M.$$

Передбачається, що це «ядро» представляє скалярний добуток між векторами ознак вибірок $\Phi(x_i)$ та $\Phi(x_j)$ в просторі високої розмірності (де Φ визначається неявно). Суть методу полягає в тому, що аналіз головних компонент виконується неявно в цьому просторі ознак з використанням обчислень, які включають лише k . Відстань між $\Phi(z)$ та $\Phi_0 = \sum_{i=1}^M \Phi(x_i)$ можливо обчислити, використовуючи лише k :

$$p(z) = k(z, z) - \frac{2}{M} \sum_{i=1}^M k(z, x_i) + \frac{1}{M^2} \sum_{i,j=1}^M k(x_i, x_j).$$

Оскільки перший член дорівнює одиниці, а останній член є сталим, випливає, що

$$p(z) = C - \frac{2}{M} \sum_{i=1}^M k(z, x_i),$$

що є протилежним до оцінки щільності Парзена вибірки з використанням гауссового ядра зі стандартним відхиленням h . Таким чином, аномалії будуть виявлені шляхом встановлення порогового значення на цій щільності, що обчислена з фонових вибірок. Можливо виконати більш повне віднімання фону, віднявши його перші q головні компоненти.

Висновки щодо самоподібності. Подібно до розрідженості, самоподібність є потужною якісною моделлю, але недоліком є те, що у більшості її застосуваннях, відсутній жорсткий механізм для визначення порогу виявлення аномалій. Одним з винятків є робота [20], яка розширює метод з роботи [6] і, таким чином, отримує жорсткий поріг виявлення аномалій за умови, що залишкове зображення є гауссовим випадковим полем.

Висновки

1. Оскільки аномалії досить важко змоделювати, у центрі уваги більшості методів виявлення аномалій знаходиться фонові модель. Методи, які використовують стохастичну модель фону, є досить ефективними при обробці зображень, які належать до обмеженого класу однорідних об'єктів, таких як текстиль або гладкофарбовані поверхні. Такі методи отримують пороги виявлення на основі оціненої функції щільності ймовірності. Однак, стохастичне моделювання фону не може бути застосоване до довільних зображень. З цієї ж причини однорідні моделі фону мають обмежену застосовність, крім того вони не мають статистично обґрунтованих механізмів для визначення порогів виявлення аномалій. Методи центр-околу успішно використовуються для підвищення яскравості, але, загалом, вони знову ж не мають механізмів виявлення аномалій. Методи центр-околу, які пропонують поріг виявлення, повинні оцінювати дві стохастичні моделі, одну для центру і одну для околу, тому є досить складними для практичного використання. Останні дві категорії розглянутих методів, а саме ті що використовують моделі розрідженості та самоподібності мають велику перевагу - універсальність: їх можна застосовувати до всіх фонових зображень, однорідних чи неоднорідних, стохастичних чи не стохастичних..

2. Для застосувань виявлення аномалій рекомендовано використовувати методи, у яких модель фону найкраще описує очікуваний фон, на якому відсутні аномалії, оскільки це, як правило, призводить до найкращої ефективності. Крім того, для того, щоб методи стали універсальними, потрібно контролювати кількість хибних виявлень. Насправді, більшість методів що розглядалися, як правило, пропонують емпіричний поріг.

3. Ефективна універсальна модель повинна:

- а) використовувати лише самоподібну чи розріджену модель фону;
- б) обробляти залишкове зображення як стохастичний процес для виявлення аномалій, як аномалій у кольоровому шумі;
- в) попередньо обробляти (вибілювати) залишкове зображення перед виявленням аномалій.

Список літератури

- [1] Ghamry, Fatma M., et al. "Survey of Image Anomaly Detection." (2022). <https://assets.researchsquare.com/files/rs-1890977/v1/2ce2b06a-890a-428d-810e-3ad8173caf7b.pdf?c=1660897768>
- [2] Du, B., Zhang, L.: Random-selection-based anomaly detector for hyperspectral imagery. IEEE Transactions on Geoscience and Remote sensing 49(5), 1578-1589 (2011)

- [3] Goldman, A., Cohen, I.: Anomaly detection based on an iterative local statistics approach. *Signal Processing* 84(7), 1225-1229 (2004)
- [4] Cohen, F.S., Fan, Z., Attali, S.: Automated inspection of textile fabrics using textural models. *IEEE Transactions on Pattern Analysis & Machine Intelligence* (8), 803-808 (1991)
- [5] Xie, X., Mirmehdi, M.: Texems: Texture exemplars for defect detection on random textured surfaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29(8), 1454-1464 (2007)
- [6] Grosjean, B., Moisan, L.: A-contrario detectability of spots in textured backgrounds. *Journal of Mathematical Imaging and Vision* 33(3), 313-337 (2009)
- [7] Perng, D.B., Chen, S.H., Chang, Y.S.: A novel internal thread defect auto-inspection system. *The International Journal of Advanced Manufacturing Technology* 47(5-8), 731-743 (2010)
- [8] Tsai, D.M., Huang, T.Y.: Automated surface inspection for statistical textures. *Image and Vision computing* 21(4), 307-323 (2003)
- [9] Iivarinen, J.: Surface defect detection with histogrambased texture features. In: *Intelligent robots and computer vision xix: Algorithms, techniques, and active vision*, vol. 4197, pp. 140-146. *International Society for Optics and Photonics* (2000)
- [10] An, J.: Variational Autoencoder based Anomaly Detection using Reconstruction Probability. *Arxiv* (2016)
- [11] Tout, K., Cogranne, R., Retraint, F.: Fully automatic detection of anomalies on wheels surface using an adaptive accurate model and hypothesis testing theory. In: *2016 24th European Signal Processing Conference*, pp. 508-512. *IEEE* (2016)
- [12] Honda, T., Nayar, S.K.: Finding "anomalies" in an arbitrary image. In: *2001. IEEE International Conference on Computer Vision*, vol. 2, pp. 516-523. *IEEE* (2001)
- [13] Tax, D.M., Duin, R.P.: Support vector data description. *Machine learning* 54(1), 45-66 (2004)
- [14] Ruff, L., Gornitz, N., Deecke, L., Siddiqui, S.A., Vandermeulen, R., Binder, A., Muller, E., Kloft, M.: Deep one-class classification. In: *International Conference on Machine Learning*, pp. 4390-4399 (2018)
- [15] Margolin, R., Tal, A., Zelnik-Manor, L.: What makes a patch distinct? In: *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1139-1146 (2013)
- [16] Li, S., Wang, W., Qi, H., Ayhan, B., Kwan, C., Vance, S.: Low-rank tensor decomposition based anomaly detection for hyperspectral imagery. In: *2015 IEEE International Conference on Image Processing*, pp. 4525-4529 (2015)
- [17] Boracchi, G., Carrera, D., Wohlberg, B.: Novelty detection in images by sparse representations. In: *2014 IEEE Symposium on Intelligent Embedded Systems*, pp. 47-54. *IEEE* (2014)
- [18] Seo, H.J., Milanfar, P.: Static and space-time visual saliency detection by self-resemblance. *Journal of vision* 9(12), 15-15 (2009)
- [19] Zontak, M., Cohen, I.: Defect detection in patterned wafers using anisotropic kernels. *Machine Vision and Applications* 21(2), 129-141 (2010)
- [20] Davy, A., Ehret, T., Morel, J.M., Delbraccio, M.: Reducing anomaly detection in images to detection in noise. In: *2018 IEEE International Conference on Image Processing*, pp. 1058-1062. *IEEE* (2018)
- [21] Hoffmann, H.: Kernel pca for novelty detection. *Pattern recognition* 40(3), 863-874 (2007)

Стаття надійшла: 18.01.2024

References

- [1] Ghamry, Fatma M., et al. "Survey of Image Anomaly Detection." (2022). <https://assets.researchsquare.com/files/rs-1890977/v1/2ce2b06a-890a-428d-810e-3ad8173caf7b.pdf?c=1660897768>
- [2] Du, B., Zhang, L.: Random-selection-based anomaly detector for hyperspectral imagery. *IEEE Transactions on Geoscience and Remote sensing* 49(5), 1578-1589 (2011)
- [3] Goldman, A., Cohen, I.: Anomaly detection based on an iterative local statistics approach. *Signal Processing* 84(7), 1225-1229 (2004)
- [4] Cohen, F.S., Fan, Z., Attali, S.: Automated inspection of textile fabrics using textural models. *IEEE Transactions on Pattern Analysis & Machine Intelligence* (8), 803-808 (1991)
- [5] Xie, X., Mirmehdi, M.: Texems: Texture exemplars for defect detection on random textured surfaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29(8), 1454-1464 (2007)
- [6] Grosjean, B., Moisan, L.: A-contrario detectability of spots in textured backgrounds. *Journal of Mathematical Imaging and Vision* 33(3), 313-337 (2009)
- [7] Perng, D.B., Chen, S.H., Chang, Y.S.: A novel internal thread defect auto-inspection system. *The International Journal of Advanced Manufacturing Technology* 47(5-8), 731-743 (2010)
- [8] Tsai, D.M., Huang, T.Y.: Automated surface inspection for statistical textures. *Image and Vision computing* 21(4), 307-323 (2003)

- [9] Iivarinen, J.: Surface defect detection with histogrambased texture features. In: Intelligent robots and computer vision xix: Algorithms, techniques, and active vision, vol. 4197, pp. 140-146. International Society for Optics and Photonics (2000)
- [10] An, J.: Variational Autoencoder based Anomaly Detection using Reconstruction Probability. Arxiv (2016)
- [11] Tout, K., Cогranne, R., Retraint, F.: Fully automatic detection of anomalies on wheels surface using an adaptive accurate model and hypothesis testing theory. In: 2016 24th European Signal Processing Conference, pp. 508-512. IEEE (2016)
- [12] Honda, T., Nayar, S.K.: Finding " anomalies" in an arbitrary image. In: 2001. IEEE International Conference on Computer Vision, vol. 2, pp. 516-523. IEEE (2001)
- [13] Tax, D.M., Duin, R.P.: Support vector data description. Machine learning 54(1), 45-66 (2004)
- [14] Ruff, L., Gornitz, N., Deecke, L., Siddiqui, S.A., Vandermeulen, R., Binder, A., Muller, E., Kloft, M.: Deep one-class classification. In: International Conference on Machine Learning, pp. 4390-4399 (2018)
- [15] Margolin, R., Tal, A., Zelnik-Manor, L.: What makes a patch distinct? In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 1139-1146 (2013)
- [16] Li, S., Wang, W., Qi, H., Ayhan, B., Kwan, C., Vance, S.: Low-rank tensor decomposition based anomaly detection for hyperspectral imagery. In: 2015 IEEE International Conference on Image Processing, pp. 4525-4529 (2015)
- [17] Boracchi, G., Carrera, D., Wohlberg, B.: Novelty detection in images by sparse representations. In: 2014 IEEE Symposium on Intelligent Embedded Systems, pp. 47-54. IEEE (2014)
- [18] Seo, H.J., Milanfar, P.: Static and space-time visual saliency detection by self-resemblance. Journal of vision 9(12), 15-15 (2009)
- [19] Zontak, M., Cohen, I.: Defect detection in patterned wafers using anisotropic kernels. Machine Vision and Applications 21(2), 129-141 (2010)
- [20] Davy, A., Ehret, T., Morel, J.M., Delbracio, M.: Reducing anomaly detection in images to detection in noise. In: 2018 IEEE International Conference on Image Processing, pp. 1058-1062. IEEE (2018)
- [21] Hoffmann, H.: Kernel pca for novelty detection. Pattern recognition 40(3), 863-874 (2007)

Відомості про авторів

Маслій Роман Васильович – к.т.н., доцент, доцент кафедри автоматизації та інтелектуальних інформаційних технологій

Maslii Roman Vasyliovych – candidate of technical sciences, associate professor in the department of automation and intelligent information technologies

Гармаш Володимир Володимирович – к.т.н., доцент, доцент кафедри автоматизації та інтелектуальних інформаційних технологій

Garmash Volodymyr Volodymyrovych – candidate of technical sciences, associate professor in the department of automation and intelligent information technologies

Ковальчук Петро Петрович – аспірант кафедри автоматизації та інтелектуальних інформаційних технологій

Kovalchuk Petro Petrovych – postgraduate, department of automation and intelligent information technologies

Кабачій Владислав Володимирович – к.т.н., доцент, доцент кафедри автоматизації та інтелектуальних інформаційних технологій

Kabachii Vladyslav Volodymyrovych – candidate of technical sciences, associate professor in the department of automation and intelligent information technologies

R.V. Maslii, V. V. Garmash, P. P. Kovalchuk, V. V. Kabachii

ANALYSIS OF ANOMALY DETECTION METHODS IN IMAGES

Vinnitsia National Technical University, Vinnitsia

УДК 519.86(075.8)

В. В. Колодний, В. В. Зубко

МЕТОД ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РАНЖУВАННЯ АЛЬТЕРНАТИВ НА ОСНОВІ ВІЗУАЛЬНИХ ТЕРНАРНИХ ПОРІВНЯНЬ

Вінницький національний технічний університет, Вінниця

Анотація. Розроблено новий метод та відповідну інформаційну технологію ранжування альтернатив, які базуються на проведенні та подальшому аналізі візуальних тернарних порівнянь і не вимагають від експерта або децидента ніяких числових або вербальних оцінок. Візуальні тернарні порівняння – це розташування трійки альтернатив на полицях переважань за принципом «чим краща альтернатива, тим вище її розташування». Для того, щоб процес виявлення переважань був надійним, наочним та активізував швидку систему інтуїтивного мислення, дециденту або експерту пропонується розташувати пред'явлені альтернативи на екрані комп'ютера згідно з його вподобаннями. Описано подальшу числову інтерпретацію візуальних тернарних порівнянь та способи отримання кардинальних результуючих ранжувань та ординальних результуючих ранжувань всієї множини альтернатив. Для підвищення надійності результатів ранжування було запропоновано використовувати дві різні форми числової інтерпретації візуальних тернарних порівнянь: за методом рядкових сум (адитивна згортка) і за шкалою Сааті (мультиплікативна згортка). В розробленому методі пом'якшується вимога щодо транзитивності переважань, а розширений контекст порівнянь альтернатив статистично згладжує незначні похибки і дозволяє діагностувати грубі помилки. Описано інформаційну технологію ранжування альтернатив на основі візуальних тернарних порівнянь, яка складається з дев'ятого взаємопов'язаних між собою етапів. Розглянуто приклад застосування розробленого методу та інформаційної технології з випадком виявлення і виправлення суперечливих тернарних порівнянь. Розроблений метод та відповідна інформаційна технологія є перспективними для використання в різноманітних галузях, що потребують ранжування альтернатив при якісному і кількісному оцінюванні (прийняття рішень, психологія, педагогіка, менеджмент, маркетинг, експертні оцінювання тощо).

Ключові слова: метод ранжування альтернатив, інформаційна технологія, візуальні тернарні порівняння, швидке інтуїтивне мислення, полиці переважань, суперечливі порівняння, ординальні ранжування, кардинальні ранжування.

Abstract. A new method and corresponding information technology of ranging alternatives have been developed, which are based on conducting and further analysis of visual ternary comparisons and do not require any numerical or verbal evaluations from an expert or decision maker. Visual ternary comparisons are the arrangement of three alternatives on the shelves of preferences according to the principle "the better the alternative is, the higher its location is." In order for the process of identification of preferences to be reliable, visual and to activate a fast system of intuitive thinking, the decision-maker or expert is suggested to arrange the presented alternatives on the computer screen according to his preferences. Further numerical interpretation of visual ternary comparisons and methods of obtaining cardinal resulting rankings and ordinal resulting rankings of the entire set of alternatives are described. To increase the reliability of ranking results, it was proposed to use two different forms of numerical interpretation of visual ternary comparisons: the method of line sums (additive convolution) and the Saaty scale (multiplicative convolution). In the developed method, the requirement for the transitivity of preferences is mitigated, and the expanded context of comparisons of alternatives statistically smoothes minor errors and allows to diagnose gross errors. Information technology for ranging alternatives based on visual ternary comparisons which consists of nine interconnected stages is described. An example of the application of the developed method and information technology in the case of identification and correction of conflicting ternary comparisons is considered. The developed method and corresponding information technology are promising for use in various fields that require ranging of alternatives in qualitative and quantitative evaluation (decision-making, psychology, pedagogy, management, marketing, expert evaluations etc.).

Key words: method of ranging alternatives, information technology, visual ternary comparisons, fast intuitive thinking, preference shelves, conflicting comparisons, ordinal rankings, cardinal rankings.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-23-31>.

Вступ

Одними з найбільш складних задач прийняття рішень є задачі з цільовою і критеріальною невизначеністю. Основним етапом процесу розв'язання таких актуальних задач є отримання та структурування інформації про переважання децидента. Існує дуже багато форм і способів отримання цієї інформації [1], але переважна більшість з них вимагає від децидентів певних числових і/або вербальних оцінок. В більшості випадків, коли дециденти не є фахівцями в галузі теорії прийняття рішень і системного аналізу, їм буває складно зорієнтуватись у цих способах та адекватно і точно описати свої вподобання.

Під *децидентом* в цій статті автори розуміють **особу, що приймає рішення**, або **експерта**, яким потрібно впорядкувати певні альтернативи за якістю або будь-якою іншою ознакою, спираючись на власний досвід і інтуїцію.

Задачі ранжування альтернатив повсякчас виникають при прийнятті різноманітних рішень і експертних оцінюваннях. Найбільш дослідженими і вживаними методами в цій галузі є методи парних порівнянь [1, 2].

Понад двадцять років тому виникла ідея застосування тернарних тривірневих ранжувань (ТТР) для виявлення переважань [3]. На основі цієї ідеї були розроблені методи та відповідні інформаційні технології візуалізації і виявлення переважань, тобто ранжування альтернатив [4-9].

Широке впровадження цих методів та інформаційних технологій в навчальному процесі ВНТУ протягом багатьох років засвідчило можливість легко, швидко і надійно «вимірювати» найрізноманітніші вподобання студентів: рівень гумору в жартах, душевність музики, масштабність історичної постаті, краю шахових комбінацій тощо. Важливо, що при виконанні завдань такого типу студенти не висловлювали ніякої вербальної або числової інформації щодо своїх вподобань, а використовували тільки своє власне візуальне швидке інтуїтивне мислення [10] і доступний пристрій (ноутбук, мобільний телефон, планшет). Слід відзначити, що студенти проявляли зацікавленість і надавали явну перевагу застосуванню інформаційних технологій на основі візуальних тернарних порівнянь перед традиційними методами чисельного парного порівняння.

Результуючі кардинальні ранжування альтернатив, отримані за різними алгоритмами, виявилися досить близькими, а результуючі ординальні ранжування співпадали в переважній більшості випадків.

Це дало можливість стверджувати про надійність та точність розроблених авторами інформаційних технологій.

Актуальність

Задачі ранжування альтернатив досить часто виникають при прийнятті різноманітних рішень в умовах цільової і критеріальної невизначеності, а також при якісному і кількісному експертному оцінюванні. Розповсюджена практика застосування методу безпосереднього числового оцінювання альтернатив та багатьох інших методів [1, 2] мало відповідає психічним особливостям децидентів [10, 11], тому розробка і застосування нових ефективних методів ранжування альтернатив є актуальними.

Мета

Метою даної статті є підвищення ефективності процесів ранжування альтернатив при прийнятті рішень і експертних оцінюваннях на основі розробки нового методу, що базується на візуальних тернарних порівняннях, та відповідної нової інформаційної технології.

Опис методу ранжування альтернатив на основі візуальних тернарних порівнянь

Як відомо, застосування математики в теорії прийняття рішень ґрунтується на ізоморфізмі відношень

$$\langle \text{краще-гірше} \rangle \Leftrightarrow \langle \text{більше-менше} \rangle. \quad (1)$$

Це потребує обов'язкового перетворення інформації про переважання децидента, поданої природною мовою, в числову форму. На жаль, не завжди ці перетворення є психологічно коректними і інтуїтивно зрозумілими, особливо в тих випадках, коли дециденти є не «еконами», а «гуманами» [11]. Це призводить до того, що матриці порівнянь альтернатив заповнюються числами, які не в повній мірі відповідають справжнім переважаням децидента, хоча створюють ілюзію точності і математичної строгості багатьох існуючих методів прийняття рішень.

Оскільки сучасна комп'ютерна техніка та мобільні пристрої з легкістю дозволяють користувачам швидко переміщувати певні об'єкти на площині екрану, було запропоновано покращити процеси виявлення переважань децидентів щодо альтернатив шляхом їх візуалізації.

Для унаочнення і полегшення процесу вираження децидентами своїх вподобань було запропоновано візуалізацію, ґрунтовану на ізоморфізмі виду

$$\langle \text{краще-гірше} \rangle \Leftrightarrow \langle \text{вище-нижче} \rangle, \quad (2)$$

який виявився більш інтуїтивно зрозумілим, ніж (1).

Подальша числова інтерпретація візуального порівняння за ізоморфізмом

$$\langle \text{вище-нижче} \rangle \Leftrightarrow \langle \text{більше-менше} \rangle \quad (3)$$

має проводитися автоматично без залучення децидента. Ця інтерпретація є також зрозумілою і більш точною, ніж (1).

Виявилося, що візуалізація порівнянь альтернатив сприяє мінімізації когнітивних зусиль децидента.

Розроблений метод належить до нового перспективного класу методів ранжування **VisTerComp** [12]. Його можна розглядати як розвиток і вдосконалення методу некрітеріального структурування множини альтернатив за допомогою аналізу ТТР [4] та методу аналізу тривірневих ранжувань (МАТР) [5].

В тривірневих ранжуваннях на додаток до широко вживаних відношень **переваги** (\succ) і **еквівалентності** (\sim) вводиться відношення **сильної переваги** ($\succ\!\succ$) [3]. Відношення сильної переваги має сенс «набагато краще», «безумовно переважає» і дає змогу дециденту «масштабувати» свої переважання. Це

дозволяє повніше та точніше використовувати можливості децидентів, які залишаються незадіяними в традиційних методах прийняття рішень.

Для того, щоб процес виявлення переважань був надійним, наочним та активізував швидку систему інтуїтивного мислення децидента [10], були використані аналогії з шаблями або з полицями шафи. Дециденту пропонується розташувати запропоновані альтернативи на екрані комп'ютера згідно з його вподобаннями. Візуальні тернарні порівняння (ВТП) – це розташування трійки альтернатив на шаблях або на полицях переважань за принципом «**чим краща альтернатива, тим вище її розташування**». Як правило, на проведення одного ВТП дециденту вистачає декілька секунд, і воно не є складнішим за парне порівняння. Навпаки, досить часто дециденти проявляли вищу зацікавленість саме до ВТП.

Розглянемо різні конфігурації тернарних порівнянь з використанням відношень \sim , \succ , \succcurlyeq (рис. 1).

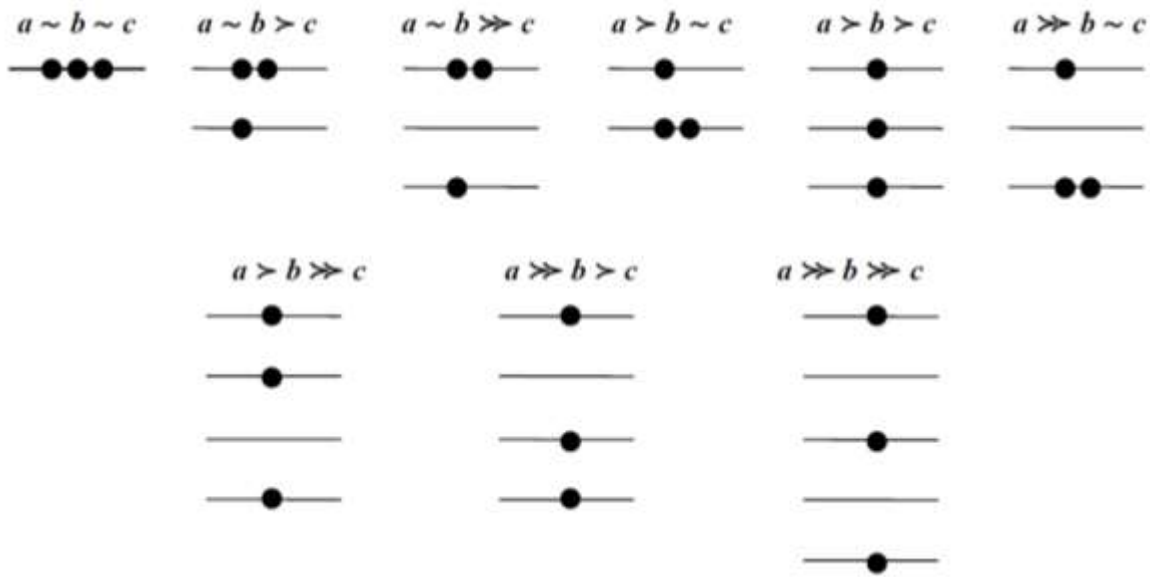


Рисунок 1 – Візуалізація різних конфігурацій ВТП на шаблях переважань

Очевидно, що отримавши результати одного ВТП, ми тим самим отримуємо три парних порівняння альтернатив. Розглянемо всі випадки породжених парних порівнянь (ППП):

$a \sim b \sim c$	\Rightarrow	$a \sim b;$	$b \sim c;$	$a \sim c;$
$a \succ b \succ c$	\Rightarrow	$a \succ b;$	$b \succ c;$	$a \succ c;$
$a \sim b \succ c$	\Rightarrow	$a \sim b;$	$b \succ c;$	$a \succ c;$
$a \succcurlyeq b \sim c$	\Rightarrow	$a \succcurlyeq b;$	$b \sim c;$	$a \succcurlyeq c;$
$a \sim b \succcurlyeq c$	\Rightarrow	$a \sim b;$	$b \succcurlyeq c;$	$a \succcurlyeq c;$
$a \succ b \succcurlyeq c$	\Rightarrow	$a \succ b;$	$b \succcurlyeq c;$	$a \succcurlyeq c;$
$a \succ b \sim c$	\Rightarrow	$a \succ b;$	$b \sim c;$	$a \succ c;$
$a \succcurlyeq b \succ c$	\Rightarrow	$a \succcurlyeq b;$	$b \succ c;$	$a \succcurlyeq c;$
$a \succcurlyeq b \succcurlyeq c$	\Rightarrow	$a \succcurlyeq b;$	$b \succcurlyeq c;$	$a \succcurlyeq c.$

Використання розробленого методу створює певну надлишковість, тому що PPP між будь-якими двома альтернативами будуть утворюватися $N-2$ разів, де N – загальна кількість альтернатив в множині. Ця **надлишковість має позитивний ефект**, оскільки відповідає відомому принципу Терстоуна, згідно з яким для отримання надійних результатів недостатньо одного парного порівняння альтернатив. Крім цього, врахування парних порівнянь в різних контекстах третьої альтернативи дозволяє статистично згладжувати можливі неточності децидентів щодо оцінювання власних переважань.

Слід зазначити, що ППП створюються та аналізуються автоматично при виконанні кожного ВТП і не потребують від децидентів додаткових когнітивних зусиль.

На основі аналізу ППП щодо розходжень між оцінками альтернатив, які були зроблені децидентом в різних контекстах, можна виділити припустимі розбіжності та неприпустимі суперечливості в ВТП.

Припустимими розбіжностями пропонується вважати відмінності виду

$$a \sim b; a > b \quad \text{та} \quad a > b; a \gg b, \quad (4)$$

тобто заміну в ППП на «сусіднє» відношення, а всі інші відмінності вважаються **неприпустимими суперечливостями**. Важливо відзначити, що розроблений метод не потребує безумовного виконання формальної умови транзитивності переважань децидентів, яка, як відомо, досить часто порушується в реальному житті [1, 10, 11]. Достатньо транзитивності з точністю до «сусіднього» відношення.

Припустимі (незначні) розбіжності можуть бути обумовлені похибками, притаманними процесам вимірювання в психології та впливом контексту вибору (ефект різного масштабування), і не вимагають корегування, а неприпустимі суперечливості свідчать про нерациональність або некомпетентність децидента і мають бути виправлені. Після виправлення неприпустимих суперечливостей з урахуванням усієї наявної інформації обчислюються результуючі кардинальні ранжування заданої множини альтернатив.

Для підвищення надійності результатів ранжування було запропоновано використовувати дві різні форми числової інтерпретації ВТП: за методом рядкових сум (**адитивна згортка**) і за шкалою Сааті (**мультиплікативна згортка**) [1]. В обох цих формах потрібно використовувати 9 пронумерованих знизу догори рівнів (рангів альтернатив). Під час проведення ВТП децидент розташовує кожну з трійки альтернатив a_i на будь-якому з дев'яти рівнів. Ранг альтернативи a_i у ВТП будемо позначати $r(a_i)$.

Розглянемо числову інтерпретацію ВТП за **методом рядкових сум** з використанням запропонованої бальної структури $\{-2; -1; 0; +1; +2\}$. При аналізі кожного ППП в таблицю B заноситься відповідний бал за такими правилами:

$$\text{якщо} \quad r(a_i) = r(a_j), \quad \text{то} \quad a_i \sim a_j \Rightarrow b_{ij} = 0; b_{ji} = 0; \quad (5)$$

$$\text{якщо} \quad r(a_i) - r(a_j) = 1, \quad \text{то} \quad a_i > a_j \Rightarrow b_{ij} = 1; b_{ji} = -1; \quad (6)$$

$$\text{якщо} \quad r(a_i) - r(a_j) > 1, \quad \text{то} \quad a_i \gg a_j \Rightarrow b_{ij} = 2; b_{ji} = -2. \quad (7)$$

Після знаходження алгебраїчної суми кожного рядка таблиці B отримаємо числову оцінку відповідних альтернатив. Отримане результуюче кардинальне ранжування альтернатив буде **центрованим**.

Розглянемо числову інтерпретацію ВТП за **шкалою Сааті**. Елементи s_{ij} таблиці S відносних пріоритетів альтернатив a_i та a_j обчислюються за такими правилами:

$$\text{якщо} \quad r(a_i) \geq r(a_j), \quad \text{то} \quad s_{ij} = r(a_i) - r(a_j) + 1; \quad s_{ji} = \frac{1}{s_{ij}}; \quad (8)$$

$$\text{якщо} \quad r(a_i) < r(a_j), \quad \text{то} \quad s_{ji} = r(a_j) - r(a_i) + 1; \quad s_{ij} = \frac{1}{s_{ji}}; \quad (9)$$

$$1 \leq r(a_i) \leq 9, \quad 1 \leq r(a_j) \leq 9. \quad (10)$$

Після знаходження середнього геометричного в кожному рядку таблиці S та нормування отримаємо результуюче **нормоване** кардинальне ранжування альтернатив.

Слід зазначити, що таблиці B і S внаслідок тернарності ВТП не є матрицями, а являють собою тривимірні масиви, але для наочності у виразах (5)-(9) пропущено третій індекс масиву k .

Перевірка ВТП на суперечливість полягає в знаходженні мінімуму і максимуму поточних значень в кожній клітинці таблиці B і перевірці виконання умови

$$\max_k \{B(i, j)\} - \min_k \{B(i, j)\} > 1.$$

Якщо ця умова виконується, то робиться висновок про наявність неприпустимої суперечливості, яку потрібно виправити.

Опис розробленої інформаційної технології

Інформаційна технологія складається з дев'ятих взаємопов'язаних між собою етапів. Ці етапи та їх взаємозв'язки зображені на рисунку 2. Взаємодія з децидентом або експертом передбачена на етапах 1, 3, 6, 9 (блоки блакитного кольору), а всі інші етапи здійснюються автоматично.

1. Початковими даними в розробленій інформаційній технології є кількість альтернатив та їх назви. Рекомендована кількість альтернатив – від 4 до 9, оскільки менша кількість не підходить для розробленого методу, а при більшій кількості альтернатив тернарних порівнянь буде багато, що може зробити процес ранжування трудомістким та незручним для децидента.

2. Таблиця **B** (для адитивної згортки) повинна ініціалізуватися нулями, а таблиця **S** (для мультиплікативної згортки) – одиницями.



Рисунок 2 – Основні етапи інформаційної технології ранжування альтернатив з допомогою ВТП

3. На етапі проведення ВТП автоматично формуються неповторювані преференційні набори з трьох альтернатив, які випадково вибираються з усієї множини. Ця трійка альтернатив демонструється дециденту на екрані (розташування альтернатив – зліва направо у випадковому порядку) та пропонується їх візуально порівняти. Під час кожного ВТП назви відповідних альтернатив переміщуються по екрану догори, причому **чим краще** альтернатива для децидента, **тим вище** вона має бути розташована. Розташування альтернатив на полицях переважань здійснюється двома кліками: перший клік активізує альтернативу, а другий вказує на обрану децидентом полицю.

4. Під час етапу числової інтерпретації ВТП відбувається обчислення і запис відповідних значень згідно з (5)-(9) в таблиці **B** і **S**.

5. Етап перевірки порівнянь на суперечливість (наявність конфлікуючих ВТП), для чого аналізуються значення в кожній клітинці таблиці **B**. Виявляються помилки децидента і ігноруються незначні розбіжності оцінок (4). Якщо суперечливості не виявлені, поточне ВТП вважається завершеним.

6. Якщо суперечливі ВТП виявлені, вони демонструються в наочному (візуальному) вигляді на полицях переважань. Децидент має можливість побачити та усвідомити суперечливість власних оцінок, а потім зкорегувати їх. Змінювати можна як поточне ВТП, так і попередні ВТП, з якими були виявлені суперечливості.

7. Після проведення всіх ВТП та корегування суперечливостей відбувається перехід до етапу розрахунку інформації для системного аналітика, на якому визначається результуючі кардинальні ранжування всіх альтернатив.

8. На етапі обчислення допоміжної інформації здійснюється розрахунок загального часу, який було використано на проведення усіх ВТП, середнього часу, який було використано для проведення одного ВТП, а також іншої статистичної інформації щодо проведення ранжування альтернатив.

9. Етап візуалізації результуючого ранжування є останнім етапом, під час якого дециденту демонструється результуюче ординальне ранжування альтернатив в простій та наочній формі.

В разі бажання децидента є можливість повторення процесу ранжування для тієї ж множини альтернатив.

Практика застосування розробленої інформаційної технології ранжування альтернатив на основі ВТП показала такі її **переваги**:

- Наочність, простота і інтуїтивна зрозумілість;
- Повна відсутність потреби в числових і вербальних оцінках децидентів;
- Висока швидкість;
- Висока надійність результатів;
- Врахування додаткового контексту порівнянь альтернатив;
- Пом'якшення вимоги щодо транзитивності переважань;
- Можливість виявляти та виправляти суперечливі оцінки;

- Вимірювання компетентності експертів і осіб, що приймають рішення;
- Універсальність і можливість застосування в різноманітних галузях прийняття рішень та експертного оцінювання.

Приклад застосування розробленої інформаційної технології

Розглянемо приклад застосування методу та інформаційної технології ранжування альтернатив в умовах критеріальної невизначеності за допомогою тернарних порівнянь з візуалізацією переважань на дев'яти полицях.

Задача. Приймається рішення щодо релокейту фермерського господарства в одну з п'яти областей України (Київська, Вінницька, Львівська, Харківська, Одеська). Керівник фермерського господарства має деяку неповну інформацію про кожну альтернативу, не в змозі сформулювати всі критерії оцінювання та покладається великою мірою на свій власний досвід і інтуїцію. Потрібно швидко та надійно проранжувати альтернативи, не використовуючи ніяких числових або вербальних характеристик і складних запитань.

Для розв'язання цієї задачі використаємо СППР ІСВП, створену авторами для перевірки ефективності розробленого методу ранжування альтернатив. Запропонуємо керівнику фермерського господарства (дециденту) виконати швидкі інтуїтивні візуальні тернарні порівняння, яких в нашому випадку загалом буде 10.

В якості назв альтернатив для зручності візьмемо назви відповідних обласних центрів $A = \{\text{Київ, Вінниця, Львів, Харків, Одеса}\}$.

В процесі виконання тернарних порівнянь СППР ІСВП виявила два випадки суперечливих порівнянь. Розглянемо докладніше один з них (рис. 3).

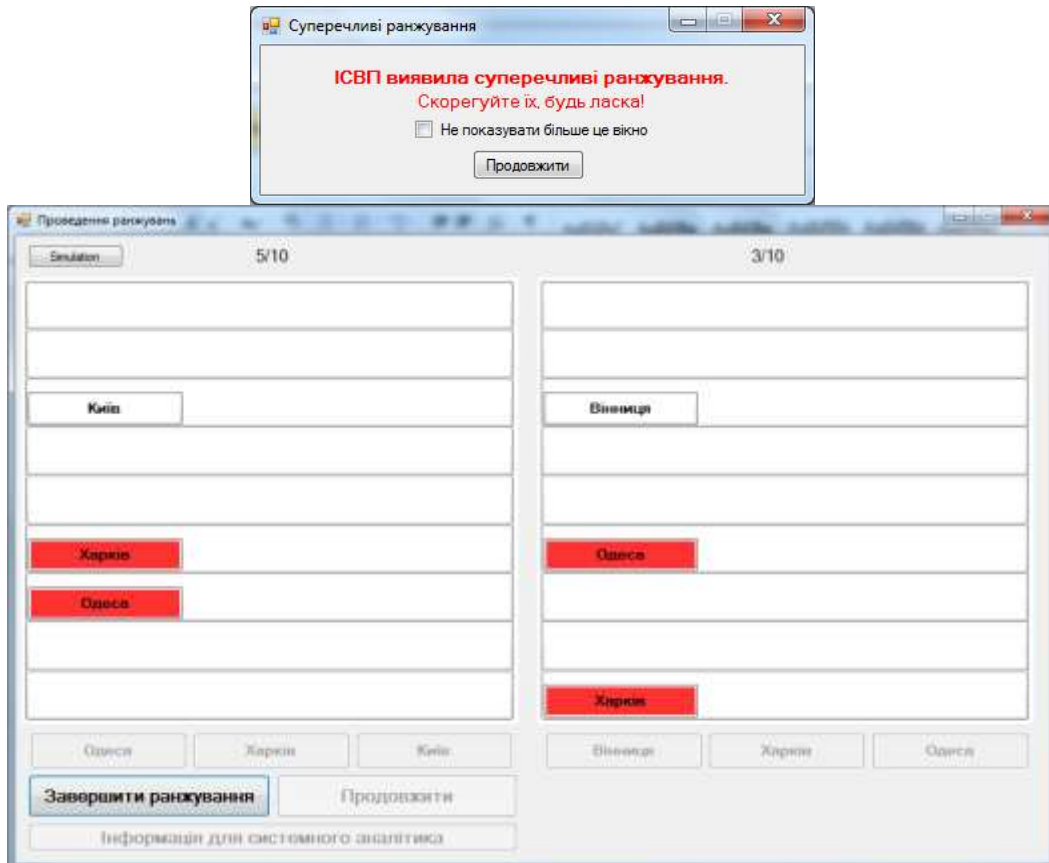


Рисунок 3 – Виявлення суперечливостей в тернарних порівняннях на полицях переважань

З порівняння 3/10 видно, що для децидента Одеса **безумовно** краще Харкова, тобто $\text{Одеса} \gg \text{Харків}$, а з порівняння 5/10 виходить, що для того ж самого децидента Харків краще Одеси, тобто $\text{Харків} > \text{Одеса}$.

Зрозуміло, що ця ситуація є неприпустимою суперечливістю і потребує виправлення. Після обмірковування децидент скорегував порівняння 5/10, перемістивши альтернативу *Харків* на дві полиці нижче, і вийшло, що $\text{Одеса} > \text{Харків}$, а це є допустимою розбіжністю з порівнянням 3/10 згідно з (4).

На рисунку 4 наведено результуюче ранжування всієї множини альтернатив. Це ранжування є **центрованим кардинальним** з візуалізацією у вигляді кольорових однонаправлених барів. Видно, що для керівника фермерського господарства **Вінниця** є найкращою альтернативою, **Київ** і **Львів** непогані, але трохи гірші, а **Одеса** і **Харків** – на останніх місцях.

На рисунку 5 наведено додаткову інформацію для системного аналітика, яка містить статистику розташування альтернатив по полицях переважань і статистику різниць в усіх 30 породжених парних порівняннях. Верхня таблиця містить всі значення тривимірного масиву **V** і результат, обчислений за методом рядкових сум. Нижня таблиця містить всі значення тривимірного масиву **S** і результат, обчислений за шкалою Сааті. Останній стовпець є результуючим **нормованим кардинальним** ранжуванням.

Оскільки ординальні ранжування альтернатив в верхній і нижній таблиці співпадають, можна зробити висновок про високу надійність отриманих результатів.

На виконання всіх десятих порівнянь (з урахуванням виправлення двох суперечливостей) було затрачено менше 2 хвилини, в середньому – 10 секунд на одне візуальне тернарне порівняння.



Рисунок 4 – Результуюче ранжування альтернатив

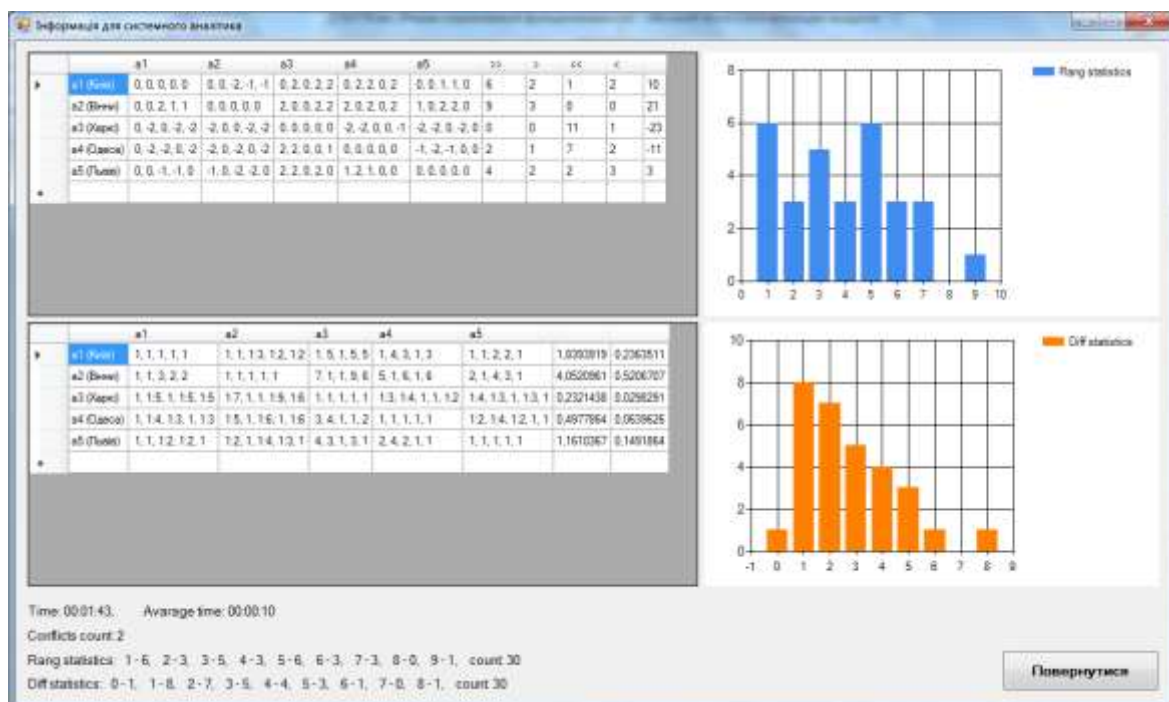


Рисунок 5 – Додаткова інформація для системного аналітика

Висновки

1. Описано новий метод ранжування альтернатив, заснований на проведенні та подальшому аналізі візуальних тернарних порівнянь.
2. Описано основні етапи інформаційної технології виявлення переважань децидента на основі цього методу.
3. Наведено приклад застосування розробленої інформаційної технології з візуалізацією альтернатив на полицях переважань.
4. Розроблений метод не потребує від децидентів ніяких числових або вербальних оцінок, є наочним та інтуїтивно зрозумілим.
5. Розширений контекст порівнянь альтернатив статистично згладжує незначні похибки і дозволяє діагностувати грубі помилки децидента.
6. В розробленому методі пом'якшується вимога щодо транзитивності переважань.
7. Проведені дослідження [12] підтверджують перспективність застосування розробленого методу та відповідної інформаційної технології при якісному і кількісному оцінюванні в різноманітних галузях, де потрібно проводити ранжування альтернатив за якістю або іншими ознаками (прийняття рішень, психологія, педагогіка, менеджмент, маркетинг, експертні оцінювання т. ін.), наприклад, для задач призначення на посаду, вимірювання в галузі емоційного інтелекту, нефактологічного оцінювання знань, аналізу споживацьких переважань, дегустаційних експертиз, некритеріального рейтингування, проведення різноманітних конкурсів тощо.

Список літератури

- [1] А. В. Катренко, та В. В. Пасічник, *Прийняття рішень: теорія та практика: підручник*. Львів, Україна: «Новий Світ – 2000», 2020.
- [2] Г. М. Гнатієнко, та В. Є. Снитюк, *Експертні технології прийняття рішень: Монографія*. Київ, Україна: ТОВ «Маклаут», 2008.
- [3] В. В. Колодний, "Трирівневі ранжування та їх застосування для виявлення переважань," у *Контроль і управління в складних системах*. Вінниця, Україна: «УНІВЕРСУМ-Вінниця», 2003, с. 238.
- [4] В. В. Колодний, та В. В. Зубко, "Метод некритеріального структурування множини альтернатив за допомогою аналізу тернарних трирівневих ранжувань," у *Proceedings of the ninth international scientific-practical conference "Internet-Education-Science" (IES-2014)*. Вінниця, Україна: ВНТУ, 2014, с. 13-14.
- [5] В. В. Зубко, "Система прийняття рішень на основі методу аналізу тернарних трирівневих ранжувань," на *XLIV науково-технічна конференція професорсько-викладацького складу, співробітників та студентів університету*. Вінниця, Україна: ВНТУ, 2015. [Електронний ресурс]. Режим доступу: <http://conf.vntu.edu.ua/allvntu/2015/initki/txt/zubko.pdf>.
- [6] В. В. Колодний, та В. В. Зубко, "Застосування гештальт-ранжувань для виявлення переваг ОПР," у *Proceedings of the tenth international scientific-practical conference «Internet-Education-Science» (IES-2016)*. Вінниця, Україна: ВНТУ, 2016, с. 43-44.
- [7] В. В. Зубко, "Інформаційна технологія для візуалізації та виявлення переважань," у *Proceedings of the tenth international scientific-practical conference «Internet-Education-Science» (IES-2016)*. Вінниця, Україна: ВНТУ, 2016, с. 58-59.
- [8] В. В. Колодний, та Д. С. Кудрявцев, "Інформаційна технологія візуального моделювання та обробки тернарних гештальт-ранжувань," *Інформаційні технології та комп'ютерна інженерія*, том 48, № 2, с. 26-34, Жовтень. 2018. doi: <https://doi.org/10.31649/1999-9941-2018-42-2-26-34>.
- [9] М. В. Лавров, та В. В. Колодний, "Мобільний застосунок для візуального тернарного ранжування альтернатив," на *XLIX науково-технічна конференція підрозділів ВНТУ, Вінниця, 27-28 квітня 2020 р.* Вінниця, Україна: ВНТУ, 2020. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/8742>.
- [10] D. Kahneman, *Thinking, Fast and Slow*. Toronto, Canada: Doubleday Canada. 2013.
- [11] R. H. Thaler, and C. R. Sunstein, *Nudge*. Longon, UK: Penguin. 2022.
- [12] В. В. Колодний, та В. В. Зубко, "Клас методів ранжування та некритеріального оцінювання об'єктів на основі візуальних тернарних порівнянь" на *Молодь в науці: дослідження, проблеми, перспективи (МН-2024)*. Вінниця, Україна: ВНТУ, 2023. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19021/15872>.

Стаття надійшла: 11.01.2024

References

- [1] A. V. Katrenko, and V. V. Pasichnyk, *Pryiniattia rishen: teoriia ta praktyka: pidruchnyk*. Lviv, Ukraina: «Novyi Svit – 2000», 2020. [in Ukrainian]

- [2] H. M. Hnatiienko, and V. Ye. Snytiuk, *Ekspertni tekhnolohii pryiniattia rishen: Monohrafiia*. Kyiv, Ukraina: TOV «Maklout», 2008. [in Ukrainian]
- [3] V. V. Kolodnyi, "Tryrivnevi ranzhuvannia ta yikh zastosuvannia dlia vyivlennia perevazhan," in *Kontrol i upravlinnia v skladnykh systemakh*. Vinnytsia, Ukraina: «UNIVERSUM-Vinnytsia», 2003, p. 238. [in Ukrainian]
- [4] V. V. Kolodnyi, and V. V. Zubko, "Metod nekryterialnoho strukturuvannia mnozhyny alter-natyv za dopomohoiu analizu ternarnykh tryrivnevykh ranzhuvan," in *Proceedings of the ninth international scientific-practical conference "Internet-Education-Science" (IES-2014)*. Vinnytsia, Ukraina: VNTU, 2014, pp. 13-14. [in Ukrainian]
- [5] V. V. Zubko, "Systema pryiniattia rishen na osnovi metodu analizu ternarnykh tryrivnevykh ranzhuvan," na *XLIV naukovo-tekhnichna konferentsiia profesorsko-vykladatskoho skladu, spivribnykiv ta studentiv universytetu*. Vinnytsia, Ukraina: VNTU, 2015. [Online]. Available: <http://conf.vntu.edu.ua/allvntu/2015/initki/txt/zubko.pdf>.
- [6] V. V. Kolodnyi, and V. V. Zubko, "Zastosuvannia heshtalt-ranzhuvan dlia vyivlennia perevah OPR," in *Proceedings of the tenth international scientific-practical conference «Internet-Education-Science» (IES-2016)*. Vinnytsia, Ukraina: VNTU, 2016, pp. 43-44.
- [7] V. V. Zubko, "Informatsiina tekhnolohiia dlia vizualizatsii ta vyivlennia perevazhan," in *Proceedings of the tenth international scientific-practical conference «Internet-Education-Science» (IES-2016)*. Vinnytsia, Ukraina: VNTU, 2016, pp. 58-59.
- [8] V. V. Kolodnyi, and D. S. Kudriavtsev, "Informatsiina tekhnolohiia vizualnoho modeliuvannia ta obrobky ternarnykh heshtalt-ranzhuvan," *Informatsiini tekhnolohii ta komp'uterna inzheneriia*, vol. 48, no. 2, pp. 26-34, October. 2018. doi: <https://doi.org/10.31649/1999-9941-2018-42-2-26-34>.
- [9] M. V. Lavrov, and V. V. Kolodnyi, "Mobilnyi zastosunok dlia vizualnoho ternarnoho ranzhuvannia alternatyv," in *XLIX naukovo-tekhnichna konferentsiia pidrozdiliv VNTU, Vinnytsia, 27-28 kvitnia 2020 r.* Vinnytsia, Ukraina: VNTU, 2020. [Online]. Available: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/8742>.
- [10] D. Kahneman, *Thinking, Fast and Slow*. Toronto, Canada: Doubleday Canada. 2013.
- [11] R. H. Thaler, and C. R. Sunstein, *Nudge*. Longon, UK: Penguin. 2022.
- [12] V. V. Kolodnyi, and V. V. Zubko, "Klas metodiv ranzhuvannia ta nekryterialnoho otsiniuvannia obiektiv na osnovi vizualnykh ternarnykh porivnian" in *Molod v nauksi: doslidzhennia, pro-blemy, perspektyvy (MN-2024)*. Vinnytsia, Ukraina: VNTU, 2023. [Online]. Available: <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19021/15872>.

Відомості про авторів

Колодний Володимир Володимирович – канд. техн. наук, доцент, доцент кафедри комп'ютерних наук

Зубко Валентин Володимирович – аспірант кафедри комп'ютерних наук

V. V. Kolodnyi, V. V. Zubko

METHOD AND INFORMATION TECHNOLOGY FOR RANGING ALTERNATIVES BASED ON VISUAL TERNARY COMPARISONS

Vinnytsia National Technical University, Vinnytsia

УДК 681.3.07

О. О. Борисюк, А. С. Сторожук, О. В. Сілагін, Є.О. Сілагін

ПОКРАЩЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ СТВОРЕННЯ ВЕБ-РЕСУРСІВ

Вінницький національний технічний університет, Вінниця

Анотація. Робота присвячена удосконаленню програмно-апаратної технології створення веб-ресурсів на основі платформи WordPress. Ця технологія базується на CMS WordPress та багаточисельних плагінах, як вбудованих в CMS, так і зовнішніх (інтегрованих). Цю технологію також доповнюють універсальні середовища веб-програмування, такі, як, наприклад Visual Studio Code, з підтримкою JavaScript, PHP та управління базами даних на MySQL, контейнеризатор Docker для локального запуску та роботи з проектом, GitHub, як основний інструмент для спільної роботи над проектом і Open Server Panel для розробки і тестування плагінів. Одним із недоліків технології створення веб-ресурсів, заснованій на платформі WordPress, є обмежений функціонал по управлінню роботи з рекламою. Це стало передумовою розробки нового цільового плагіна, що розширює функціональні можливості та автоматизує процеси по управлінню рекламою. В результаті проведеної декомпозиції функціоналу плагіна, створено діаграми класів Front-end та Back-end частин. Діаграми класів визначають самі класи та їх атрибути, методи та взає-мов'язки між ними. У контексті плагіна це включає класи, що відповідають за обробку реклам-них кампаній, статистику, інтерфейси до бази даних, тощо. Розроблено також діаграми послідовності для Front-end та Back-end частин. Вони відображають послідовність виконання операцій та взаємодію об'єктів у часі. Для обох частин плагіна розроблені також діаграми активностей, що дозволяють візуалізувати послідовність дій та процесів, що відбуваються в різних частинах плагіна, та діаграми станів, які допомагає визначити різні стани та переходи між ними для компонентів плагіна, наприклад, для відстеження стану рекламних кампаній (активна, неактивна, завершена тощо). Це може бути корисним для представлення бізнес-логіки та процесів прийняття рішень.

Ключові слова: WEB-ресурс, плагін, Wordpress, реклама, діаграма класів, діаграма послідовності, діаграма активностей, діаграма станів

Abstract. The work is devoted to the improvement of software and hardware technology for creating web resources based on the WordPress platform. This technology is based on the WordPress CMS and numerous plugins, both built into the CMS and external (integrated). This technology is also complemented by universal web programming environments, such as, for example, Visual Studio Code, with support for JavaScript, PHP and MySQL database management, Docker container for local startup and working with the project, GitHub as the main tool for collaborative work on project and Open Server Panel for developing and testing plugins. One of the disadvantages of the technology for creating web resources based on the WordPress platform is limited functionality for managing work with advertising. This became a prerequisite for the development of a new targeted plugin that expands functionality and automates the processes of advertising management. As a result of the decomposition of the plug-in functionality, class diagrams of Front-end and Back-end parts were created. Class diagrams define the classes themselves and their attributes, methods, and relationships between them. In the context of the plugin, this includes classes responsible for processing advertising campaigns, statistics, interfaces to the database, etc. Sequence diagrams for Front-end and Back-end parts have also been developed. They reflect the sequence of operations and the interaction of objects over time. For both parts of the plugin, activity diagrams have also been developed, which allow you to visualize the sequence of actions and processes occurring at different times of the plugin, and state diagrams, which help to define different states and transitions between them for plugin components, for example, to track the state of advertising campaigns (active, inactive, completed, etc.). This can be useful for representing business logic and decision-making processes.

Key words: WEB resource, plugin, Wordpress, advertising, class diagram, sequence diagram, activity diagram, state diagram

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-32-39>.

Вступ

У сучасному цифровому світі інформаційні технології відіграють важливу роль у розвитку та оптимізації веб-ресурсів. Завдяки швидкому росту інтернет-простору і зростаючій конкуренції, важливо мати ефективні засоби управління веб-ресурсами та рекламою. Технологія створення веб-ресурсів на основі платформи CMS WordPress є однією із базових у секторі середньої та підвищеної функціональності, але її можливості по управлінню рекламою є досить обмеженими [1]. Це є передумовою для покращення даної технології через розробку та інтеграцію у WordPress нового плагіна, який надає розширені можливості управління рекламою на веб-ресурсі [2].

Актуальність

Актуальність розробки плагіна для WordPress з функціональними можливостями управління рекламою на веб-ресурсі в контексті інформаційної технології з проектування WEB-ресурсів базується на постійному рості рекламного середовища в Інтернеті. В сучасному світі, де веб-ресурси є невід'ємною складовою бізнесу, ефективна реклама стає критично важливою для досягнення успіху в онлайн середовищі. Реклама на веб-ресурсах не тільки забезпечує залучення цільової аудиторії, але і є джерелом доходу для власників веб-ресурсів. Зростання популярності платформи WordPress, яка використовується для створення веб-ресурсів, робить розробку плагіна для управління рекламою на WordPress-сайтах особливо актуальною. Це дозволяє веб-розробникам і власникам сайтів розширювати функціональність своїх ресурсів і забезпечувати ефективну рекламну стратегію безпосередньо на своєму веб-сайті.

Мета

Метою дослідження є покращення існуючої технології створення WEB-ресурсів. Це покращення досягається за рахунок розробки та реалізації нового плагіна з розширеним функціоналом по управлінню рекламою та автоматизацією статистичних процесів.

Задачі

Для досягнення поставленої мети потрібно розв'язати такі задачі:

1. Сформулювати перелік функціональних вимог до роботи плагіна по управлінні рекламою на веб-ресурсі;
2. Змоделювати роботу плагіна засобами UML;
3. Реалізувати Front-end та Back-end частину плагіна;
4. Інтегрувати новий плагін з технологією розробки на платформі WordPress

Розв'язання задач

Сформулюємо перелік функцій, які повинен відпрацьовувати новий плагін по управлінню рекламою на веб-ресурсі, це:

- створення інтерфейсу для додавання та налаштування рекламних блоків на веб-сайті;
- виведення рекламних банерів у відповідних місцях на сторінках веб-ресурсу;
- можливість відслідковування та статистичного аналізу ефективності рекламних кампаній.

В результаті проведеної декомпозиції системи, що забезпечує виконання представленого функціоналу, створюємо діаграму класів, яка дозволяє визначити класи та їх атрибути, методи та взаємозв'язки між ними. Для проектування плагіна це класи, що відповідають за обробку рекламних кампаній, статистику, інтерфейси до баз даних, тощо [3].

На Front-end частині плагіна створено 5 класів, Діаграма цих класів зі встановленими зв'язками зображена на рисунку 1.

Клас `AdvertisementCampaign` представляє рекламну кампанію і має атрибути для зберігання назви, матеріалу, бюджету, часу початку та закінчення кампанії, а також її статусу. Методи цього класу дозволяють створювати та редагувати кампанії, а також змінювати їх статус.

Клас `AdvertisementMaterial` відповідає за матеріал реклами і містить інформацію про тип матеріалу та його вміст. Цей клас має метод для створення нового матеріалу.

Атрибути `CampaignStatus` визначають можливі статуси для рекламних кампаній, такі як: активна, призупинена або завершена.

Клас `AdvertisementManager` містить методи для створення нових кампаній, редагування існуючих кампаній та зміни їх статусу. Цей клас взаємодіє з класом `AdvertisementCampaign` для управління кампаніями.

Клас `UserInterface` відповідає за інтерфейс користувача і містить методи для відображення деталей кампанії та повідомлень про помилки. Цей клас взаємодіє з користувачем, показуючи інформацію та отримуючи від нього вхідні дані.

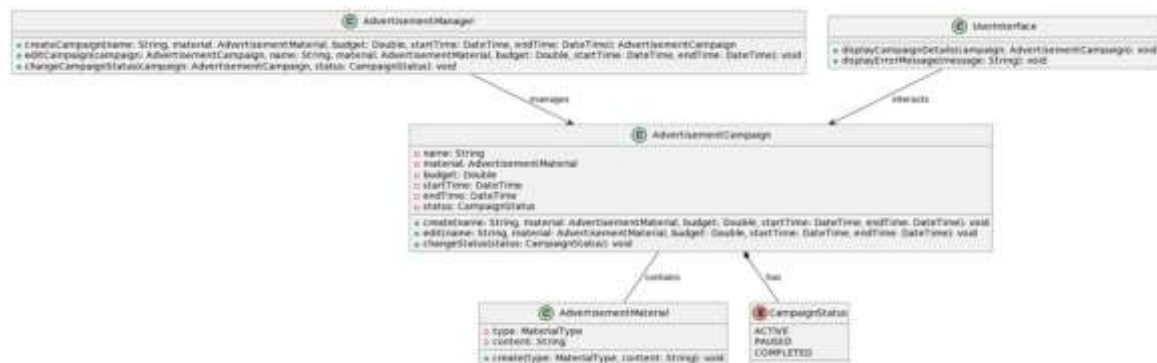


Рисунок 1 – Діаграма класів Front-end частини плагіна

На Back-end частині плагіна створено 6 класів. Діаграма цих класів зі встановленими зв'язками зображена на рисунку .

Клас `Advertiser` відображає рекламодавця і може містити інформацію про компанію, контактні дані та пов'язані рекламні кампанії.

Клас AdPlacement представляє місце розміщення реклами на веб-ресурсі. Він може включати інформацію про розмір рекламного блоку, площу на веб-сайті, цільову аудиторію та інші параметри.

Клас AdStats призначений для відстеження статистики рекламних кампаній. Цей клас містить атрибути, які представляють кількість переглядів, кліків, конверсій і інші метрики для кожної кампанії або місяця розміщення.

Клас AdManagementSystem відповідає за управління рекламними кампаніями, рекламодавцями, місцями розміщення та статистикою. Він включає методи для додавання, редагування, видалення та відстеження рекламних об'єктів.

Клас DatabaseConnector створений для взаємодії з базою даних WordPress. Цей клас забезпечує методи для збереження та отримання даних про рекламні об'єкти.

Клас Logger використовується для ведення журналу подій та реєстрації помилок.

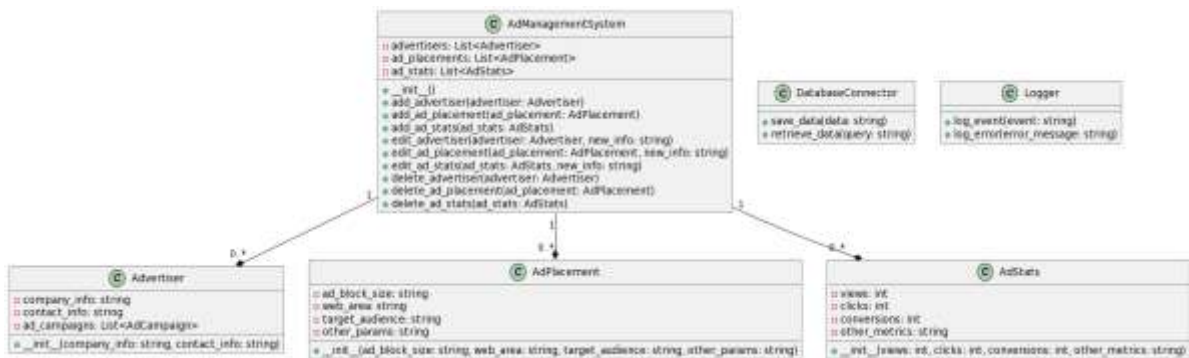


Рисунок 2 – Діаграма класів Back-end частини плагіна

Діаграма послідовностей відображає послідовність виконання операцій та взаємодію об'єктів у часі. В даному випадку, це використовується для показу того, як обробляються запити на рекламу та відповіді на них [4]. Діаграма послідовності для Front-end частини показана на рисунку 3, а Back-end частини на рисунку 4.



Рисунок 3 – Діаграма послідовності Front-end частини плагіна

Діаграма активностей дозволяє візуалізувати послідовність дій та процесів, що відбуваються в частинах плагіна. Це може бути корисним для представлення бізнес-логіки та процесів прийняття рішень [5]. Вона показує послідовність дій, які виконуються користувачем та системою під час створення нової рекламної кампанії.

Діаграма активностей для Front-end частини плагіна показана на рисунку 5.

1. Користувач вибирає 'Створити кампанію': Користувач розпочинає процес, обираючи опцію "Створити кампанію".

2. Перевірка прав користувача: Система перевіряє, чи користувач має адміністраторські права. Якщо так, відображається форма створення кампанії. Якщо ні, користувач отримує повідомлення про відмову в доступі.

3. Користувач заповнює деталі кампанії: Користувач вводить дані для нової кампанії.

4. Валідація деталей кампанії: Система перевіряє введені дані на валідність. Якщо дані валідні, відправляється запит на створення кампанії на back-end. Якщо дані не валідні, користувач отримує повідомлення про помилки валідації.

5. Відображення повідомлення про успіх або помилку: Після відповіді від Back-end, система відображає повідомлення користувачеві про успішне створення кампанії або показує повідомлення про помилку, якщо операція не вдалася.

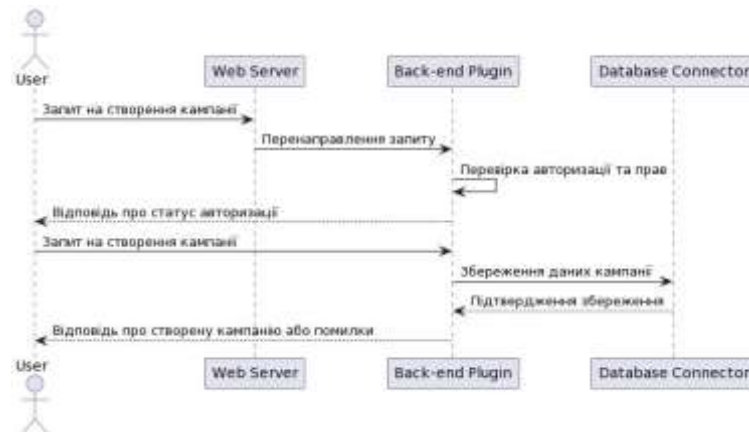


Рисунок 4 – Діаграма послідовності Back-end частини плагіна

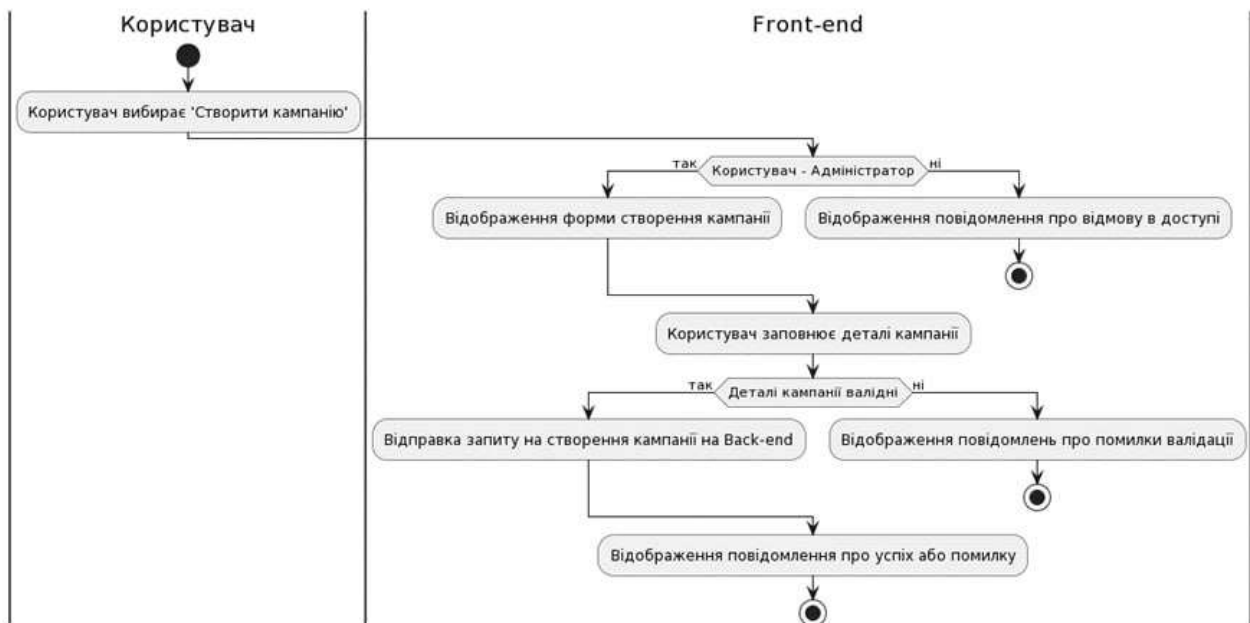


Рисунок 5 – Діаграма активностей Front-end частини плагіна

Діаграма активностей для Back-end частини плагіна показана на рисунку 6.

1. Користувач починає операцію "Створення нової рекламної кампанії".
2. Система відображає форму створення кампанії для користувача.
3. Користувач вводить інформацію про кампанію, таку як: назва, бюджет, цільова аудиторія тощо.
4. Система перевіряє, чи коректно введені дані користувачем. Якщо дані некоректні, процес переходить до кроку 6.
5. Якщо дані коректні, система зберігає інформацію про нову кампанію в базі даних.
6. Система повідомляє користувача про помилку та відображає необхідні вказівки для виправлення.

7. Користувач виправляє помилку та повторює процес введення даних.
8. Процес повторюється до тих пір, поки дані не будуть введені коректно.
9. Коли дані введені коректно, система зберігає інформацію про нову кампанію в базі даних та завершує операцію.



Рисунок 6 – Діаграма активностей Back-end частини плагіна

Діаграма станів допомагає визначити різні стани та переходи між ними для компонентів плагіна. Наприклад, для відстеження стану рекламних кампаній (активна, неактивна, завершена тощо) [6]. Діаграма станів Front-end частини плагіна для об'єкта "Рекламна кампанія" показана на рисунку 7.

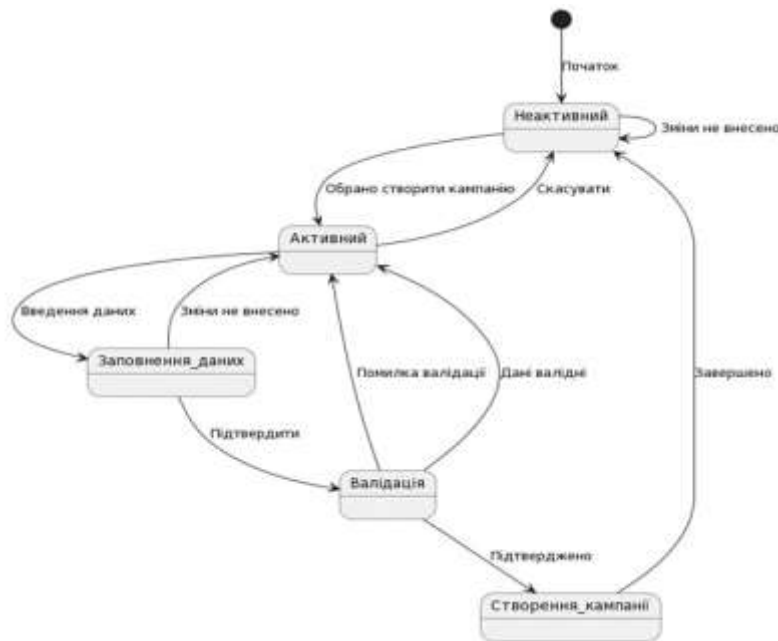


Рисунок 7 – Діаграма станів Front-end частини плагіна

На ній відображаються наступні стани:

1. Неактивний: Це початковий стан, коли система неактивна і чекає вибору користувача для створення кампанії.
2. Активний: Після того як користувач обрав створити кампанію, система переходить у стан "Активний". Звідси користувач може ввести дані для кампанії або скасувати створення.
3. Заповнення даних: Якщо користувач починає вводити дані, система переходить у стан "Заповнення даних". З цього стану користувач може виправляти введені дані або надсилати їх на валідацію.

4. Валідація: В системі проводиться валідація введених даних. Якщо дані невірні, система повертається у стан "Активний" та відображає помилки валідації. Якщо дані валідні, система переходить у стан "Створення кампанії".

5. Створення кампанії: У цьому стані система створює кампанію на основі введених та валідних даних. Після створення кампанії, система переходить у стан "Неактивний".

Діаграма станів Back-end частини плагіна для об'єкта "Рекламна кампанія" показана на рисунку 8.

1. Стан "Створено": Кампанія створена і збережена в базі даних. В цьому стані можна змінити параметри кампанії.

2. Стан "Активна": Кампанія активна і відображається на веб-ресурсі. Рекламні матеріали відображаються користувачам.

3. Стан "Пауза": Кампанія призупинена, і рекламні матеріали не відображаються користувачам. Кампанію можна відновити.

4. Стан "Завершено": Кампанія завершена, і відображення рекламних матеріалів припинено. В цьому стані кампанію можна архівувати або видалити.

5. Стан "Архів": Кампанія переміщена в архів і неактивна. Можливість редагування або відновлення обмежена.

6. Стан "Видалено": Кампанія видалена з бази даних і не може бути відновлена. Ця діаграма станів показує різні стани, в яких може перебувати рекламна кампанія в back-end частині плагіна для WordPress. Перехід між станами відбувається відповідно до дій адміністратора та параметрів кампанії.

Для реалізації плагіна вибрано середовище Visual Studio Code. Воно підтримує як JavaScript (для Front-end розробки), так і PHP (для Back-end розробки) [5,6,7]. Оскільки проект використовує JavaScript та PHP, VSCode надає розширену підтримку для цих мов програмування, включаючи автодоповнення, перевірку помилок та інші корисні функції. Крім того VSCode легко інтегрується з популярними системами контролю версій, такими як Git, які використано для організації роботи в команді.

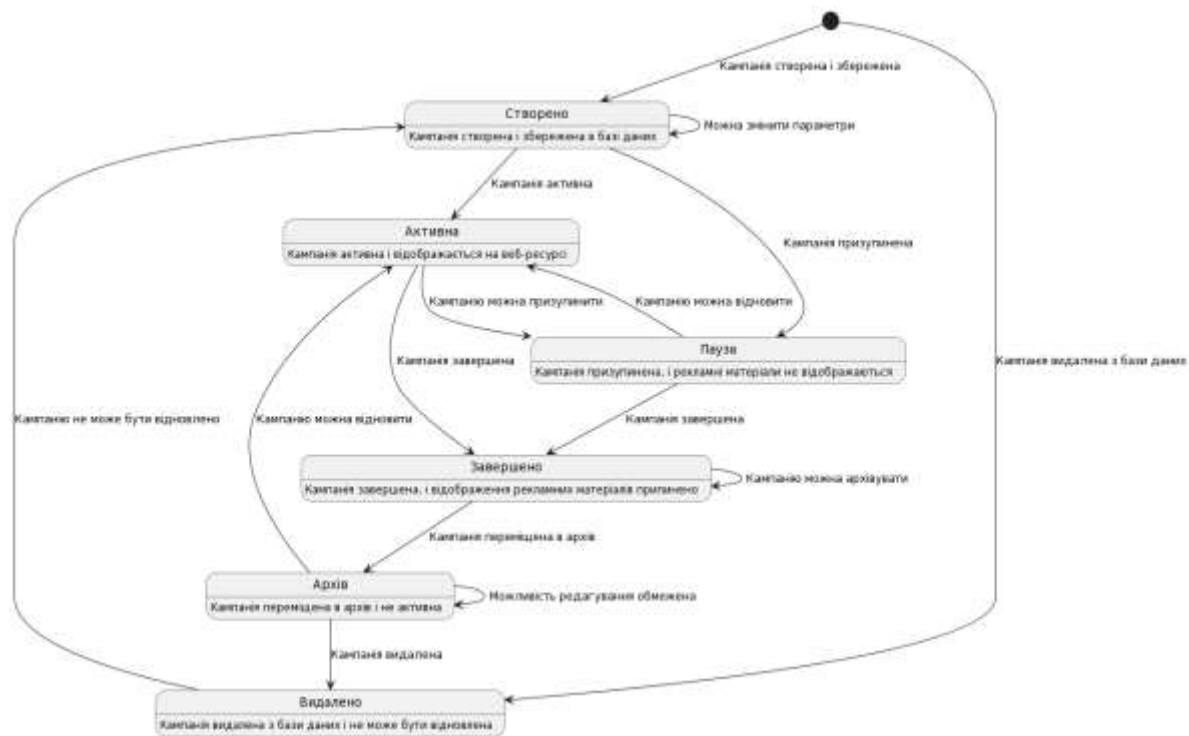


Рисунок 8 – Діаграма станів Back-end частини плагіна

Плагін забезпечений зручним та інтуїтивним інтерфейсом, це сприяє зменшенню часу, витраченого на налаштування рекламних блоків і підвищує загальну задоволеність користувачів. І, нарешті, про інтеграцію плагіна у WordPress. Це стандартна процедура через вікно «Add New Plugin» в адмін-панелі Wordpress і складається із процедур завантаження, встановлення та активації. Після активації плагін буде доступний у вкладці «Плагіни», а також він буде відображатися у бічній панелі Wordpress. Схема покращеної технології із вбудованим плагіном показана на рисунку 9.

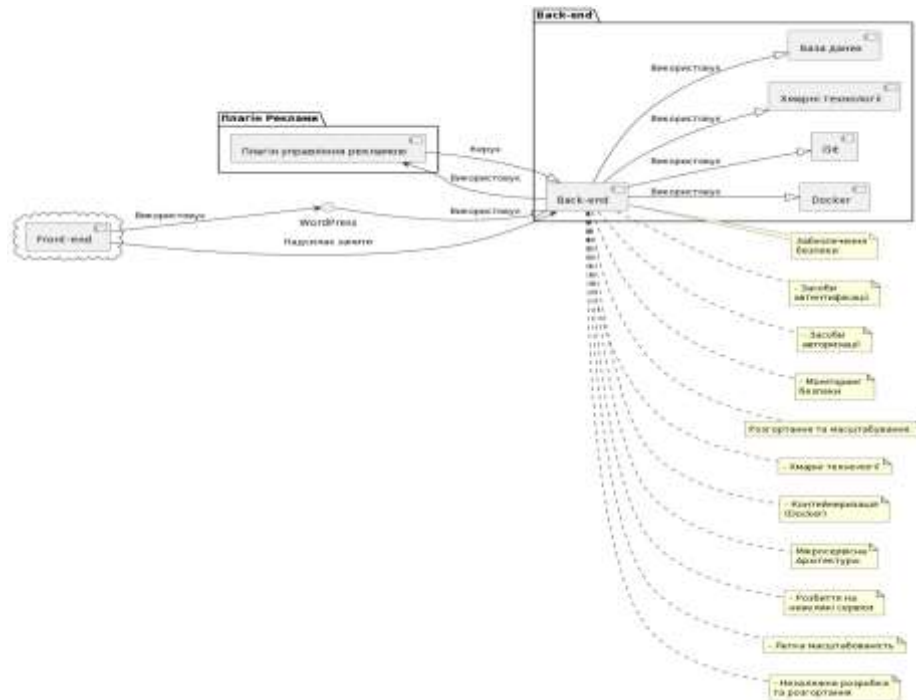


Рисунок 9 – Схема покращеної технології з інтегрованим плагіном

Висновки

Всі завдання, поставлені перед дослідженням, виконані у повному об'ємі. Мета дослідження - покращення існуючої інформаційної технології створення WEB-ресурсів досягається за рахунок розробки та інтеграції в технологію нового плагіна з розширеним функціоналом по управлінню рекламою та автоматизацією статистичних процесів. Розширений функціонал реалізований через:

- надання більших можливостей по управлінню рекламою, включаючи налаштування розміру, місцезнаходження, часу відображення рекламних блоків та вибір цільових аудиторій, що поліпшує ефективність рекламних кампаній;
- інтеграцію з аналітичними системами та іншими засобами моніторингу реклами, забезпечуючи користувачам широкі можливості для відслідковування та статистичного аналізу результатів рекламних кампаній.

Покращено існуючу інформаційну технологію створення WEB-ресурсів, плагін, який одержав назву WPAds, відкриває нові можливості управління рекламою на веб-ресурсах, поліпшуючи якість веб-сайтів, що працюють на платформі WordPress, та підвищуючи рентабельність рекламних кампаній. Це створює основу для подальших досліджень і розвитку технологій управління рекламою в Інтернеті.

Список літератури

1. Цветкова Ю.В., Сторожук А.С., Борисюк О.О., Сілагін, «Розробка сайту стартапів «Sikorsky challenge»: проектування та дизайн сайту» в Матеріали конференції факультету інтелектуальних інформаційних технологій та автоматизації (ФІТА-2022)», Вінниця, 2022. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2022/paper/view/15233/12833>
2. А. С. Сторожук, О. О. Борисюк, А. В. Сілагін «Розробка плагіна у CMS WordPress для управління рекламою на web-ресурсі», Матеріали конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2024)», Вінниця, 2023. [Електронний ресурс]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19491/16147>
3. Діаграма класів [Електронний ресурс] – Режим доступу до ресурсу: http://mmsa.kpi.ua/sites/default/files/disciplines/%D0%A0%D0%BE%D0%B7%D1%80%D0%BE%D0%B1%D0%BA%D0%B0%20%D1%96%20%D1%82%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC/didkovska_m_v_testing_lecture_5.pdf.
4. UML Sequence Diagram Tutorial [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lucidchart.com/pages/uml-sequence-diagram>.

5. UML Sequence Diagram Tutorial [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lucidchart.com/pages/uml-sequence-diagram>.
6. State Machine Diagram Tutorial [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lucidchart.com/pages/uml-state-machine-diagram>.

Стаття надійшла: 26.01.2024

References

1. Tsvyetskova YU.V., Storozhuk A.S., Borysyuk O.O., Silahin , «Rozrobka saytu startapiv «Sikorsky challenge»:proektuvannya ta dyzayn saytu» v Materialy konferentsiyi fakul'tetu intelektual'nykh informatsiynykh tekhnolohiy ta avtomatyzatsiyi (FIITA-2022)», Vinnytsya, 2022. [Elektronnyy resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2022/paper/view/15233/12833> Data zvernennya: Cherv. 2022
2. A. S. Storozhuk, O. O. Borysyuk, A. V. Silahin «Rozrobka plahina u CMS WordPress dlya upravlinnya reklamoyu na web-resursi», Materialy konferentsiyi «Molod' v nauksi: doslidzhennya, problemy, perspektyvy (MN-2024)», Vinnytsya, 2023. [Elektronnyy resurs]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19491/16147> Data zvernennya: Hruden' 2023
3. Diahrama klasiv [Elektronnyy resurs] – Rezhym dostupu do resursu: http://mmsa.kpi.ua/sites/default/files/disciplines/%D0%A0%D0%BE%D0%B7%D1%80%D0%BE%D0%B1%D0%BA%D0%B0%20%D1%96%20%D1%82%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC/didkovska_m_v_testing_lecture_5.pdf.
4. UML Sequence Diagram Tutorial [Elektronnyy resurs] – Rezhym dostupu do resursu: <https://www.lucidchart.com/pages/uml-sequence-diagram>.
5. UML Sequence Diagram Tutorial [Elektronnyy resurs] – Rezhym dostupu do resursu: <https://www.lucidchart.com/pages/uml-sequence-diagram>.
6. State Machine Diagram Tutorial [Elektronnyy resurs] – Rezhym dostupu do resursu: <https://www.lucidchart.com/pages/uml-state-machine-diagram>

Відомості про авторів

Сілагін Олексій Віталійович – канд. техн. наук., доцент, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

Olexiy V. Silagin – Cand. Sc. (Eng.), assistant Professor of Computer Science Department, Vinnytsia National Technical University, Vinnytsia,

Сторожук Антон Сергійович – магістрант кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця

Anton S. Storozhuk – magistant of the Computer Science Department, Vinnytsia National Technical University, Vinnytsia

Борисюк Олександр Олегович – магістрант кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця

Oleksandr O. Borysiuk – magistant of the Computer Science Department, Vinnytsia National Technical University, Vinnytsia

Сілагін Єгор Олексійович – асистент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

Yegor O. Silagin – assistant of Computer Science Department, Vinnytsia National Technical University, Vinnytsia

O.O. Borysiuk, A.S. Storozhuk, O.V. Silagin, Y.O. Silagin

IMPROVEMENT OF INFORMATION TECHNOLOGY FOR THE CREATION OF WEB RESOURCES

Vinnytsia National Technical University, Vinnytsia

УДК 004.7

Т.І. Коробейнікова, Т.Б. Федчук

ОГЛЯД ПИТАННЯ БЕЗПЕЧНОГО ДОСТУПУ ДО РЕСУРСІВ СИСТЕМИ ДОМЕННИХ ІМЕН

Національний університет «Львівська політехніка»

Анотація. Система доменних імен (DNS) виконує перетворення IP-адреси сервера у доменне ім'я, що дозволяє користувачам отримувати доступ до ресурсів без необхідності запам'ятовувати їх IP-адреси. Цей протокол є невід'ємною частиною сучасного Інтернету. Однак, усі комунікації між клієнтом та сервером відбуваються по незашифрованому каналі, що робить їх вразливими до різних атак, таких як: Spoofing, Eavesdropping, Phishing та інших. Для подолання даної проблеми було розроблено протоколи DNSSEC (DNS Secure), DoT (DNS over TLS) та DNS over HTTPS (DoH). Серед них останній, DoH, найкраще справляється із забезпеченням безпеки DNS-даних. DoH шифрує DNS-трафік між клієнтом та сервером та забезпечує конфіденційність та цілісність даних. Однак це призводить до проблеми у правильному визначенні DoH-трафіку. В даній статті будуть описані засоби дослідження виявлення та аналізу небезпечного DNS-трафіку, що базуються на основі аналізаторів трафіку та методу ML. Запропоновано комбіновану методіку для подолання загроз та подані порівняльні характеристики протоколів безпеки DNS. Таким чином існує необхідність у застосуванні гібридного методу дослідження шкідливого DNS-трафіку, що базується на комплексному використанні аналізаторів трафіку, машинного навчання та людського досвіду для отримання статистичних даних. Тому ця область досліджень є важливою а також малодослідженою в аспекті безпеки доменних структур. Ціллю даного дослідження є продовження розвитку та вивчення технології DNS за допомогою протоколів шифрування та ідентифікації, а також аналізу шкідливого трафіку з використанням алгоритмів машинного навчання.

Ключові слова: Хост, інкапсуляція, класифікатори трафіку, Система Доменних Імен, Машинне Навчання, рекурсивний ресолвер.

Abstract. The Domain Name System (DNS) is responsible for translating server's IP address into a domain name, enabling an end user to access a resource without having to remember it's IP address. This protocol is the basis of the modern Internet, but all messages between the client and the server pass through an unprotected communication channel, which makes it vulnerable to various types of attacks (Spoofing, Eavesdropping, Phishing and others). To overcome this problem, DNSSEC (DNS Secure), DoT (DNS over TLS) and DNS over HTTPS (DoH) protocols were developed. The last one was the most effective. DoH encrypts DNS traffic between the client and the server and also guarantees data integrity and confidentiality. This creates a problem in the correct recognition of DoH traffic. The article will describe research tools for detecting and analyzing malicious DNS traffic based on traffic analyzers and machine learning methods. Comprehensive methods for overcoming threats will be proposed and comparative characteristics of DNS security protocols will be presented. Thus, there is a need to apply a hybrid method of investigating malicious DNS traffic based on the combined use of traffic analyzers, machine learning, and human expertise to obtain statistical data. And that is why this topic of research is relevant, insufficiently researched in terms of the security of domain structures. This work is dedicated to the further development and research of DNS technology using encryption protocols and identification and analysis of malicious traffic, based on machine learning algorithms.

Key words: Host, encapsulation, traffic classifiers, Domain Name System, Machine Learning, recursive resolver.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-40-53>.

Вступ та актуальність

Інформаційні технології стали невід'ємною частиною життя сучасного людства і активно використовуються у повсякденні, професійній діяльності, також в освіті (в т.ч., дистанційній) й науці [1]. Розвиток сучасного Інтернету прискорюється, включаючи значний обсяг веб-ресурсів, що є наслідком грамотно побудованої ієрархічної системи доменних імен DNS, що є невід'ємною складовою в інформаційних технологіях. Протокол DNS перетворює доменні імена в IP адреси і навпаки. Традиційно запити DNS є незашифрованими, що робить їх вразливими до перехоплення, модифікації чи аналізу.

Методи безпечного DNS-трафіку мають на меті гарантувати безпеку та конфіденційність при функціонуванні системи доменних імен. DNS схильний до різного роду атак, скажімо: Spoofing, Eavesdropping, Phishing [2-5]. Отже, забезпечення безпеки DNS-трафіку стає все більш важливим завданням як у науковій, так і в практичній сфері, оскільки зловмисники використовують сучасні методи та швидкі підходи для прослуховування, перехоплення та крадіжки DNS-даних. [4, 6]

Одним із сучасних засобів подолання вразливостей DNS є DNS over HTTPS (DoH). Відомо, що для підвищення безпеки протоколу DNS застосовують шифрування трафіку і його подальше передавання через прихований складений канал. Зрозуміло, що для успішного проведення досліджень, виявлення та аналізу небезпечного DoH-трафіку найбільш ефективно та актуально використовувати методи машинного навчання.[7].

Згідно проведених досліджень у роботах авторів Qasem Abu Al-Haija, Manar Alohaly, Ammar Odeh, автори показали двоступеневу схему виявлення зловмисного DoH трафіку [6, 8] за допомогою комбінації різних методів навчання, вони пропонують двошарову систему. На першому рівні трафік аналізується за допомогою алгоритму «випадкових лісів» (Random Forest, RF), що дозволяє ідентифікувати його як DoH або не-DoH. На другому рівні, DoH-трафік аналізується за допомогою класифікатора «адаптивних дерев» (Adaboost, ADT), щоб визначити, чи є він безпечним DoH або шкідливим DoH. Дана система працює з мінімальною кількістю ознак, які були відібрані з використанням аналізу головних компонентів (PCA), і

зменшує кількість вибірок за допомогою методу випадкової недостатньої вибірки. Експериментальна оцінка, яку вони провели, показала, що система має високу продуктивність з точністю прогнозування на рівні 99,4%, а також мінімальні часові витрати, які становлять 0,83 секунди для першого шару та 2,27 секунди для другого. Це нашоує нас на думку, що ефективність машинного навчання у дослідженні DoH-трафіку є високою.

Отже, існує потреба у подальшому дослідженні і розвитку безпеки сервісу DNS із використанням протоколів шифрування, процесів аналізу та визначенню шкідливого трафіку за допомогою алгоритмів машинного навчання (ML, machine learning).

Мета

Метою цього дослідження є ретельний аналіз питання безпечного доступу до ресурсів системи доменних імен, з метою подальшого вивчення способів поліпшення ефективності виявлення та ідентифікації загрозового DNS-трафіку за допомогою алгоритмів ML для забезпечення безпеки та конфіденційності DNS-даних в межах клієнт-серверних сесій.

Задачі

1. Виконати огляд вразливостей сервісу DNS;
2. Виконати ґрунтовний аналіз протоколів DNS, DoH та DoT;
3. Окреслити розвиток сервісів та протоколів безпечного доступу до ресурсів доменних структур.

Аналіз вразливостей сервісу DNS

Відомо, що кожен комп'ютер в мережі Інтернет має унікальну IP-адресу, що дозволяє іншим комп'ютерам спілкуватися з ним. У початковій стадії розвитку мережі Інтернет користувачі могли отримати доступ до веб-сервера, використовуючи його IP-адресу. Наприклад, для відвідування веб-сайту CloudFlare користувач повинен ввести числову IP-адресу веб-сервера 104.16.132.229, замість символічної cloudflare.com.

У 1980-х роках надзвичайний ріст кількості хостів в Інтернеті призвів до ускладнення процесу запам'ятовування та управління IP-адресами кожного окремого хоста [9]. Paul Mockapetris вирішив цю проблему, запропонувавши систему доменних імен (DNS). Дана система здійснювала перетворення числових ідентифікаторів хостів на символічні альтернативи і навпаки [10].

За оригінальною концепцією, DNS мав ієрархічну структуру подібну до дерева, яка складалася з трьох рівнів: кореневого рівня (Root Layer), верхнього рівня або рівня домену (Top Level Domain – TLD) і авторитетного рівня (Authoritative Layer) [10]. Процес перетворення символічних імен на IP-адресу починається з моменту, коли інтернет-клієнти, а саме веб-браузери, подають DNS-запит і передають його до рекурсивного ресолвера (Recursive DNS resolver), який, у свою чергу, передає запити до декількох ітеративних ресолверів. DNS-ресолвер – це сервер, призначений для прийому запитів від клієнтських машин через веб-браузери. Зазвичай ресолвер відповідає за додаткові запити, щоб задовольнити DNS-запити клієнта. Він має надіслати запит до кореневого ресолвера для домену верхнього рівня (наприклад: .com, .edu, .gov і т. д.). Сервер домену верхнього рівня (TLD) є наступним кроком у пошуку конкретної IP-адреси і містить останню частину імені хоста (наприклад: для сайту example.com сервером верхнього рівня є "com"). Цей самий процес повторюється для ресолвера TLD, який надсилає запит до авторитетного ресолвера, наприклад example.com. Авторитетний сервер імен є останньою ланкою у запиті до сервера імен і, якщо він має доступ до запису, до якого був здійснений запит, він повертає IP-адресу для відповідного імені хоста зворотньо до DNS-ресолвера, який зробив початковий запит. У кінці рекурсивний ресолвер може здійснити запит про піддомен www всередині домену example.com і повернути клієнту його IP-адресу, як показано на рисунку 1.

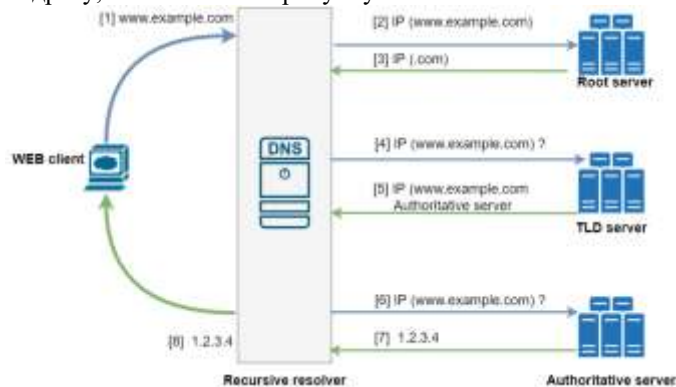


Рисунок 1 – Схема функціонування DNS

DNS-трафік не зашифрований, а запити та відповіді надсилаються у відкритому вигляді (UDP/53), і це означає, що будь-хто може слідкувати за обміном даних. Навіть якщо використовується HTTPS, сам запит DNS не шифрується [11,12]. Такий відкритий вид комунікації дає можливість зловмисникам здійснювати атаки на передані DNS-дані. Протокол DNS не має вбудованих механізмів захисту, що створює очевидні загрози для цілісності, автентифікації та конфіденційності. На рисунку 2 зображена модель потенційних DNS-загроз. Початкові DNS-повідомлення, що передаються мережею, не захищені від втручання і можуть бути замінені «в реальному часі» нападником, що може залишитися непоміченим для клієнта. Через відсутність автентифікації, зловмисник може прикидатися справжнім DNS-ресолвером за допомогою атаки "людина посередині" (Man In The Middle) [3–4, 13]. Якщо зловмисник успішно виконає таку атаку, він може надсилати клієнту підроблені IP-адреси, що перенаправляють трафік на шкідливі сервери.



Рисунок 2 – Модель потенційної DNS загрози

Додатково, нападники можуть використовувати відсутність конфіденційності в DNS. Якщо зловмисник має контроль над маршрутом DNS-трафіку, він може стратегічно блокувати конкретний потік даних, застосовуючи різні види обмежень (DNS Policy). Ці обмеження можуть фільтрувати запити DNS користувача та згідно з установленими правилами перенаправляти трафік до неіснуючого ресурсу або просто блокувати запит і повертати помилку для клієнта. Ще один, менш активний метод, полягає у захопленні та аналізі DNS-трафіку для збору даних про активність користувача. З огляду на широке поширення DNS-трафіку, це може призвести до повної втрати конфіденційності для користувача Інтернету.

Прогалина у захисті конфіденційності даних впливає не лише на безпеку, а іноді й на права людини [14]. Важливий внесок у збереження конфіденційності особистих даних користувачів внесла постанова GDPR (The General Data Protection Regulation – Загальний Регламент Захисту Даних), яка набрала чинності 25 травня 2018 року і є найсуворішим законом про конфіденційність і безпеку в світі. Незважаючи на те, що він був прийнятий Європейським Союзом (ЄС), цей закон накладає обов'язки на організації у будь-якому регіоні, де вони здійснюють направлення або збирають дані, пов'язані з особами в ЄС [15, 16].

Згідно з Global DNS Threat Report [17], який представив Ромен Фушеро, дослідник із кібербезпеки IDC (International Data Corporation), більше, ніж 88% організацій у всьому світі зазнали атак на систему DNS протягом 2022 року, що в середньому становить 7 атак на кожну організацію. Звіт також показав, що DNS-фішинг, підробка DNS, зараження шкідливим програмним забезпеченням через DNS-трафік та атаки DoS/DDoS були найпоширенішими атаками на сервіс DNS. У результаті таких атак організації в середньому втратили 942 тис. доларів, відповідно до кожної атаки [18].

Аналіз протоколів DNS, DoH та DoT

Для розв'язання проблеми безпеки DNS-даних у 1999 році був розроблений набір специфікацій DNSSEC з метою забезпечення автентифікації кінцевих точок та цілісності даних, однак він залишав проблеми з конфіденційністю не вирішеними. Система DNSSEC перетворювала IP-адресу на доменне ім'я з криптографічною цілісністю. Таким чином, DNSSEC міг бути використаний для імітації або маніпулювання DNS-даними, або ж для дослідження та перенаправлення цих даних. Проте DNSSEC не вирішував проблеми конфіденційності і мав низький рівень впровадження [19].

У минулому протокол HTTP також мав схожі проблеми з безпекою даних, як DNS, і не мав відповідних механізмів безпеки до впровадження SSL (Secure Sockets Layer), а потім TLS (Transport Layer Security). Використання TLS і SSL у HTTP призвело до розвитку протоколу HTTPS. TLS і SSL діють як проміжний шар, забезпечуючи цілісність, шифрування та автентифікацію.

Проміжний шар безпеки TLS відіграє ключову роль для протоколів DoH (DNS over HTTPS) та DoT (DNS over TLS). DoT – це протокол безпеки, який використовує шифрування та інкапсуляцію DNS-запитів і відповідей в стандартний TLS-сегмент транспортного рівня. При використанні DoT на стороні веб-клієнта ініціюється TLS-сесія із ресолвером, що включає перевірку його сертифікатів публічного ключа та обчислення секретного ключа. Після встановлення сесії відбувається обмін зашифрованим DNS-трафіком через порт (TCP/853) [20].

Проте, у 2018 році DoT не став загальноприйнятим стандартом, і DoH не був впроваджений як альтернативний для уніфікованого використання [19]. Однак, криптографічні властивості DoH такі ж, як у DoT, DoH шифрує DNS-трафік для забезпечення цілісності і конфіденційності DNS-з'єднання. На противагу від DoT, DoH передає дані не з трафіком TLS, а за допомогою повідомлень HTTPS. Ці HTTPS-повідомлення передаються через TCP/443, як і звичайний трафік HTTPS [2–5, 21]. Таким чином, можна провести порівняння мережевого стеку протоколів DNS, DoT та DoH. (рис. 3).

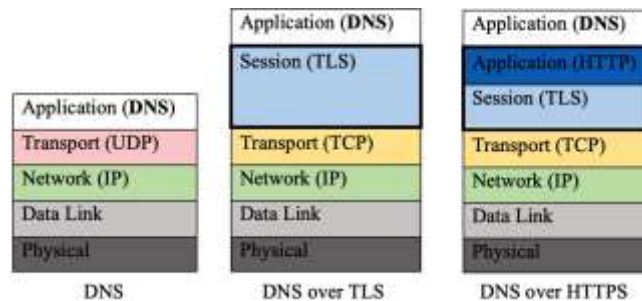


Рисунок 3 – Еквіваленти мережевого стеку протоколів DNS, DoT та DoH у порівнянні [11]

Протокол DoH працює за схемою запит-відповідь, із урахуванням відмінностей між версіями HTTP. HTTP 1.1 офіційно не рекомендований RFC [8] через низьку продуктивність, однак більшість ресолверів та браузерів підтримують його. Головна проблема обмеження продуктивності HTTP 1.1 – це відсутність підтримки декількох одночасних запитів у межах одного з'єднання. Згідно із дослідженнями авторів К. Hunek, D. Vekshin, J. Luxemburk, T. Sejka, A. Wasicek, браузери Chrome версії 94 та Firefox версії 91 зменшують затримку продуктивності, створюючи декілька паралельних з'єднань (зазвичай два). Перемикаючись між цими з'єднаннями, вони можуть виконувати квазіодносні запити. Згідно з RFC 8484 [8], кожне повідомлення містить лише один DNS-запит або DNS-відповідь. Таким чином, мережеві сканери можуть підраховувати кількість запитів/відповідей, переданих у шифрованому каналі, що надає об'єктивнішу інформацію про обмін DNS-повідомлень [8]. Проте, ніяка інша інформація не може бути безпосередньо отримана з мережевих сегментів, що мають TLS-шифрування.

З огляду на концепцію мережевого рівня, DoH подібний до стандартного обміну даними через HTTPS. Він встановлює з'єднання через TCP/443, проводить TLS handshake та передає дані у зашифрованому вигляді. Це дозволяє аналізувати вміст DNS-запитів та надає додатковий рівень захисту. Типова система, що базується на аналізі DNS-даних – це батьківський контроль, який блокує доступ до певних web-ресурсів шляхом вибіркового блокування DNS-запитів [22]. Навпроти, коректне розпізнавання DoH є складною задачею, для вирішення якої потрібно використовувати спеціалізовані моделі машинного навчання. Наразі не відомий жоден комерційний продукт, який би використовував статистичні методи або ML для розпізнавання та блокування DoH трафіку.

Давайте розглянемо протокол DoT. Він використовує порт TCP/853 і підтримує традиційну фільтрацію за портами TCP/UDP. Це дозволяє мережевим інженерам управляти та блокувати DNS-трафік для захисту мережі від зловмисників, зберігаючи конфіденційність DNS-зв'язку. Однак це може мати свої недоліки, такі як відкритий порт TCP/853 для атак. Наприклад, зловмисники можуть атакувати цей порт із використанням великого обсягу трафіку, щоб призупинити роботу DoT. В таких випадках протокол DoH стає важливим рішенням, оскільки він інкапсулює DNS-трафік у звичайні HTTPS-запити, що робить DNS-з'єднання менш помітним для традиційних засобів фільтрації за портами TCP/UDP. Однак, відсутність видимості в мережі може також означати, що атаки можуть пройти непоміченими. Таким чином, зловмисники можуть використовувати протокол DoH для створення прихованих каналів з зовнішніми серверами керування командами, що дозволяє їм здійснювати крадіжки даних та інші дії [23].

Протокол DoH був прийнятий Міжнародною організацією стандартизації мережевих технологій (IETF) як документ RFC (RFC 8484 [24]) у 2018 році. На даний момент існує дві реалізації цього протоколу. Перша реалізація, згідно з RFC 8484, використовує класичний формат "Wire" DNS, який інкапсулюється у протоколі HTTPS. "Wire format" - це двійкове представлення об'єкта DNS; зазвичай це Повідомлення (Message) або Ресурсний запис (Resource Record). Методи Write і Read визначені у типі змінних IWireSerialiser, використовуються для серіалізації та десеріалізації об'єкта DNS. Класи WireWriter і WireReader використовуються для кодування та декодування типів даних. У даному представленні об'єкта DNS також визначені зручні методи для підтримки байтового масиву або потоку. Повідомлення в форматі «Wire Format» передаються через HTTP-запити GET/POST, відповідно до визначень, наведених у RFC 1035.

Існує альтернативний підхід до DoH, який використовує формат JSON згідно з RFC 8427 [25]. У цьому випадку дані DNS кодуються і передаються через HTTPS-запит GET. Зараз більшість DNS-провайдерів (приблизно 90%) використовують традиційний «Wire format», який може бути переданий через HTTPS-GET (наприклад, <https://dns-resolver.com/?dns=<base64-encoded-query>>) або HTTPS-POST [26]. Тим не менш, підтримка DoH на основі JSON спостерігається лише у приблизно 30% DNS-провайдерів [27]. У практичному застосуванні всі браузері, які підтримують DoH, використовують формат «Wire format», що сумісний із RFC 8484, разом із методом POST HTTP. Під час POST-запитів, DNS-запит включається у тіло HTTP-запиту, а тип MIME (application/dns-message) вказується у заголовку Content-Type. Медіатип (MIME) вказує формат файлу або документа.

Використання JSON формату було запропоновано Google і, хоча цей формат не є офіційно стандартизованим, він дозволяє уникнути потреби в парсері DNS-формату та полегшує аналіз DNS-повідомлень, що подаються у текстовій формі [28]. Підхід JSON відрізняється читабельністю та зручністю маніпулювання даними на основі текстових повідомлень.

Деякі основні браузері пропонують використання JSON, хоча цей формат не є активним за замовчуванням. На рисунку 4 наведено приклад відповіді на DNS-запит типу AAAA для домену example.com, де записи AAAA відповідають доменній IPv6-адресі.

```
{
  "Status": 0,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": true,
  "CD": false,
  "Question": [
    {
      "name": "example.com.",
      "type": 28
    }
  ],
  "Answer": [
    {
      "name": "example.com.",
      "type": 28,
      "TTL": 86400,
      "data": "2001:db8:85a3:0:0:8a2e:370:7334"
    }
  ]
}
```

Рисунок 4 – Приклад DNS-відповіді на AAAA запит

Відповідно до постійного збільшення кількості доменних структур і складності фіксації зашифрованого DoH-трафіку, стає очевидним, що дослідження з'єднань DoH і виявлення шкідливого трафіку залишаються актуальними завданнями для науковців.

Подальший розвиток сервісів та протоколів безпечного доступу до ресурсів доменних структур

DNS over HTTPS має декілька відмінностей від DNS over TLS, на зразок використання механізмів HTTP/2 (механізм HTTP Push, стиснення HTTP-заголовків, паралельність потоків тощо), використання TLS 1.2 і вище та інтеграція з загальною системою HTTP (кеш, проксі, аутентифікація, тощо). Особливість моделі передачі даних HTTP Push: клієнт надсилає серверу запит лише один раз. Після першого запиту сервер продовжує надсилати нові оновлення клієнту, допоки вони доступні. Клієнт не повинен думати про надсилання додаткових запитів на сервер для отримання даних. Це значно

економить пропускну здатність мережі та зменшує навантаження на сервер. Якщо клієнт (міжсерверна комунікація) знаходиться в тому самому просторі, що й сервер, або якщо сервер встановлює безпечне з'єднання з клієнтом, клієнт може бути підключений через кінцеву точку API, яка називається URL-адресою зворотного виклику.

Важливим є те, що DoH було обрано як механізм безпеки для DNS-даних у веб-браузерах завдяки гнучкій інтероперабельності браузерів з API протоколу HTTP [28]. І саме тому DoH є в центрі уваги наукових досліджень в галузі мережевої безпеки.

Відомо, що дослідження цифрових відбитків DoT та DoH активно проводились [28-31]. Цифровий відбиток (digital fingerprint) – це унікальний цифровий ідентифікатор, використовується для забезпечення автентифікації. Він містить набір даних, які ідентифікують налаштування браузера та клієнтського пристрою як унікальні. Програмне забезпечення для зняття відбитків зберігає дані відбитків на стороні сервера, які поза межами доступу для користувача. Це дозволяє ідентифікувати та відстежувати інтернет-користувачів, навіть якщо вони відхиляють дозвіл на використання cookie. Цифровий відбиток розширив відстеження користувачів і пристроїв без використання файлів cookie у реальності, і його стало надзвичайно важко контролювати або регулювати.

Звісно, так як DoT може бути ідентифікованим завдяки використанню порту tcp/853, водночас DoH не має очевидної відмінності від звичайного HTTPS-трафіку, оскільки використовує tcp/443. Тому одним із завдань цієї роботи є ідентифікація DoH-трафіку, з яким не справляються традиційні фаєрволи та аналізатори даних. Вирішення даної задачі потребує гібридного підходу у використанні методів ML та попередніх наукових досліджень у галузі мережевих технологій та кібербезпеки [32].

Відповідно до досліджень науковців K. Hunek, D. Vekshin, J. Luxemburk, T. Sejka, A. Wasicek – JSON формат даних передбачений переважно для одноразових запитів додатками, які не вимагають великої продуктивності або швидкого часу відповіді [8]. Затримка роботи протоколу DNS безпосередньо впливає на продуктивність мережевих програм [33]. Значна кількість дослідників провели вимірювання наслідків впровадження DoH на продуктивність, і ці результати узагальнено у таблиці 1. Порівняльний аналіз досліджень стосується впливу DoH на продуктивність. Параметри вимірювання включають дані та джерело вимірювань, а результати визначають основні висновки щодо впливу DoH на продуктивність порівняно з традиційним DNS.

Таблиця 1 – Порівняння досліджень, пов'язаних з продуктивністю DoH. Вимірювання

<i>Автор</i>	<i>Рік</i>	<i>Параметри вимірювання</i>	<i>Результати</i>
McManus [34]	2018	Користувачі Firefox	Незначний вплив, додана затримка 6 мс
Böttger та ін. [35]	2019	Один клієнт	Незначний вплив на затримку під час повторного використання з'єднання
Borgolte та ін. [22]	2019	Самоемульовані мережеві умови	Вибірковий вплив, в залежності від умов мережі
Hounsel та ін. [36]	2020	Самоемульовані мережеві умови	Вибірковий вплив, в залежності від умов мережі
Hounsel та ін. [37]	2021	Згенеровано через кінцеві точки по всій Північній Америці	Вибірковий вплив, залежно від використовуваного ресолвера DoH
Chhabra та ін. [38]	2021	Глобальні вимірювання серед 224 країн	Вибірковий вплив, залежно від умов мережі
Mbewe та ін. [39]	2021	Згенеровано через кінцеві точки по всій Африці	Вибірковий вплив, залежно від умов мережі
Jerabek та ін. [40]	2022	Згенеровані, одна локація	Вибірковий вплив, залежно від використовуваного ресолвера DoH

Перше дослідження щодо затримки DoH, опубліковане МакМанусом [34] з Mozilla у 2018 році, показало, що середня затримка програм, спричинена DoH, складає всього 6 мс. Наступне дослідження, проведене Бёттгером та іншими [35], сконцентроване на порівнянні виконання DoH з традиційним DNS. Їхні результати показують, що DoH додає значну затримку, коли з'єднання використовується для одного запиту. Однак, якщо з'єднання DoH використовується повторно для кількох запитів, додаткова затримка мінімальна. Інше дослідження, проведене Хаунселлом та іншими [36], показує, що затримка DoH і надійність значно залежать від вибору ресолвера. Це також підтверджують Джерабек та інші [40], які досліджували поведінку розпізнавача DoH і розподіл розмірів пакетів DoH залежно від використаного ресолвера. Згідно з їхніми результатами, деякі ресолвери DoH використовують довгі HTTP-заголовки, що призводить до більших пакетів і, отже, до більших накладних витрат.

Більш детальне дослідження було проведено Чхаброю та іншими [38], які досліджували вплив DoH на продуктивність у всьому світі. Їхні результати показують, що користувачі з країн з високим рівнем доходу та якісною інтернет-інфраструктурою мають менші шанси на сповільнення продуктивності, спричинене DoH, що може вплинути нерівномірно на користувачів з країн із меншими економічними можливостями. Їхні висновки також підтверджуються дослідженнями Хаунселла та інших [37], Боргольте та інших [22] і Мбеве та інших [39], які також показують, що DoH має незначний вплив при низьких мережевих затримках. Згідно з цими дослідженнями [22, 38, 41] при роботі з перевантаженими або мобільними мережами 3G, традиційний DNS значно перевершує DoH.

На 2023 рік, DoH підтримується (деколи навіть включається за замовчуванням) більшістю актуальних веб-браузерів на сьогоднішній день, таких як Chrome (починаючи з версії 83.0), Edge, Firefox, Opera та Brave. Присутні також рідні резолвери з підтримкою DoH у Microsoft Windows [8] і сучасних дистрибутивах GNU/Linux (наприклад, через systemd-resolved). DoH підтримується основним програмним забезпеченням сервера доменних імен, таким як BIND (починаючи з версії 9.17.10), KNOT resolver (починаючи з версії 5.2.0) і Unbound (починаючи з версії 1.12.0). Також існує проксі-сервер DoH від Cloudflare, який називається cloudflared. Принаймні вісім реалізацій клієнта DoH відомі, а також щонайменше шість серверних реалізацій, які перераховані на dnsCrypt.info.

Використання клієнтського DoH-трафіку було досліджено S.Garcia та ін. [42]. У статті представлено три великі набори даних від великого європейського університету, великого європейського інтернет-провайдера послуг та глобальної компанії із кібербезпеки. Результати показують, що обсяг трафіку DoH зріс протягом 2020 року; однак DoH залишається відносно рідкісним порівняно з традиційним DNS. Підсумок досліджень, пов'язаних з впровадженням DoH, показаний у таблиці 2.

Таблиця 2 – Порівняння параметрів DoH

<i>Автор</i>	<i>Рік</i>	<i>Параметри Вимірювання</i>	<i>Результати</i>
Деессіо та ін. [43]	2019	Через відкриті резолвери	Впровадження < 1%
Garcia та ін. [42]	2021	Адресний простір IPv4 Трафік від 3 організацій	931 DoH-сумісні IP-адреси, обсяг трафіку DoH зростає, DoH зустрічається відносно рідко.

Оскільки основною перевагою DoH є підвищена конфіденційність кінцевих користувачів [21], її було детально вивчено багатьма дослідниками [25, 44]. Загалом існує загальний скептицизм щодо достатності шифрування DNS для збереження конфіденційності користувачів. Тому були запропоновані додаткові механізми приватності DNS під назвою EDNS (Extension Mechanisms for DNS – механізми розширення для DNS) padding. Клієнти з підтримкою DoH відправляють запити з додаванням випадкового вмісту, щоб вирівняти розміри всіх пакетів. Padding зменшує можливість витoku інформації через сторонній канал. Атака сторонніми каналами (side-channel attack) – це експлоїт системи безпеки, спрямований на збір інформації або вплив на виконання програми системи, шляхом вимірювання або використання непрямих ефектів системи чи її апаратного забезпечення, а не націлювання безпосередньо на програму чи її код. Найчастіше ці атаки спрямовані на вилучення конфіденційної інформації, зокрема криптографічних ключів, шляхом вимірювання випадкових апаратних випромінювань.

Цифрові відбитки web-сайтів можуть бути уражені атаками сторонніми каналами. Атака на відбиток web-сайту (Website fingerprinting – WFP) є окремим випадком аналізу трафіку. Вона виконується локальним перехоплювачем (eavesdropper) і має на меті отримати інформацію про вміст (тобто web-сайт, до якого спрямовується запит) зашифрованих і анонімних з'єднань шляхом спостереження за шаблонами мережі між відправником і першим вузлом анонімізації (тобто вузлом входу). Тут зловмисник просто використовує метадані, такі як розмір пакета та його напрямок, не порушуючи шифрування, щоб (пасивно) перехопити мережевий трафік, зловмисник або контролює скомпрометований мережевий пристрій на шлях або керує вузлом зловмисного входу. Атака на відбитки базується на припущенні, що з'єднання з кожним сайтом створює унікальну послідовність розмірів пакетів, яку зловмисник може використовувати для визначення переданого та зашифрованого вмісту [45]. Bushart і співавтори [46] та Siby [45] провели атаку на відбитки web-сайтів, використовуючи трафік DoH, із відключеним EDNS padding. Автори вказують, що їх підхід потребує менше даних для обробки, зберігаючи при цьому аналогічну точність порівняно з традиційними відбитками, які винайшов Edward Richard Henry ще наприкінці 19-го століття. Обидва документи також оцінювали трафік з увімкненим EDNS padding і вони успішно визначали запитовані імена з точністю більше ніж 70% при використанні HTTP1.1.

Нупек та ін. [8] провели експеримент, схожий на [45], визначаючи дійсні запити із трафіку DoH; однак вони намагалися визначити фактичний обсяг трафіку DoH і показали, що можливо визначити кількість запитів або версій протоколу HTTP для доменів, які використовували DoH за допомогою стандартного протоколу. Більше того, їм вдалося розпізнати доменні імена з точністю 90% при

використанні HTTP 1.1.

Нунек та ін. [33] провели експеримент, аналогічний атаці WFP [45] і полягав у вивченні поведінки реалізації протоколу DoH у web-браузерах Firefox і Chrome, а також рівня деталізації, який можна виявити шляхом спостереження та аналізу інформації на рівні пакетів. У роботі було використано навченого класифікатора ML, який надавав певне уявлення про окремі доменні імена лише на основі захопленого зашифрованого з'єднання DoH. Метою дослідження було визначення реальних запитів в межах одного DNS-повідомлення. Вони аналізували форму трафіку DoH і трафік мав такі критерії: кількість запитів, версії протоколу HTTP, розміри повідомлень DoH. Останній параметр, вони використовували, щоб визначити запитані доменні імена з точністю 90% при використанні HTTP 1.1 та 70% при використанні HTTP2. Однак їх метод виявився непридатним, коли було увімкнено функцію використання EDNS.

Атака на зниження приватності була досліджена Huang та ін. [47]. Вони провели атаку, блокуючи з'єднання DoH, змушуючи браузер повертатися до традиційного незашифрованого DNS без помітного сповіщення в інтерфейсі користувача. Згідно з дослідженням [47], виробники браузерів не вважають цю атаку вразливою, але скоріше добре задокументованою функцією, яка також описана в RFC 8310 [48]. Вплив атаки на зниження може бути зменшений за допомогою відповідного сповіщення про втрату приватності, однак жоден з виробників браузерів не планує інтегрувати його [47].

Інше питання приватності, пов'язане з DoH – це централізація провайдерів DoH, можлива кореляція та зловживання IP-адресами клієнтів і DNS-запитами. Проблема централізації даних розглядається у пропозиції про Oblivious DoH (ODOH), яка використовує анонімний проксі для запитів. Проксі має інформацію про IP-адреси клієнтів, але не може перевіряти вміст пакетів. Ресолвери можуть читати вміст пакетів, але не знають IP-адреси клієнта поза проксі. В даний час ODOH перебуває на стадії розробки проекту RFC з доступним відкритим кодом [8].

У таблиці 3 представлено порівняння досліджень DoH щодо конфіденційності. У сфері застосування для простоти вводяться спрощені позначення: *C* – співвідношення зашифрованих і незашифрованих DNS-даних на рекурсивному ресолвері, *FP* – атака на відбитки (Fingerprinting attack), *DG* – атака на пониження, *P* – пропозиція нової технології.

Таблиця 3 – Порівняння приватності DoH

<i>Автор</i>	<i>Рік</i>	<i>Сфера застосування</i>	<i>Результати</i>
Shulman та ін. [49]	2014	<i>C</i>	Виконання кореляційної атаки для виведення предметної області.
Bushart та ін. [46]	2019	<i>FP</i>	ML-модель для розпізнавання веб-сайтів, точність 86,1% без механізму захисту.
Siby та ін. [45]	2019	<i>FP</i>	ML-модель для відбитків веб-сайтів, точність 90,08% без захисного механізму.
Нунек та ін. [42]	2019	<i>FP</i>	ML-модель для визначення доменного імені за запитом, точність 90,14% без механізму захисту.
Huang та ін. [47]	2020	<i>DG</i>	Виконання атаки на пониження версії DoH у веб-браузерах.
Singanamalla та ін. [50]	2020	<i>P</i>	Пропозиція Oblivious DoH щодо підвищення рівня конфіденційності користувачів DoH.

На основі досліджень [22, 33, 51] щодо впливу масового розгортання DoH, можна зробити висновок, що протокол DoH є проблемою безпеки, оскільки багато існуючих автоматизованих інструментів мережевої безпеки покладаються на незашифровані DNS-повідомлення. Атакери можуть використовувати підвищену конфіденційність у зашифрованих DNS-повідомленнях, щоб приховувати свої шкідливі дії (визміна DNS-трафіку, викрадення DNS-даних між клієнтом та сервером, проведення MITM-атаки, тощо). Навіть якщо DoH забезпечує конфіденційність DNS, він не захищає від підміни DNS-розпізнавання («отруєння DNS-кешу») та дозволяє створення DNS-тунелів [8]. Отруєння DNS-кешу (DNS poisoning) – це внесення фальшивої інформації в DNS-кеш, у такий спосіб, що DNS-запити повертають неправильну відповідь, а користувачі перенаправляються на підбірні веб-сайти. Отруєння DNS-кешу також відоме як «DNS spoofing». Оскільки DNS-перетворювачі зазвичай не можуть перевірити дані у своїх кешах, неправильна DNS-інформація залишається в кеші, доки не протермінується «час життя» (Time to live – TTL) або доки її DNS-запис не буде видалений вручну. Низка вразливостей робить можливим отруєння DNS-кешу, але основна проблема полягає в тому, що DNS створено для набагато меншого за розмірами Інтернету та базується на принципі довіри.

Останнім часом було проведено багато досліджень з інтенсивності використання трафіку DoH. Загалом з'явився науковий інтерес до теми «DNS resolving у кібербезпеці», та все ж є ще багато тем, які

були малодосліджені або не дослідженні взагалі. Це дає підґрунтя для розвитку напрямку наукового дослідження протоколу DoH, який з точки зору безпеки можна розділити на дві категорії: 1) Виявлення присутності DoH в мережі та 2) Виявлення шкідливого DoH-трафіку.

Висновки

У даній роботі було досліджено понад 50 наукових джерел, це дозволило проаналізувати основні принципи та функції протоколів безпечного доступу в доменних структурах. Була сформульована основна проблематика протоколу DoH – це складність розпізнавання та аналізу його даних під час клієнт серверних сесій. Запропонований гібридний механізм для ефективного виявлення та подальшого аналізу DoH-трафіку, що базується на комбінованому використанні алгоритмів аналізу трафіку, ML та набутого людського досвіду для збору статистичних даних.

Система доменних імен DNS є важливою складовою для доступу до інтернет-ресурсів, забезпечуючи послідовність, гранульованість та ієрархічність. Дана система є необхідною для функціонування інформаційного простору та її неможливо повністю замінити. Однак через свої особливості вона стає джерелом ризику, яким зловмисники легко можуть скористатися. Ці ризики включають атаки на цілісність DNS-трафіку, наприклад атаки типу MITM; атаки на конфіденційність DNS-даних, такі як DNS Spoofing, DNS poisoning і DNS Fishing; атаки, які спрямовані на порушення автентифікації DNS-трафіку, наприклад Website fingerprinting attack; а також атаки, спрямовані на виведення з ладу DNS-ресолверів, такі як DoS та DDoS.

Впровадження нового протоколу DNS over HTTPS усуває загрози, притаманні традиційному DNS, забезпечуючи шифрування та конфіденційність даних в межах клієнт-серверних з'єднань, проте водночас створює додаткове навантаження на трафік.

Розробка істотно нових моделей для дослідження та аналізу DoH-трафіку із забезпеченням високої ефективності ключових показників може надати мережевим інженерам, кіберінженерам та фахівцям в галузі захисту комп'ютерних мереж якісні рішення, що необхідні для створення кібербезпечного інформаційного простору, його управління, моніторингу та неперервного захисту.

Дані фактори дозволяють сформулювати подальші етапи дослідження: 1. Аналіз та розпізнавання шкідливого DoH-трафіку; 2. Дослідження ефективності застосування ML-тренованої моделі ідентифікації шкідливого типу трафіку; 3. Удосконалення методології виявлення шкідливого DoH-трафіку; 4. Дослідження алгоритмів роботи аналізатора перенаправлення даних; 5. Удосконалення технології розпізнавання шкідливого DoH-трафіку з допомогою класифікатора машинного навчання; 6. Розробка методики безпечного доступу до ресурсів DNS; 7. Оцінка застосування інформаційної системи доступу до ресурсів DNS.

Список літератури

- [1] Трояновська Т. І. Інформаційна технологія доставки контенту у системах комп'ютеризованої підготовки спеціалістів. // Гороховський О. І., Трояновська Т. І., Азаров О. Д. Монографія. Вінниця : ВНТУ, 2016. –160 с.
- [2] Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.
- [3] Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.
- [4] Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
- [5] Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навч. посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2013 р.) - 500 с.
- [6] Abu Al-Haija, Q.; Alohaly, M.; Odeh, A. A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach. *Sensors* 2023, 23, 3489. <https://doi.org/10.3390/s23073489>.
- [7] Коробейнікова Т.І. Інформаційна технологія безпечного доступу до ресурсів DNS на базі ML-тренованих моделей ідентифікації трафіку / Коробейнікова Т.І., Федчук Т. Б. // International periodical scientific journal «SWorldJournal» – 2023. – № 21 (part 1) (September, 2023). – С. 80–91. ISSN: 2663-5712. DOI:10.30888/2663-5712.2023-21-01.
- [8] Karel Hunek, Dmytro Vekshin, Jan Luxemburk, Tomas Cejka, Armin Wasicek, “Summary of DNS over HTTPS Abuse”, volume 4, 2016.
- [9] Jose, G.-L.; Mary, K.S.; Carol, A.W. Internet Protocol Handbook. In *The Domain Name System (DNS) Handbook*; DTIC: Fort Belvoir, VA, USA, 1989; Volume 4.

- [10] Paul, M. Domain Names–Implementation and Specification; Internet Engineering Task Force; ISI: Marina del Rey, CA, USA, 1987.
- [11] Park, J.; Khormali, A.; Mohaisen, M.; Mohaisen, A. Where are you taking me? Behavioral analysis of open DNS resolvers. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Portland, OR, USA, 24–27 June 2019; pp. 493–504.
- [12] Cheng, Y.; Liu, Y.; Li, C.; Zhang, Z.; Li, N.; Du, Y. In-Depth Evaluation of the Impact of National-Level DNS Filtering on DNS Resolvers over Space and Time. *Electronics* 2022, 11, 1276.
- [13] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027 - 2051, March 2016.
- [14] Pavur, J.; Moser, D.; Lenders, V.; Martinovic, I. Secrets in the sky: On privacy and infrastructure security in dvb-s satellite broadband. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 277–284.
- [15] Ben Wolford, "What is GDPR, the EU's new data protection law?" <https://gdpr.eu/what-is-gdpr>.
- [16] Böttger, T.; Cuadrado, F.; Antichi, G.; Fernandes, E.L.; Tyson, G.; Castro, I.; Uhlig, S. An Empirical Study of the Cost of DNS-over-HTTPS. In Proceedings of the Internet Measurement Conference, Amsterdam, The Netherlands, 21–23 October 2019; pp. 15–21.
- [17] Romain Fouchereau, "Securing Anywhere Networking. DNS Security for Business Continuity and Resilience". June 2022.
- [18] Romain, F. DNS Security for Business Continuity and Resilience; IDC: Needham, MA, USA, 2022.
- [19] DNS Over HTTPS Traffic Analysis and Detection. Carlos López Romera, Carlos Hernández Gañán, Víctor García Font 2nd June, 2020.
- [20] Hu, Z.; Zhu, L.; Heidemann, J.; Mankin, A.; Wessels, D.; Hoffman, P.E. Specification for DNS over Transport Layer Security (TLS); Internet Engineering Task Force: Fremont, CA, USA, 2016.
- [21] Hoffman, P.E.; McManus, P. DNS Queries over HTTPS (DoH); Internet Engineering Task Force: Fremont, CA, USA, 2018.
- [22] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmitt, "How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem," *Performance, and Policy in the Internet Ecosystem (July 27, 2019)*, 2019.
- [23] Albulayhi, K.; Smadi, A.A.; Sheldon, F.T.; Abercrombie, R.K. IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. *Sensors* 2021, 21, 6432. [CrossRef] [PubMed]
- [24] P. E. Hoffman and P. McManus, "DNS Queries over HTTPS (DoH)," RFC 8484, Tech. Rep. 8484, Oct. 2018. P. Mockapetris, "Domain names - implementation and specification," RFC 1035 (Internet Standard), RFC Editor, pp. 1–55. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc1035.txt>
- [25] E. Brumaghin and C. Grady, "Covert channels and poor decisions: The tale of dnsmessenger," Mar 2017. [Online]. Available: <https://blog:talosintelligence.com/2017/03/dnsmessenger.html>
- [26] C. Cimpanu, "Here's how to enable DoH in each browser, ISPs be damned," Dec 2020, <https://www.zdnet.com/article/dns-over-https-willeventually-roll-out-in-all-major-browsers-despite-isp-opposition/>. P. E. Hoffman, "Representing DNS Messages in JSON," RFC 8427. [Online]. Available: <https://rfc-editor.org/rfc/rfc8427.txt>
- [27] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, "Large scale measurement on the adoption of encrypted DNS," *CoRR*, vol. abs/2107.04436, 2021. [Online]. Available: <https://arxiv.org/abs/2107.04436>
- [28] DNS Over HTTPS Traffic Analysis and Detection. Carlos López Romera, Carlos Hernández Gañán, Víctor García Font 2nd June, 2020.
- [29] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang, "An Investigation on Information Leakage of DNS over TLS," in *CoNEXT '19: Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, 2019.
- [30] Bushart Jonas and Christian Rossow, "Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS," *CoRR*, vol. abs/1907.01317, July 2019.
- [31] Marc Juarez, Sandra Siby, Claudia Díaz, Vallina-Rodriguez Narseo, and Carmela Troncoso, "Encrypted DNS --> Privacy? A Traffic Analysis Perspective," in *NDSS Symposium*, 2020.
- [32] K. Bumanglag and H. Kettani, "On the Impact of DNS Over HTTPS Paradigm on Cyber Systems," in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 2020, pp. 494–499.
- [33] K. Hynek and T. Cejka, "Privacy Illusion: Beware of Unpadded DoH," in *2020 11th IEEE Information Technology, Electronic and Mobile Communication conference (IEMCON)*, 2020.
- [34] P. McManus, Aug 2018. [Online]. Available: <https://blog:nightly.mozilla.org/2018/08/28/firefox-nightly-securedns-experimental-results>.
- [35] T. Böttger, F. Cuadrado, G. Antichi, E. L. a. Fernandes, G. Tyson, I. Castro, and S. Uhlig, "An Empirical Study of the Cost of DNS-over-HTTPS," in *Proceedings of the Internet Measurement Conference*, ser.

- IMC '19. New York, NY, USA: Association for Computing Machinery, 2019, p.15–21. [Online]. Available: <https://doi.org/10.1145/3355369:3355575>
- [36] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, Comparing the Effects of DNS, DoT, and DoH on Web Performance. New York, NY, USA: Association for Computing Machinery, 2020, p.562–572. [Online]. Available: <https://doi.org/10.1145/3366423:3380139>
- [37] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster, “Can Encrypted DNS Be Fast?” in Passive and Active Measurement, O. Hohlfeld, A. Lutu, and D. Levin, Eds. Cham: Springer International Publishing, 2021, pp.444–459
- [38] R. Chhabra, P. Murley, D. Kumar, M. Bailey, and G. Wang, “Measuring DNS-over-HTTPS Performance around the World,” in Proceedings of the 21st ACM Internet Measurement Conference, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 351–365. [Online]. Available: <https://doi.org/10.1145/3487552:3487849>.
- [39] E. S. Mbewe and J. Chavula, “On QoE Impact of DoH and DoT in Africa: Why a User’s DNS Choice Matters,” in Towards new e-Infrastructure and e-Services for Developing Countries, R. Zitouni, A. Phokeer, J. Chavula, A. Elmokashfi, A. Gueye, and N. Benamar, Eds. Cham: Springer International Publishing, 2021, pp. 289–304.
- [40] K. Jerabek, O. Rysavy, and I. Burgetova, “Measurement and characterization of DNS over HTTPS traffic,” 2022. [Online]. Available: <https://arxiv.org/abs/2204.03975>.
- [41] Mbewe, Enock & Chavula, Josiah. (2021). On QoE Impact of DoH and DoT in Africa: Why a User’s DNS Choice Matters. 10.1007/978-3-030-70572-5_18.
- [42] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, “Large scale measurement on the adoption of encrypted DNS,” CoRR, vol. abs/2107.04436, 2021. [Online]. Available: <https://arxiv.org/abs/2107.04436>.
- [43] C. Deccio and J. Davis, “DNS Privacy in Practice and Preparation,” in Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies, ser. CoNEXT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 138–143.
- [44] T. Jensen, “Windows Insiders can now test DNS over HTTPS,” May 2020. [Online]. Available: <https://techcommunity.microsoft.com/t5/networkingblog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282>.
- [45] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, “Encrypted DNS → Privacy? A Traffic Analysis Perspective,” Dec 2020.
- [46] J. Bushart and C. Rossow, “Padding ain’t enough: Assessing the privacy guarantees of encrypted dns,” arXiv preprint arXiv:1907.01317, 2019.
- [47] Q. Huang, D. Chang, and Z. Li, “A Comprehensive Study of DNS-over-HTTPS Downgrade Attack,” in 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20), 2020.
- [48] S. Dickinson, D. K. Gillmor, and T. Reddy.K, “Usage Profiles for DNS over TLS and DNS over DTLS,” RFC 8310, Mar. 2018. [Online]. Available: <https://www.rfc-editor.org/info/rfc8310>.
- [49] H. Shulman, “Pretty bad privacy: Pitfalls of DNS encryption,” in Proceedings of the 13th Workshop on Privacy in the Electronic Society, 2014, pp.191–200.
- [50] S. Singanamalla, S. Chunhapanya, M. Vavrusa, T. Verma, P. Wu, M. Fayed, K. Heimerl, N. Sullivan, and C. A. Wood, “Oblivious DNS over HTTPS (odoh): A practical privacy enhancement to DNS,” CoRR, vol. abs/2011.10121, 2020. [Online]. Available: <https://arxiv.org/abs/2011.10121>.
- [51] A. Fidler, B. Hubert, J. Livingood, J. Reid, and N. Leymann, “DNS over HTTPS (DoH) Considerations for Operator Networks,” Internet Engineering Task Force, Internet-Draft draft-reid-doh-operator-00, Mar. 2019, work in Progress. [Online]. Available: <https://datatracker.ietf.org/doc/html/draft-reid-doh-operator-00>.

Стаття надійшла: 04.03.2024.

References

- [1] Troyanovs'ka T. I. Informatsiyna tekhnolohiya dostavky kontentu u systemakh komp'yuteryzovanoi pidhotovky spetsialistiv. // Horokhovs'kyi O. I., Troyanovs'ka T. I., Azarov O. D. Monohrafiya. Vinnytsya : VNTU, 2016.–160 s.
- [2] Komp'yuterni merezhi: navch. posibnyk / T. I. Korobeŭnikova, S. M. Zakharchenko. – L'viv: Vydavnytstvo L'vivs'koï politekhniki, 2022. – 228 s.
- [3] Tekhnolohii zakhystu lokal'nykh merezh na osnovi obladnannya CISCO : navch. posibnyk / T. I. Korobeŭnikova, S. M. Zakharchenko. – L'viv: Vydavnytstvo L'vivs'koï politekhniki, 2021. – 188 s.
- [4] Troyanovs'ka T. I. Pobudova zakhyshchennykh merezh na bazi obladnannya kompaniyi Cisco. // Zakharchenko S.M., Troyanovs'ka T. I., Boyko O.V. Navchal'nyy posibnyk. Vinnytsya : VNTU, 2017. – 133 s.
- [5] Komp'yuterni merezhi / O. D. Azarov, S. M. Zakharchenko, O. V. Kaduk, M. M. Orlova, V. P.

- Tarasenko // Navch. posibnyk. – Vinnytsya: VNTU, 2013./MONU (Lyst №1/11 – 8260 vid 15.05 2013 r.) - 500 s.
- [6] Abu Al-Haija, Q.; Alohaly, M.; Odeh, A. A Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach. *Sensors* 2023, 23, 3489. <https://doi.org/10.3390/s23073489>.
- [7] Korobeynikova T.I. Informatsiyna tekhnolohiya bezpechnoho dostupu do resursiv DNS na bazi ML-trenovanykh modeley identyfikatsiyi trafiku / Korobeynikova T.I., Fedchuk T. B. // International periodical scientific journal «SWorldJournal» – 2023. – № 21 (part 1) (September, 2023). – S. 80–91. ISSN: 2663-5712. DOI:10.30888/2663-5712.2023-21-01.
- [8] Karel Hynek, Dmytro Vekshin, Jan Luxemburk, Tomas Cejka, Armin Wasicek, “Summary of DNS over HTTPS Abuse”, volume 4, 2016.
- [9] Jose, G.-L.; Mary, K.S.; Carol, A.W. Internet Protocol Handbook. In *The Domain Name System (DNS) Handbook*; DTIC: Fort Belvoir, VA, USA, 1989; Volume 4.
- [10] Paul, M. *Domain Names–Implementation and Specification*; Internet Engineering Task Force; ISI: Marina del Rey, CA, USA, 1987.
- [11] Park, J.; Khormali, A.; Mohaisen, M.; Mohaisen, A. Where are you taking me? Behavioral analysis of open DNS resolvers. In *Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Portland, OR, USA, 24–27 June 2019; pp. 493–504.
- [12] Cheng, Y.; Liu, Y.; Li, C.; Zhang, Z.; Li, N.; Du, Y. In-Depth Evaluation of the Impact of National-Level DNS Filtering on DNS Resolvers over Space and Time. *Electronics* 2022, 11, 1276.
- [13] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027 - 2051, March 2016.
- [14] Pavur, J.; Moser, D.; Lenders, V.; Martinovic, I. Secrets in the sky: On privacy and infrastructure security in dvb-s satellite broadband. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Miami, FL, USA, 15–17 May 2019; pp. 277–284.
- [15] Ben Wolford, “What is GDPR, the EU’s new data protection law?” <https://gdpr.eu/what-is-gdpr>.
- [16] Böttger, T.; Cuadrado, F.; Antichi, G.; Fernandes, E.L.; Tyson, G.; Castro, I.; Uhlig, S. An Empirical Study of the Cost of DNS over HTTPS. In *Proceedings of the Internet Measurement Conference*, Amsterdam, The Netherlands, 21–23 October 2019; pp. 15–21.
- [17] Romain Fouchereau, “Securing Anywhere Networking. DNS Security for Business Continuity and Resilience”. June 2022.
- [18] Romain, F. *DNS Security for Business Continuity and Resilience*; IDC: Needham, MA, USA, 2022.
- [19] DNS Over HTTPS Traffic Analysis and Detection. Carlos López Romera, Carlos Hernández Gañán, Víctor García Font 2nd June, 2020.
- [20] Hu, Z.; Zhu, L.; Heidemann, J.; Mankin, A.; Wessels, D.; Hoffman, P.E. *Specification for DNS over Transport Layer Security (TLS)*; Internet Engineering Task Force: Fremont, CA, USA, 2016.
- [21] Hoffman, P.E.; McManus, P. *DNS Queries over HTTPS (DoH)*; Internet Engineering Task Force: Fremont, CA, USA, 2018.
- [22] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmitt, “How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem,” *Performance, and Policy in the Internet Ecosystem* (July 27, 2019), 2019.
- [23] Albulayhi, K.; Smadi, A.A.; Sheldon, F.T.; Abercrombie, R.K. IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. *Sensors* 2021, 21, 6432. [CrossRef] [PubMed]
- [24] P. E. Hoffman and P. McManus, “DNS Queries over HTTPS (DoH),” RFC 8484, Tech. Rep. 8484, Oct. 2018. P. Mockapetris, “Domain names - implementation and specification,” RFC 1035 (Internet Standard), RFC Editor, pp. 1–55. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc1035.txt>
- [25] E. Brumaghin and C. Grady, “Covert channels and poor decisions: The tale of dnsmessenger,” Mar 2017. [Online]. Available: <https://blog:talosintelligence.com/2017/03/dnsmessenger.html>
- [26] C. Cimpanu, “Here’s how to enable DoH in each browser, ISPs be damned,” Dec 2020, <https://www.zdnet.com/article/dns-over-https-willeventually-roll-out-in-all-major-browsers-despite-isp-opposition/>. P. E. Hoffman, “Representing DNS Messages in JSON,” RFC 8427. [Online]. Available: <https://rfc-editor.org/rfc/rfc8427.txt>
- [27] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, “Large scale measurement on the adoption of encrypted DNS,” *CoRR*, vol. abs/2107.04436, 2021. [Online]. Available: <https://arxiv.org/abs/2107.04436>
- [28] DNS Over HTTPS Traffic Analysis and Detection. Carlos López Romera, Carlos Hernández Gañán, Víctor García Font 2nd June, 2020.
- [29] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang, "An Investigation on Information Leakage of DNS over TLS," in *CoNEXT '19: Proceedings of the 15th International Conference on Emerging*

Networking Experiments And Technologies, 2019.

- [30] Bushart Jonas and Christian Rossow, "Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS," CoRR, vol. abs/1907.01317, July 2019.
- [31] Marc Juarez, Sandra Siby, Claudia Díaz, Vallina-Rodriguez Narseo, and Carmela Troncoso, "Encrypted DNS --> Privacy? A Traffic Analysis Perspective," in NDSS Symposium, 2020.
- [32] K. Bumanglag and H. Kettani, "On the Impact of DNS Over HTTPS Paradigm on Cyber Systems," in 2020 3rd International Conference on Information and Computer Technologies (ICICT), 2020, pp. 494–499.
- [33] K. Hynek and T. Cejka, "Privacy Illusion: Beware of Unpadded DoH," in 2020 11th IEEE Information Technology, Electronic and Mobile Communication conference (IEMCON), 2020.
- [34] P. McManus, Aug 2018. [Online]. Available: <https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-securedns-experimental-results>.
- [35] T. Böttger, F. Cuadrado, G. Antichi, E. L. a. Fernandes, G. Tyson, I. Castro, and S. Uhlig, "An Empirical Study of the Cost of DNS-over-HTTPS," in Proceedings of the Internet Measurement Conference, ser. IMC '19. New York, NY, USA: Association for Computing Machinery, 2019, p.15–21. [Online]. Available: <https://doi.org/10.1145/3355369:3355575>
- [36] Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, Comparing the Effects of DNS, DoT, and DoH on Web Performance. New York, NY, USA: Association for Computing Machinery, 2020, p.562–572. [Online]. Available: <https://doi.org/10.1145/3366423:3380139>
- [37] Hounsel, P. Schmitt, K. Borgolte, and N. Feamster, "Can Encrypted DNS Be Fast?" in Passive and Active Measurement, O. Hohlfeld, A. Lutu, and D. Levin, Eds. Cham: Springer International Publishing, 2021, pp.444–459
- [38] R. Chhabra, P. Murley, D. Kumar, M. Bailey, and G. Wang, "Measuring DNS-over-HTTPS Performance around the World," in Proceedings of the 21st ACM Internet Measurement Conference, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 351–365. [Online]. Available: <https://doi.org/10.1145/3487552:3487849>.
- [39] E. S. Mbewe and J. Chavula, "On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters," in Towards new e-Infrastructure and e-Services for Developing Countries, R. Zitouni, A. Phokeer, J. Chavula, A. Elmokashfi, A. Gueye, and N. Benamar, Eds. Cham: Springer International Publishing, 2021, pp. 289–304.
- [40] K. Jerabek, O. Rysavy, and I. Burgetova, "Measurement and characterization of DNS over HTTPS traffic," 2022. [Online]. Available:<https://arxiv.org/abs/2204.03975>.
- [41] Mbewe, Enock & Chavula, Josiah. (2021). On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters. 10.1007/978-3-030-70572-5_18.
- [42] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, "Large scale measurement on the adoption of encrypted DNS," CoRR, vol. abs/2107.04436, 2021. [Online]. Available: <https://arxiv.org/abs/2107.04436>.
- [43] C. Deccio and J. Davis, "DNS Privacy in Practice and Preparation," in Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies, ser. CoNEXT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 138–143.
- [44] T. Jensen, "Windows Insiders can now test DNS over HTTPS," May 2020. [Online]. Available: <https://techcommunity.microsoft.com/t5/networkingblog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282>.
- [45] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, "Encrypted DNS -> Privacy? A Traffic Analysis Perspective," Dec 2020.
- [46] J. Bushart and C. Rossow, "Padding ain't enough: Assessing the privacy guarantees of encrypted dns," arXiv preprint arXiv:1907.01317, 2019.
- [47] Q. Huang, D. Chang, and Z. Li, "A Comprehensive Study of DNS-over-HTTPS Downgrade Attack," in 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20), 2020.
- [48] S. Dickinson, D. K. Gillmor, and T. Reddy.K, "Usage Profiles for DNS over TLS and DNS over DTLS," RFC 8310, Mar. 2018. [Online]. Available: <https://www.rfc-editor.org/info/rfc8310>.
- [49] H. Shulman, "Pretty bad privacy: Pitfalls of DNS encryption," in Proceedings of the 13th Workshop on Privacy in the Electronic Society, 2014, pp.191–200.
- [50] S. Singanamalla, S. Chunhapanaya, M. Vavrusa, T. Verma, P. Wu, M. Fayed, K. Heimerl, N. Sullivan, and C. A. Wood, "Oblivious DNS over HTTPS (odoh): A practical privacy enhancement to DNS," CoRR, vol. abs/2011.10121, 2020. [Online]. Available: <https://arxiv.org/abs/2011.10121>.
- [51] Fidler, B. Hubert, J. Livingood, J. Reid, and N. Leymann, "DNS over HTTPS (DoH) Considerations for Operator Networks," Internet Engineering Task Force, Internet-Draft draft-reid-doh-operator-00, Mar. 2019, work in Progress. [Online]. Available: <https://datatracker.ietf.org/doc/html/draft-reid-doh-operator-00>.

Відомості про авторів

Коробейнікова Тетяна Іванівна, к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana, PhD, associate professor of information technology security department, National university "Lvivska Politechnika"

Федчук Тарас Богданович, аспірант кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Fedchuk Taras, graduate student of information technology security department, National university "Lvivska Politechnika"

T. Korobeinikova, T. Fedchuk

**OVERVIEW OF SECURE ACCESS TO DOMAIN NAME SYSTEM
RESOURCES**

Lviv Polytechnic National University, Lviv

КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 621.391

О.Д. Азаров, І. С. Колесник, Л.В. Крупельницький

СИСТЕМА ЦИФРОВОГО ГЕНЕРУВАННЯ АНАЛОГОВИХ СИГНАЛІВ

Вінницький національний технічний університет, Вінниця

Анотація. Генератор є важливою ланкою в багатьох електронних пристроях, чи це тестове, лабораторне обладнання, медичні або радіоелектронні системи. Крім технічних характеристик, важливими для користувача залишаються такі параметри, як зручність застосування, компактність і низька вартість генераторів. Тому, передумовою для подальшої роботи стало проведення дослідження та оцінка характеристик наявних систем цифрового створення аналогових сигналів. Проведене дослідження дозволило детально розглянути методики створення аналогових сигналів, інструменти для їх виконання, принципи роботи, їх сильні та слабкі сторони. На жаль, пристрої, які пропонують більшість виробників, є дорогими. У зв'язку з цим залишається актуальною проблема створення бюджетного макета генератора, здатного замінити більш дорогі чи застарілі моделі. Виробляється велика кількість інтегральних мікросхем, що дозволяють генерувати сигнали різної форми. Ці мікросхеми відрізняються за способом синтезу сигналів та технічними характеристиками. За методом синтезу сигналів вони поділяються на прямі аналогові синтезатори, непрямі синтезатори на основі фазового автопідстроювання частоти, прямі цифрові синтезатори та гібридні синтезатори. В даний час найбільшою популярністю користуються синтезатори на основі прямого цифрового синтезу завдяки перевагам, пов'язаним з широкою роздільною здатністю за частотою, високою якістю сигналу, можливістю цифрового керування, низькою вартістю, малим розміром корпусів та енергоспоживанням. На основі аналізу були запропоновані покращення, для цього розроблено структурну схему системи, описані нові блоки, їх роль та механізм дії, вибрані актуальні компоненти електроніки. Обґрунтовано вибір основних компонентів, якими є мікроконтролери STM32 з ядром Cortex-M4F від STMicroelectronics та цифровий синтезатор AD9850 від Analog Devices, Inc. В результаті була спроектована система цифрового генерування аналогових сигналів.

Ключові слова: система, генератор, ЦАП, DDS, STM32, AD9850.

Abstract. The generator is an important link in many electronic devices, whether it is test, laboratory equipment, medical or radio-electronic systems. In addition to technical characteristics, parameters such as ease of use, compactness and low cost of generators remain important for the user. Therefore, the prerequisite for further work was the study and evaluation of the characteristics of the existing systems for the digital generation of analog signals. The carried out research allowed to consider in detail the methods of creating analog signals, tools for their implementation, principles of operation, their strengths and weaknesses. Unfortunately, the devices offered by most manufacturers are expensive. A large number of integrated circuits are produced that allow you to generate signals of various shapes. These chips differ in the way the signals are synthesized [3] and in their specifications. According to the method of signal synthesis, they are divided into direct analog synthesizers, indirect synthesizers based on phase autotuning, direct digital synthesizers, and hybrid synthesizers. Currently, the most popular are synthesizers based on direct digital synthesis due to the advantages associated with high frequency resolution, high signal quality, digital control, low cost, small cabinet size, and power consumption. Based on the analysis, improvements were proposed. For this purpose, a structural diagram of the system has been developed, new blocks were described, their role and mechanism of action, and relevant electronic components were selected. The choice of main components, which are STM32 microcontrollers with Cortex-M4F core from STMicroelectronics and digital synthesizer AD9850 from Analog Devices, Inc., was justified. As a result, a system for the digital generation of analog signals was designed.

Key words: system, generator, DAC, DDS, STM32, AD9850.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-54-61>.

Вступ

Ще кілька років тому прямі цифрові синтезатори частоти (DDS) були рідкістю і мали обмежену сферу застосування, їх поширене використання було обмежене через складність реалізації, а також недостатньо широким діапазоном робочих частот. В сучасній електроніці DDS вже не сприймаються розробниками як складні, незрозумілі і дорогі пристрої.

Генератори відіграють ключову роль у функціонуванні великої кількості електронних пристроїв, зокрема, тестового та лабораторного обладнання, технічних систем для обслуговування різноманітних об'єктів. Важливими характеристиками для користувача, крім технічних параметрів, є зручність використання, компактність та доступність генераторів у фінансовому сенсі. Проте, більшість пристроїв, що пропонуються виробниками, є високобюджетними. Тому актуальним залишається питання створення економічного прототипу генератора, який би міг замінити більш дорогі або застарілі моделі.

Актуальність

Існує велика кількість інтегральних мікросхем, які дозволяють генерувати сигнали різних форм. Ці мікросхеми відрізняються за методом синтезу сигналів та технічними характеристиками. За способом синтезу вони поділяються на прямі аналогові синтезатори, непрямі синтезатори на основі фазового автопідстроювання частоти, прямі цифрові синтезатори та гібридні синтезатори. На сьогоднішній день найпопулярнішими є синтезатори на основі прямого цифрового синтезу (Direct Digital Synthesis, або DDS).

Для установки і управління цифровим синтезатором необхідний мікроконтролер. На сьогоднішній час найбільшою популярністю користуються мікроконтролери STM32.

Сімейство 32-розрядних мікроконтролерів STM32 на базі процесору Arm Cortex-M розроблене для того, щоб надати користувачам нові можливості, допомогою нових можливостей. Ці можливості полягають у поєднанні підвищення високої продуктивності при обробці цифрових сигналів у реальному часі і ефективності роботи з низьким енергоспоживанням, а ще забезпеченні простоти розробки при її повній інтеграції. Більшість моделей цієї платформи можна програмувати через USB-порт, що дозволяє підключити плату безпосередньо до комп'ютера. Пристрої на базі STM32 можуть функціонувати автономно або спільно з комп'ютерним програмним забезпеченням. Управління макетом може здійснюватися за допомогою периферійних пристроїв, таких як дисплеї, кнопки, сканери, або через персональний комп'ютер.

Мета

Метою дослідження є вдосконалення системи цифрового генерування аналогових сигналів за рахунок заміни окремих вузлів структурної схеми.

Постановка задач

1. Виконати аналіз існуючих систем цифрового генерування аналогових сигналів.
2. Розробити структурну схему.
3. Розробити програмне забезпечення для керування мікропроцесором.
4. Запропонувати варіанти модифікації та вдосконалення генераторів аналогових сигналів.
5. Дослідити та промодельовати варіанти цифрового генерування аналогових сигналів.

Аналіз аналогів

Генератори сигналів довільної форми можна поділити на генератори сигналів довільної форми і стандартних функцій (AFG) і генератори сигналів довільної форми (AWG).

AFG і AWG мають деякі спільні риси, хоча за конструкцією AFG є більш спеціалізованим приладом. Фактично, AWG являє собою складну систему відтворення, що створює сигнали на основі збережених цифрових даних, які описують рівні напруги сигналу змінного струму, який постійно змінюється [1].

Універсальні генератори сигналів Rigol DG5352 застосовують прямий цифровий синтез (технології DDS), що забезпечує стабільні, точні і «ідеальні» синусоїдальні сигнали з мінімальними спотвореннями. Генератори сигналів Rigol DG5352 прості при використанні: мають користувацькі інтерфейси і зручне управління, оскільки є візуальні інструкції. Вбудовані функції модуля AM, FM, PM і FSK значно розширюють сфери використання генератора.

Звукові генератори Rigol DG5352 можуть імітувати сигнали датчиків чи електронні схеми, це дозволяє використовувати звук для встановлення і тестування різного обладнання, а ще для обслуговування та досліджень. [3]

PROTEK 9305 – одна з наймасовіших та найвідоміших серій генераторів сигналів довільної форми, форма вихідного сигналу: прямокутник, синус, імпульс, трикутник, пилкоподібний, сходовий, довільний, кардіограма, $\sin(x)/x$, експонента, шум, логарифм тощо [1].

Прилад Hantek DDS-3005 має автоматичне калібрування. Генератор Hantek DDS-3005 може створювати спеціальні та стандартні електромагнітні сигнали різних видів: синусоїди, прямокутні, імпульсні, пилкоподібні, тощо. [1]

Універсальність дозволяє застосовувати пристрій під час налагодження, перевірки та налаштування різних каналів зв'язку та високоточних радіоелектронних приладів. Вирізняється дуже низьким рівнем спотворення, високоточними результатами роботи завдяки низькому рівню похибки та оптимальним співвідношенням ціни і якості, може працювати з різними приладами.

Генератор сигналів Hantek DDS-3005 може працювати підключеним до ПК та автономно, в цьому генераторі є вбудований двоканальний частотомір діапазон якого сягає 2.7 ГГц.

Так як, пристрій має USB-інтерфейс, то для його роботи не потрібний блок живлення чи батареї. Користувач може створювати параметри сигналу, рисувати точку за допомогою комп'ютерної миші [6].

Розв'язання поставлених задач

Прямий цифровий синтез (ДЦС) – один з найпопулярніших методів синтезу частот, який використовується в області цифрової обробки даних для отримання сигналу з необхідною частотою та фази сигналу фіксованої опорної частоти. Частоту, амплітуду і фазу сигналу можна регулювати в будь-який момент часу. Генератори DDS не схильні до температурного дрейфу та старіння. Єдиний елемент, який має нестабільність, є ЦАП. Завдяки високим технічним характеристикам генераторів DDS, сьогодні можна розробляти як звичайні синтезатори частот, так і аналогові функціональні генератори.

Виходячи з того, як побудовані класичні рішення генераторів (див. рис. 1), варто врахувати існуючі рішення та запропонувати вдосконалення. Принцип роботи синтезатора DDS [2, 9] полягає в наступному: в накопичувачі фази (НФ) формується послідовність кодів вихідного сигналу, що лінійно змінюється в часі. Як накопичувач фази використовується накопичувач суматор (SM). Він являє собою регістр (RG), що перезавантажується в кожному такті роботи пристрою величиною, що дорівнює його старому вмісту, плюс деяка постійна добавка (код частоти). Вміст регістру RG лінійно збільшується в часі, а збільшення залежить від величини постійної добавки. Нагромаджуючий суматор, що використовується для формування коду фази, називають акумулятором фази. Акумулятор фази працює з періодичними переповненнями, що відповідає періодичній зміні функції і тактується по частоті f_{clk} від генератора (G). Частота переповнення акумулятора дорівнює вихідній частоті, і визначається за формулою: $f_{out} = K * f_0 / 2^n$, де f_{out} – вихідна частота, f_0 – тактова частота, K – код частоти, n – розрядність акумулятора фази.

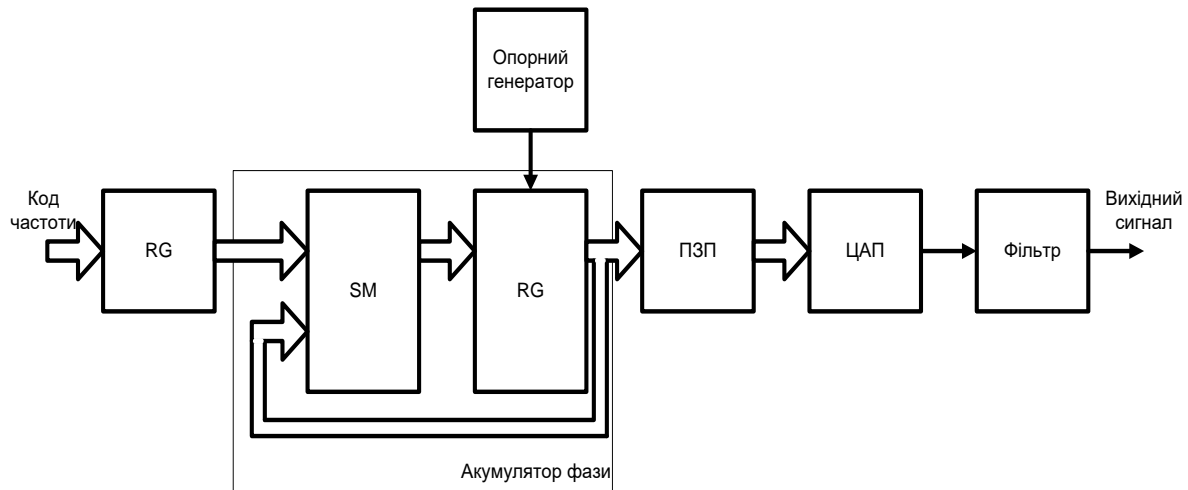


Рисунок 1 – Структура прямого цифрового синтезатора частоти

Зміни в накопичувачі фази відбуваються під впливом тактової частоти f_0 , що виробляється опорним генератором (ОГ), та коду частоти, яка генерується синтезатором. Значення амплітуди сигналу, що відповідають поточній фазі сигналу, вибираються з перекодувальної таблиці (Look Up Table), що розміщується в ПЗП. Вибір значення \sin проводиться за адресою в ПЗП із потрібною фазою. Значення з комірок пам'яті надходять на цифро-аналоговий перетворювач (ЦАП), де виходить «ступінчастий» синусоїдальний сигнал. Для згладжування вихідного сигналу на виході ЦАП розташовується нижній фільтр частот (ФНЧ).

В якості вдосконалення запропоновано структурну схему (рисунок 2) в якій замінити окремі вузли: регістри, накопичувач суматор, постійний запам'ятовуючий пристрій, опорний генератор на єдиний блок на базі мікроконтролерної системи, а також покласти на нього функції формувача коду фази, контролю поточної фази, значень для АЦП і функцій керування всією системою. Функції всіх згаданих вузлів виконуватиме мікроконтролер STM32.

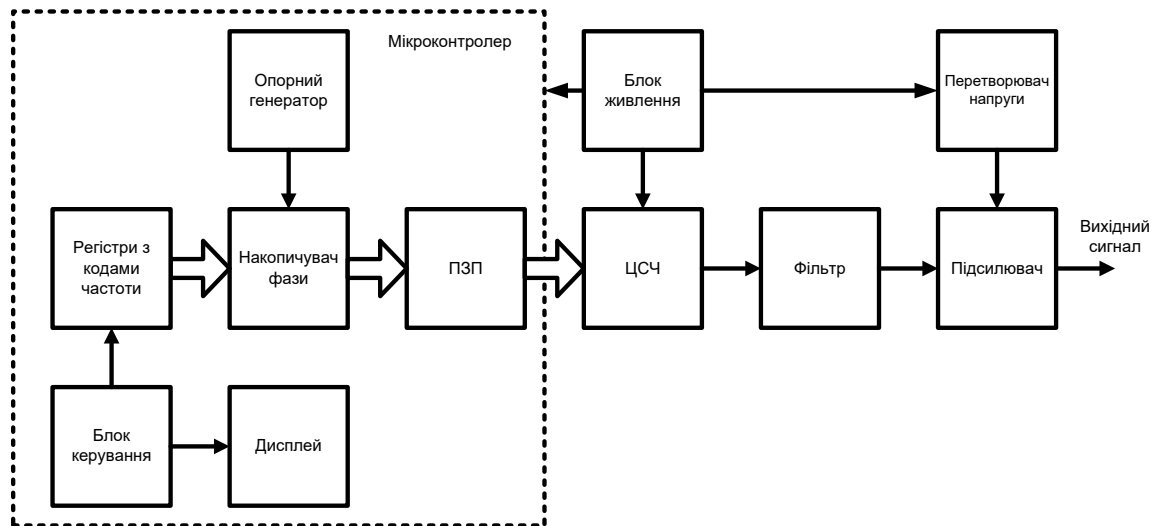


Рисунок 2 – Структура схема системи цифрового генерування аналогових сигналів

ЦАП замінити на сучасний високочотний швидкодіючий цифровий синтезатор частоти (ЦСЧ) AD9850 з цифровим керуванням із можливістю послідовної та паралельної передачі даних. Додати підсилювач вихідного сигналу для збільшення сили виходу. Такий підхід дозволить покращити характеристики генерування, підвищити точність та гнучкість управління, можливість подальшого вдосконалення і інтегрування в різні галузі діяльності.

Вдосконалення в розробці, яка проектується, можна продемонструвати на роботі генератора сигналів довільної форми (Arbitrary Waveform Generator) з комплекту віртуальних приладів NI ELVIS II. Для початку роботи з приладом, користувачем вказується файл, у якому міститься набір значень сигналу, що генерується (Waveform Name), і частота дискретизації (Update Rate), тобто частота, з якою відбувається зчитування цих значень з файлу (рисунок 3).

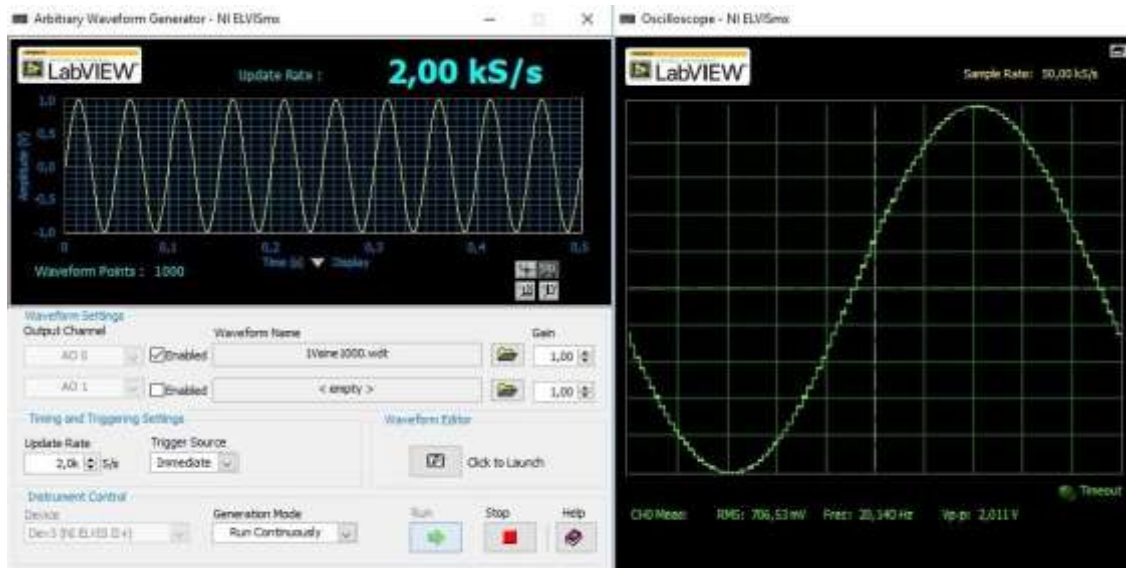


Рисунок 3 – Генерація гармонійного сигналу частотою 20 Гц

Збільшуючи чи зменшуючи частоту дискретизації, можна відповідно збільшувати чи зменшувати частоту вихідного сигналу.

Отриманий сигнал має «ступінчастий» вигляд і вимагає згладжування через ФНЧ, який взято з комплекту віртуальних приладів NI ELVIS II, його розрахунок, проведено за формулою:

$$\omega_{\text{гп}} = \frac{1}{C \times R'}$$

де ω_p – гранична частота фільтра, C – ємність конденсатора, R – опір резистора, можна підібрати відповідні елементи для ФНЧ.

Амплітудно-частотна характеристика (АЧХ) фільтра наведена на рисунку 5.

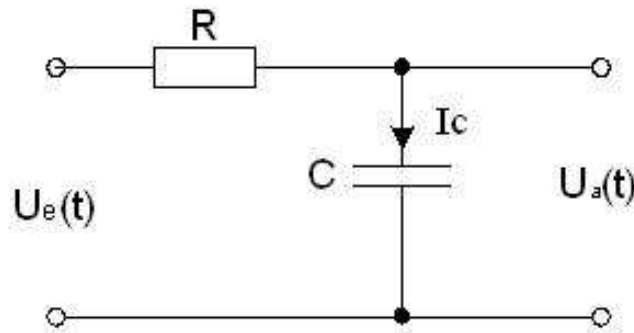


Рисунок 4 – Найпростіша схема ФНЧ до виходу генератора сигналів довільної форми

Вибираємо частоту сигналу генератора так, щоб вона потрапляла у смугу пропускання фільтра, наприклад, 700 Гц.

На рисунку 6 представлений вихідний сигнал генератора сигналів довільної форми до (сигнал 1) і після (сигнал 2) фільтрації. Результат згладжування сигналу фільтром помітний навіть візуально.

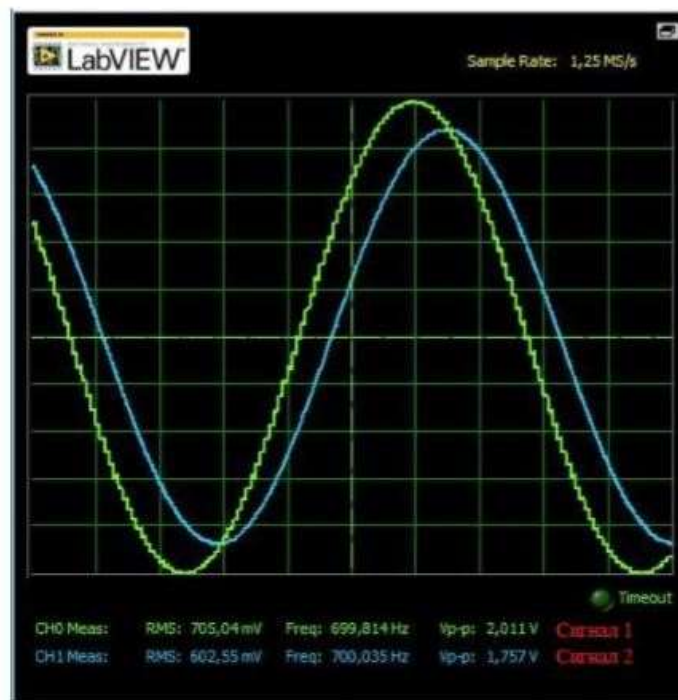


Рисунок 5 – Амплітудно-частотна характеристика ФНЧ

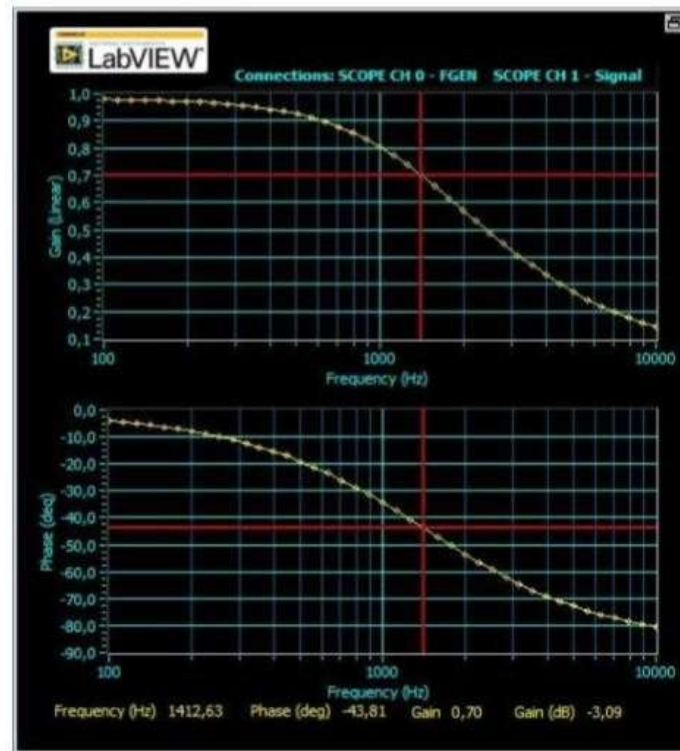


Рисунок 6 – Сигнал до та після фільтрації

Аналізатором спектра можна спостерігати суттєву зміну коефіцієнта гармонійних спотворень (КГС, англ. – Total Harmonic Distorsions – THD) сигналу після проходження через фільтр (рисунок 7). Як очевидно з рисунків без фільтра цей коефіцієнт дорівнює 1,07% (спектр 1), і з фільтром - 0,07% (спектр 2).

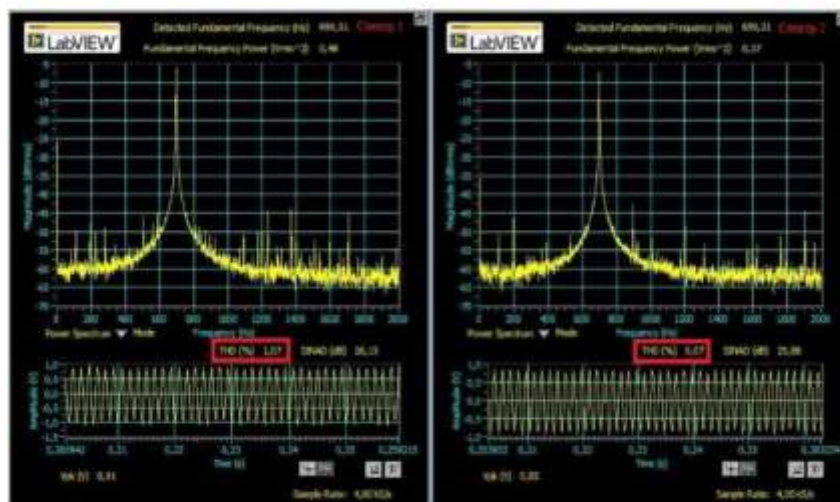


Рисунок 7 – Спектр сигналу до (ліворуч) та після (праворуч) фільтрації

Висновки

В межах цього дослідження виконано огляд та аналіз існуючих систем цифрового генерування аналогових сигналів, що дало змогу вивчити існуючі методи генерування

аналогових сигналів та засобів для їх реалізації, принципи їх функціонування і наявні переваги та недоліки.

Відповідно до розглянутих існуючих варіантів запропоновано вдосконалення.

Розроблено структурну схему системи, описано нововведені блоки та їх призначення і функціонування, підбрано реальні компоненти сучасної електроніки.

Після запропонованого вдосконалення є можливість реалізації декілька варіантів модифікації генераторів аналогових сигналів, а саме, побудувати таких генераторів:

- із використанням технічних можливостей плати STM32F4 Discovery;
- із використанням цифрового синтезатора AD9850 та STM32F4 Discovery, а також ArduinoLCDKeypadShield— для відображення інформації та зручного керування;
- STM32F429I Disco та цифрового синтезатора AD9850.

Список літератури

- [1] Carmine Noviello, *Mastering STM32*: eBook. Leanpub, 2018.
- [2] О.С. Кравчук, та В.І. Манаєнков, «Розробка функціонального генератора сигналів на основі прямого цифрового синтезу», *Радіоелектронні та комп'ютерні системи*. № 4 (23). С. 22 - 26. 2007.
- [3] STM32F103C8 - Mainstream Performance line, Arm Cortex-M3 MCU with 64 Kbytes of Flash memory, 72 MHz CPU, motor control, USB and CAN.. [Електронний ресурс]. Режим доступу: <https://www.st.com/en/microcontrollers/microprocessors/stm32f103c8.html>
- [4] STM32CubeMX - STM32Cube initialization code generator. [Електронний ресурс]. Режим доступу: <https://www.st.com/en/development-tools/stm32cubemx.html> (дата звернення: 08.06.2021).
- [5] STM32 32-bit Arm Cortex MCUs. [Електронний ресурс]. Режим доступу: <https://www.st.com/en/microcontrollers/stm32-32-bit-arm-cortex-mcus.html>
- [6] Getting started with STM32 [Електронний ресурс]. Режим доступу: https://wiki.st.com/stm32mcu/wiki/STM32StepByStep:STM32_step_by_step_overview.
- [7] STM32-base project. [Електронний ресурс]. Режим доступу: <https://stm32-base.org/guides/gettingstarted.html>.
- [8] STM32 microcontroller GPIO configuration for hardware. [Електронний ресурс]. Режим доступу: <an4899-stm32-microcontroller-gpio-configuration-for-hardware-settings-and-lowpower-consumption.pdf>.
- [9] В.Н.Чинков, *Цифрові засоби вимірюваної техніки військового призначення: підручник*, Х.: ХУПС, 2007.

Стаття надійшла: 04.03.2024.

References

- [1] Carmine Noviello, *Mastering STM32*: eBook. Leanpub, 2018.
- [2] O.S. Kravchuk, V.I. Manayenkov, "Rozrobka funktsional'noho heneratora syhnaliv na osnovi pryamooho tsyfrovoho syntezu", *Radioelektronni ta komp'yuterni systemy*. pp. 22 - 26. № 4 (23). 2007.
- [3] STM32F103C8 - Mainstream Performance line, Arm Cortex-M3 MCU with 64 Kbytes of Flash memory, 72 MHz CPU, motor control, USB and CAN. [Online]. Available: <https://www.st.com/en/microcontrollers/microprocessors/stm32f103c8.html>.
- [4] STM32CubeMX - STM32Cube initialization code generator [Online]. Available: <https://www.st.com/en/development-tools/stm32cubemx.html>.
- [5] STM32 32-bit Arm Cortex MCUs. [Online]. Available: <https://www.st.com/en/microcontrollers/stm32-32-bit-arm-cortex-mcus.html>.
- [6] Getting started with STM32 [Online]. Available: https://wiki.st.com/stm32mcu/wiki/STM32StepByStep:STM32_step_by_step_overview
- [7] STM32-base project: veb-sayt. [Online]. Available: <https://stm32-base.org/guides/gettingstarted.html>.
- [8] STM32 microcontroller GPIO configuration for hardware. [Online]. Available: <an4899-stm32-microcontroller-gpio-configuration-for-hardware-settings-and-lowpower-consumption.pdf>.
- [9] Chynkov V.N. *Tsyfrovi zasoby vumiryuvanoyi tekhniki viys'kovoho pryznachennya: pidruchnyk*. Kh.: KHUPS, 2007.

Відомості про авторів

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

Azarov, Olexiy D. – Doctor of Science (Tech.), head of the Department of Computer Engineering, Vinnytsya National Technical University

Колесник Ірина Сергіївна – кандидат технічних наук, доцент кафедри обчислювальної техніки, ВНТУ

Kolesnyk, Iryna S. – PhD, Assistant Professor of the Department of Computer Engineering, Vinnytsya National Technical University

Крупельницький Леонід Віталійович – кандидат технічних наук, доцент кафедри обчислювальної техніки, ВНТУ

Krupelnitskyi, Leonid V – PhD, Assistant Professor of the Department of Computer Engineering, Vinnytsya National Technical University

O. Azarov, I. Kolesnyk, L. Krupelnitsky

DIGITAL GENERATION SYSTEM FOR ANALOG SIGNALS

Vinnytsya National Technical University, Vinnytsya

UDC 615. 471.03:616.073

S.V. Pavlov¹, Waldemar Wójcik², R.L. Holyaka³,
O.D. Azarov¹, L.E. Nykyforova⁴, O.V.Kaduk¹

ELECTRIC THERMAL MODELING OF TEMPERATURE-DEPENDENT VAC OF THE TRANSISTOR-TYPE CONVERTERS IN BIOMEDICAL ENGINEERING

¹Vinnitsia National Technical University, 95, Khmelnitske shosse, 21021, Vinnitsia, Ukraine,²Lublin University of Technology, Poland³Lviv Polytechnic National University, Ukraine⁴National University of Life and Environmental Sciences of Ukraine

Анотація. В статті розглянуто шляхи вирішення проблеми нестабільності ітераційних процесів при аналізі ВАХ вимірювальних перетворювачів з від'ємним диференціальним опором, обумовленим самонагрівом цих перетворювачів. Розроблено експрес-метод визначення меж, в яких забезпечується коректний електротепловий DC аналіз. Відповідно до розглянутої задачі розроблено методу синтезу електротермічної моделі транзисторних структур термодатчиків потоку. Аналізуючи модель біполярного транзистора з точки зору впливу температури саморозігріву на ВАХ, необхідно розглянути, як мінімум, три механізми впливу температури. Слід зазначити, що, як і в представлених раніше моделях, мова йде не тільки про вплив температури навколишнього середовища на параметри транзистора, але і про його самонагрівання, тобто про прямий вплив потужності, що виділяється в структурі транзистора, на його електрофізичні параметри. Запропоновано спосіб синтезу електротеплових моделей терморезистивних, діодних та транзисторних структур первинних перетворювачів теплових сенсорів потоку. На відміну від відомих пакетів схемного моделювання (PSpice чи MicroCAP) запропонований спосіб дозволяє за один цикл DC аналізу отримати ВАХ з врахуванням самонагріву вищевказаних перетворювачів. Розроблено комплексну методику електротеплового моделювання вимірювальних перетворювачів теплових сенсорів потоку, що включає в себе синтез кола заміщення імпульсної температурної релаксації та спосіб формування ВАХ перетворювачів в режимі їх самонагріву струмом живлення. З точки зору практичного використання транзисторів у схемах вимірювальних перетворювачів термодатчиків необхідно забезпечити не тільки достатній нагрів структури транзистора, але й достатню електричну термостійкість його функціонування. Для цього необхідно використовувати, зокрема, емітуючі стабілізуючі резистори або диференціальне з'єднання пари транзисторів з джерелом струму.

Ключові слова: вимірювальні перетворювачі, електротеплове моделювання, самонагрів перетворювачів, біомедичні прилади та системи.

Abstract. Considered problems of instability of iterative processes in the analysis of I/V measuring converters with negative differential resistance caused by self-heating of these converters. An express method of determining the limits in which correct electrothermal DC analysis is provided has been developed. According to the problems considered the method of the synthesis of the electrothermal model of the transistor structures of thermal flow sensors. Analyzing the model of the bipolar transistor from the point of view of the impact of self-heating temperature on VAC, it is necessary to consider, at least, three mechanisms of temperature impact. It should be noted that, as in the models presented before, we speak not only of the impact of the ambient temperature on the parameters of the transistor, but on its self-heating, i.e., direct impact of power released in the transistor structure on its electric physical parameters. A method of synthesis of electrothermal models of thermoresistive, diode and transistor structures of primary converters of thermal flow sensors is proposed. In contrast to well-known circuit modeling packages (PSpice or MicroCAP), the proposed method allows you to obtain I-V characteristics in one cycle of DC analysis, taking into account the self-heating of the above-mentioned converters. A complex method of electro-thermal modeling of measuring transducers of thermal flow sensors has been developed, which includes the synthesis of a pulse temperature relaxation substitution circuit and a method of forming I-V converters in the mode of their self-heating by the supply current. It is obvious, that from the point of view of practical usage of the transistors in the circuits of measuring converters of thermal flow sensors it is necessary to provide not only the sufficient heating of the transistor structure but also the sufficient electric thermal stability of its operation. For this purpose it is necessary to use, in particular, emitting stabilizing resistors or differential connection of the pair of the transistors with current supply.

Keywords: measuring transducers, electrothermal modeling, biomedical devices and systems.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-62-68>.

Introduction

In the given section complex technique of the electric thermal modeling of the measuring converters of thermal flow sensors, is presented; it contains the synthesis of the equivalent circuit of the pulse temperature relaxation and the method of formation of converters VAC in the self heating mode by the supply current. Problems of the iteration process instability in the process of VAC analysis of the measuring converters with negative differential resistance, caused by self-heating, are considered [1,2,3].

Method of the synthesis of electric thermal models of thermoresistive, diode and transistor structures of the primary thermal flow sensors converters was suggested. Unlike the known packages of circuit modeling this method enables one to obtain VAC during one cycle of DC analysis, taking into account the self-heating of the above-mentioned converters [4,5,6,].

Method

Primary converters of thermal flow sensors can serve not only thermoresistive or diode structures but transistors, mainly bipolar n-p-n structures. Their advantage is a wide range of the supply (heating) modes and temperature measurement modes selection. Basic heating in the bipolar structures is realized by the heat release on the reverse-biased p-n junction. As it will be shown in Section 4, unlike thermoresistive converters the usage of the transistor structure enables it to form the current output that provides higher values of transducing steepness [7,8,9].

From the point of view of primary converters of thermal flow sensors, the advantage of the transistor structures as compared with the diode structures is more efficient usage of the supply circuit energy - voltage drop on diode structures, as a rule, does not exceed 0.8 V (for silicon structures), it means, in particular, that at 5 V supply source practically the whole voltage ($5 - 0.8 = 4.2$ V) drops on current forcing circuit. It is obvious that not more than 20 % of supply circuit energy will be spent on heating the diode structure. Instead, the voltage drop on the transistor structure (on reverse-biased collector p-n junction) can be randomly regulated by the resistive divider of basic circuit voltage, that provides maximum energy profit [10,11,12].

According to the problems, put forward in this section, we will consider the method of the synthesis of the electrothermal model of the transistor structures of thermal flow sensors. Analyzing the model of the bipolar transistor from the point of view of the impact of self-heating temperature on VAC, it is necessary to consider, at least, three mechanisms of temperature impact. It should be noted, that, as in the models presented before, we speak not only of the impact of the ambient temperature on the parameters of the transistor, but on its self-heating, i.e., direct impact of power released in the transistor structure on its electric physical parameters. It is obvious that model studies of self-heating must be conducted in a single cycle, when the temperature is not an independent value but is determined by the power of the transistor [13,14,15].

The first mechanism of the temperature impact is analogous to the above-mentioned diode structures - increase of temperature stipulates the decrease of voltage drop on p-n junction $V_{pn} = f_1(T)$ of the transistor structure. In case of direct connection of the transistor the temperature drift of voltage on emitter - base junction is important, and in case of inverse connection - on collector-base junction. The second mechanism is connected with the sharp increase of the reverse currents of p-n junction $I_S = f_2(T)$ in the process of their heating - mainly, reverse-biased collector-base junction. The third mechanism of the impact - it is the temperature drift of the current increase coefficient of the transistor structure $B_F = f_3(T)$. These three mechanisms were taken into consideration in the process of model development (equivalent circuit) of the electric thermal analysis of the bipolar transistor VAC (Fig. 1).

Thermal modeling of the resistive and diode structures

The given equivalent circuit is based on Ebers-Moll model (if necessary it may be based on the still more complex Poon-Gummel charging model) as well as on the principles of electric thermal modeling of the resistive and diode structures, considered in the previous sections [16,17,18].

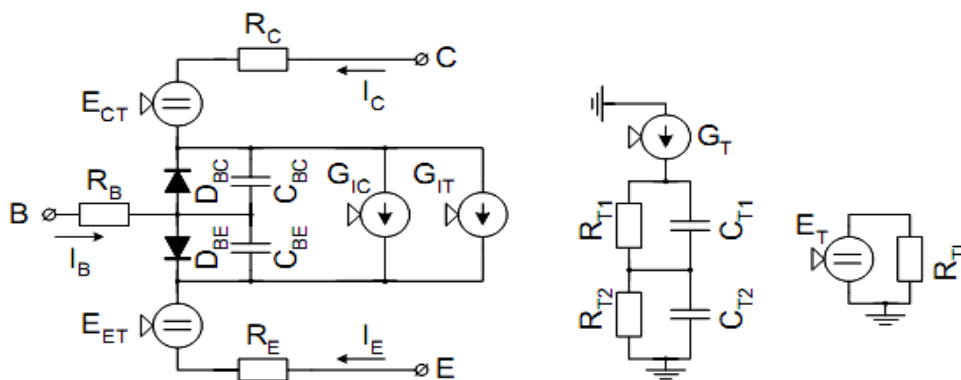


Figure 1 –Model of electric thermal analysis of the bipolar transistor VAC

Conventional for Ebers-Moll model [1, 2] is emitter and collector p-n junction D_{BE} , D_{BC} , stray barrier capacitance of which is presented by the capacitors C_{BE} , C_{BC} . Resistive components of the transistor structure are presented by the resistances of base, emitter and collector sections R_B , R_E , R_C . Current transmission coefficient of the structure is described by the controlled current source G_{IC} . Mathematical presentation of such a traditional transistor model is described in detail in the monographs and instruction manuals, using PSpice or MicroCAP packages [2, 3], that is why, its further consideration is not performed [19,20,21].

The characteristic feature of the suggested model is the presence of two controlled voltage sources E_{CT} , E_{ET} and controlled current source G_{IT} . Besides, the electric thermal model contains the above-considered circuits of pulse thermal relaxation G_T , R_{T1} , C_{T1} , R_{T2} , C_{T2} and thermal resistance E_T , R_{TL} . Principles of voltage sources specification E_{CT} , E_{ET} , which form temperature-dependent component of the voltage drop on the forward-biased p-n junction $\Delta V_{pn} = f_1(T)$, have already been considered in the process of the electric thermal study of the diode structures [22].

The impact of the temperature on the current of the reverse-biased p-n junction $I_S = f_2(T)$ similarly Ebers-Moll model can be represented in the form:

$$I_S T = I_{S0} \exp\left(\left(\frac{T}{T_0} - 1\right) \frac{E_G(T)}{\phi_T}\right) \left(\frac{T}{T_0}\right)^{X_{T1}}$$

where X_{T1} – is the exponent of the temperature dependence of the reverse current I_{S0} .

The reverse currents (typically not greater than several microamperes) as compared with the heating current (hundreds of milliamperes) can be neglected. However, the participation of the reverse-biased collector p-n junction current in the total basic current, amplified several hundreds of times, cannot be neglected. That is why, it is expedient to combine it with the third mechanism - temperature drift of current amplification factor of the transistor structure $B_F = f_3(T)$:

$$B_F(T) = B_F \left(\frac{T}{T_0}\right)^{X_{TB}}$$

where X_{TB} – is the exponent of the temperature dependence of the current amplification factor B_F . This combined mechanism is presented by the controlled source G_{IT} .

Demonstration of the efficiency of the developed electric thermal model

For the demonstration of the efficiency of the developed electric thermal model of the transistor self heating we will consider two typical results of its output VAC modeling (Fig. 2-5).

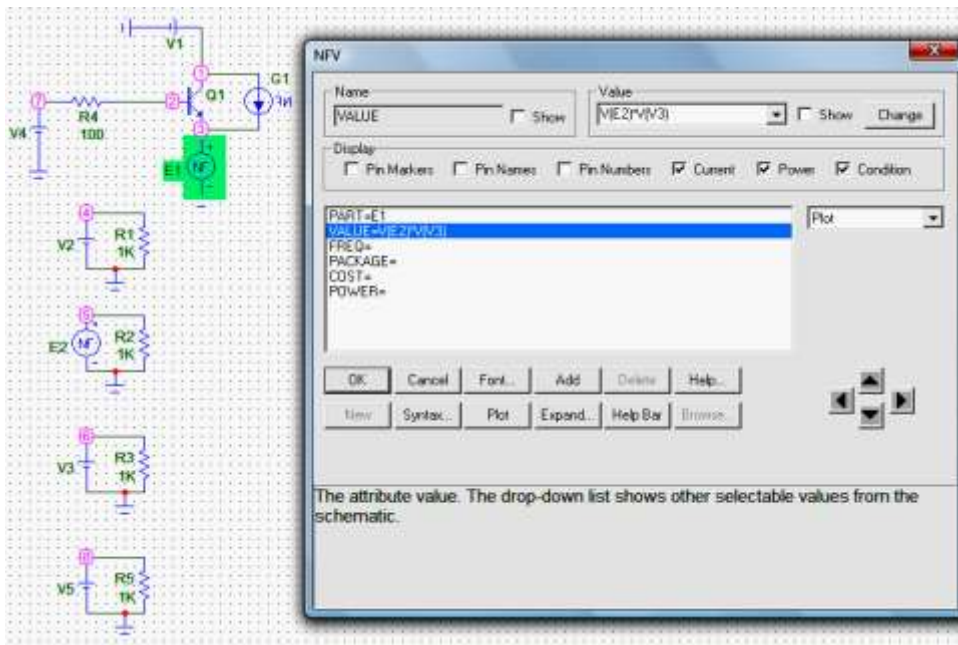


Figure 2 – Specification of the controlled voltage source of the electric thermal model of the bipolar transistor

To simplify the results, given below, not a separate components of the transistor equivalent circuit are used but the conventional Ebers-Moll model (n-p-n transistor Q1) is used, the given model, for carrying out the electric thermal modeling is supplemented with the corresponding controlled sources: source E1 describes functional dependence $\Delta V_{pn} = f_1(T)$, source G1 - functional dependencies $I_S = f_2(T)$ and $B_F = f_3(T)$, source V2 - thermal resistance of the transistor structure, source E2 - overheating temperature of the structure, relatively the ambient temperature, source V3 – TKV_{pn} coefficient, and source V5 – coefficients X_{T1} and X_{TB} . The supply voltage of the collector circuit is supplied from the source V1, and base circuit - from the source V4 and resistor R4.

Experimental results

The first result of modeling (Fig. 3) is obtained only with the account of the temperature dependence of the voltage drop on the emitter p-n junction. It can be seen that if the transistor current increases (signal 1), its heating occurs and (signal 2) voltage drop decrease on the emitter p-n junction (signal 3) takes place. These effects increase if the thermal resistance (graphs a, b, c) of the transistor structure increases.

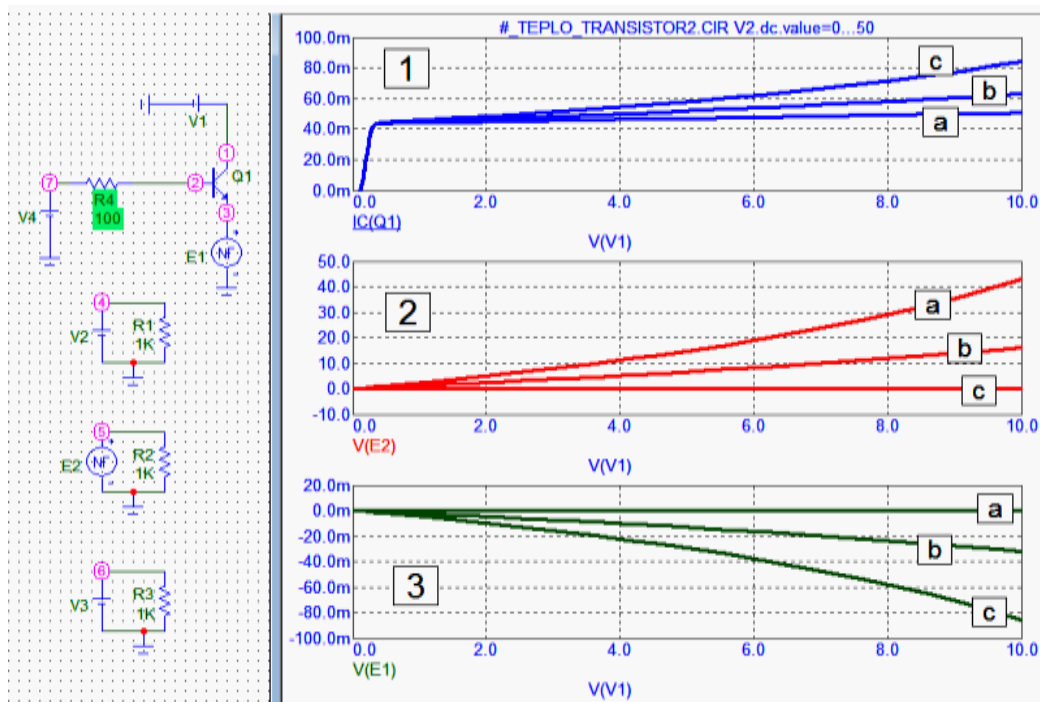


Figure 3 – Result of DC analysis of the bipolar transistor output VAC with the account of $V_{pn} = f_1(T)$ mechanism at several values of the thermal resistance Z_Q

The second result of modeling (Fig 4) takes into account all the above-considered mechanisms of the temperature impact. As it is seen, the modulation of the transistor VAC in the process of its self heating is greater, it is stipulated not only by the temperature drift of the voltage on the emitter p-n junction but also by the increase of the current amplification coefficient of the transistor in the process of its self-heating.

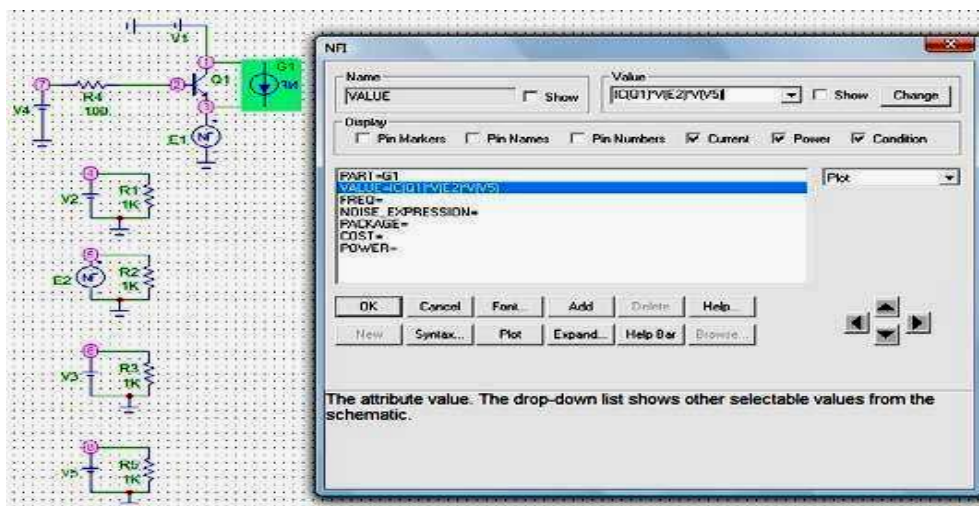


Figure 4 – Specification of the controlled current source of the bipolar transistor electric thermal model

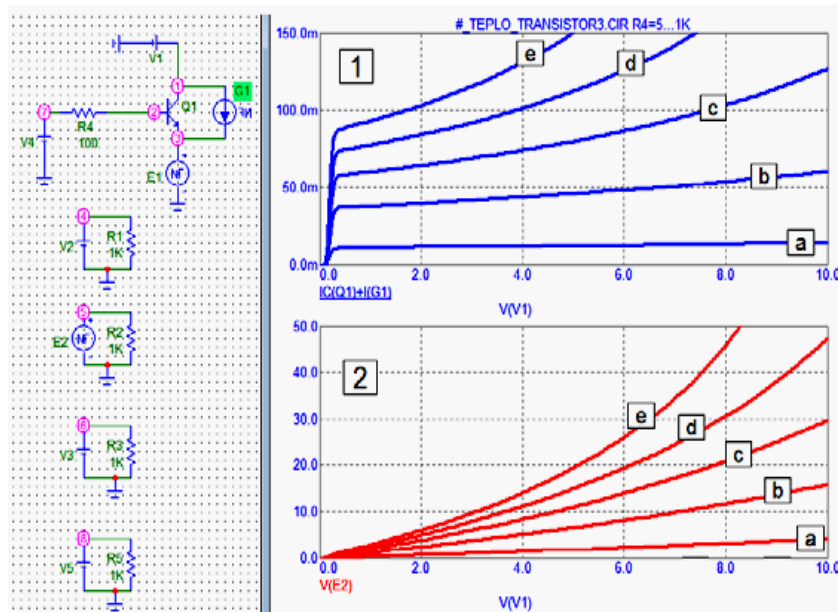


Figure 5 – Result of DC analysis of bipolar transistor VAC with the account of the mechanisms $V_{pn} = f_1(T)$, $I_S = f_2(T)$, $B_F = f_3(T)$ at several values of thermal resistance Z_Q

Conclusions

1. It is obvious, that from the point of view of practical usage of the transistors in the circuits of measuring converters of thermal flow sensors it is necessary to provide not only the sufficient heating of the transistor structure but also the sufficient electric thermal stability of its operation. For this purpose it is necessary to use, in particular, emitting stabilizing resistors or differential connection of the pair of the transistors with current supply.
2. A method of synthesis of electrothermal models of thermoresistive, diode and transistor structures of primary converters of thermal flow sensors is proposed. In contrast to well-known circuit modeling packages (PSpice or MicroCAP), the proposed method allows you to obtain I-V characteristics in one cycle of DC analysis, taking into account the self-heating of the above-mentioned converters.
3. A complex method of electro-thermal modeling of measuring transducers of thermal flow sensors has been developed, which includes the synthesis of a pulse temperature relaxation substitution circuit and a method of forming I-V converters in the mode of their self-heating by the supply current.

References

- [1] Y. Fang and W. W. Liou. Computations of the Flow and Heat Transfer in Microdevices Using DSMC With Implicit Boundary Conditions // J. Heat Transfer. – 2002. – Vol. 124. – P. 338–345.
- [2] W.W. Liou and Y. Fang. Implicit Boundary Conditions for Direct Simulation Monte Carlo Method in MEMS Flow Predictions // CMES. – 2000. – Vol. 1, No. 4, – P. 119–128.
- [3] Y. Weiping, L. Chong, L. Jianhua, M. Lingzhi and N. Defang. Thermal distribution microfluidic sensor based on silicon // Sensors and Actuators B. – 2005. – Vol. 108. – P. 943–946.
- [4] B.W. van Oudheusden. Silicon thermal flow sensors // Sensors and Actuators A: Phys. – 1992. № 30. – PP. 5–26.
- [5] M. Ashauer, H. Glosch, F. Hedrich, N. Hey, H. Sandmaier, W. Lang. Thermal flow sensor for liquids and gases based on combinations of two principles // Sensors and Actuators A. – 1999. Vol. 73. – PP. 7–13.
- [6] F. Jiang, Y.-C. Tai, C.-M. Ho, R. Karan, M. Garstenauer. Theoretical and experimental studies of micromachined hot-wire anemometers // International Electron Devices Meeting (IEDM), San Francisco, December 11–14. – 1994. PP. 139–142.
- [7] J.J. van Baar, R.W. Wiegerink, T.S.J. Lammerink, G.J.M. Krijnen, M. Elwenspoek. Micromachined structures for the thermal measurements of fluid and flow parameters // J. Micromech. Microeng. – 2001. – № 11. – PP. 311–318.

- [8] T. S. T. Lammerink, N. R. Tas, M. Elwenspoek, J. H. J. Fluitman. Micro-liquid flow sensor // *Sensors and Actuators A*. – 1993. – PP. 45-50.
- [9] P.M. Handford, P. Bradshaw. The pulsed-wire anemometer // *Exp. Fluids* 7. – 1989. – PP. 125–132.
- [10] Ellis Menga, Po-Ying Li, Yu-Chong Tai. A biocompatible Parylene thermal flow sensing array // *Sensors and Actuators A*. – 2008. № 144. –PP. 18–28.
- [11] A. Margelov. Honeywell gas flow sensors [Electronic resource] / A. Margelov // *Chip News*. — 2005. — № 9 (102). — С.56—58.
- [12] Z.Yu. Gotra, R.L. Holyaka, S.V. Pavlov, S.S. Kulenko, O.V. Manus Differential thermometer with high resolution // *Technology and construction in electronic equipment*. - 2009. - No. 6 (84). - P. 19 - 23.3.Ю.
- [13] Pavlov S. V. *Information Technology in Medical Diagnostics* //Waldemar Wójcik, Andrzej Smolarz, July 11, 2017 by CRC Press - 210 Pages.
- [14] Wójcik W., Pavlov S., Kalimoldayev M. *Information Technology in Medical Diagnostics II*. London: (2019). Taylor & Francis Group, CRC Press, Balkema book. – 336 Pages.
- [15] *Highly linear Microelectronic Sensors Signal Converters Based on Push-Pull Amplifier Circuits* / edited by Waldemar Wojcik and Sergii Pavlov, Monograph, (2022) NR 181, Lublin, Comitet Inzynierii Srodowiska PAN, 283 Pages. ISBN 978-83-63714-80-2.
- [16] Pavlov Sergii, Avrunin Oleg, Hrushko Oleksandr, and etc. System of three-dimensional human face images formation for plastic and reconstructive medicine // *Teaching and subjects on bio-medical engineering Approaches and experiences from the BIOART-project Peter Arras and David Luengo (Eds.)*, 2021, Corresponding authors, Peter Arras and David Luengo. Printed by Acco cv, Leuven (Belgium). - 22 P. ISBN: 978-94-641-4245-7.
- [17] Kukharchuk, Vasyl V., Sergii V. Pavlov, Volodymyr S. Holodiuk, Valery E. Kryvonosov, Krzysztof Skorupski, Assel Mussabekova, and Gaini Karnakova. 2022. "Information Conversion in Measuring Channels with Optoelectronic Sensors" *Sensors* 22, no. 1: 271. <https://doi.org/10.3390/s22010271>
- [18] Avrunin, O.G.; Nosova, Y.V.; Pavlov, S.V.; Shushliapina, N.O.; and etc. Research Active Posterior Rhinomanometry Tomography Method for Nasal Breathing Determining Violations. *Sensors* **2021**, *21*, 8508. doi: 10.3390/s21248508, <https://www.mdpi.com/1424-8220/21/24/8508>.
- [19] Avrunin, O.G.; Nosova, Y.V.; Pavlov, S.V.; and etc. Possibilities of Automated Diagnostics of Odontogenic Sinusitis According to the Computer Tomography Data. *Sensors* 2021, 21, 1198. <https://doi.org/10.3390/s21041198>.
- [20] Vasyl V. Kukharchuk, Sergii V. Pavlov, Samoil Sh. Katsyv, and etc. "Transient analysis in 1st order electrical circuits in violation of commutation laws", *PRZEGLĄD ELEKTROTECHNICZNY*, ISSN 0033-2097, R. 97 NR 9/2021, p. 26-29, doi:10.15199/48.2021.09.05.
- [21] *Sensors of electric magnetic radiation for bioengineering research* / G. S. Tymchyk; V. I. Skytsiuk, M. A. Waintraub, T. R. Klochko. – K. : S.E. Lesia, 2004. – 64 p.
- [22] Osadchuk O. V Microelectronic frequency converters on the base of the transistor structures with negative resistance / O. V. Osadchuk. – Vinnytsia: UNIVERSUM- Vinnytsia, 2000. – 303 p.

Надійшла до редакції 20.03.2024

Видано за грантової підтримки Національного фонду досліджень України в рамках проекту 2022.01/0135 "Розробка лазерно-фотонного лікувально-діагностичного комплексу медичної реабілітації пацієнтів з політравмами різного ступеня важкості"

Information about authors

Pavlov Sergii – D.Sc., Professor of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

Wójcik Waldemar – D.Sc., Professor, director of the Institute of Electronics and Information Technology at Lublin University of Technology. Doctor Honoris Causa of five Universities in Ukraine and Kazakhstan

Holyaka Roman – D.Sc., Professor of Electronic Device of Information-Computer Technologies Department, Lviv Polytechnic National University

Azarov Olexiy – D.Sc. Professor, head of Computer Technology Department, Vinnytsia National Technical University

Nykyforova Larysa - Doctor of Technical Sciences, Professor of the Department of Automation and Robotic Systems named after Academician I.I. Martynenko, *National University of Life and Environmental Sciences of Ukraine*

Kaduk Oleksandr - Ph.D., associate professor associate professor of Computer Engineering Department, Vinnytsia National Technical University

С.В.Павлов¹, Вальдемар Вуйцік², Р.Л. Голяка³, О.Д. Азаров¹,
Л.Є. Никифорова⁴, О.В. Кадук¹

ЕЛЕКТРОТЕРМІЧНЕ МОДЕЛЮВАННЯ ТЕМПЕРАТУРНО-ЗАЛЕЖНИХ ВАХ ПЕРЕТВОРЮВАЧІВ ТРАНЗИСТОРНОГО ТИПУ В БІОМЕДИЧНІЙ ІНЖЕНЕРІЇ

¹Вінницький національний технічний університет

²Люблінський університет технологій, Польща

³Національний університет «Львівська Політехніка»

⁴Національний університет біоресурсів та природокористування України

УДК 004.056:681.2

В.І. Маліновський, Л.М. Куперштейн, В.В. Лукічов

**МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ КІБЕРЗАГРОЗ ТА ІНФОРМАЦІЙНИХ
ВПЛИВІВ У МІКРОКОНТРОЛЕРАХ**

Вінницький національний технічний університет

Анотація. В роботі наведено матеріали окремих досліджень аналізу впливу кіберзагроз на інформаційні процеси в мікроконтролерах (МК). Проведено оптимізацію існуючої математичної моделі кіберзагроз та оцінювання інформаційних впливів, а також виконано оцінку і аналіз основних інформаційних ризиків кіберзагроз у мікроконтролерах, які працюють в складі систем управління різноманітних як загальних, так і спеціалізованих пристроїв. Проведено вдосконалення математичної моделі кіберзагроз для оцінки кіберзагроз у мікроконтролерах із врахуванням факторів самих інформаційних впливів. Визначено основні показники оцінки ризиків кіберзагроз в мікроконтролерах, які враховуються в математичній моделі кіберзагроз для інформаційної системи мікроконтролерів. Вдосконалена математична модель описує сумарний вплив інформаційних загроз та втручань та основні вектори кібератак у МК. Дана модель також дозволяє оцінювати додаткові шкідливі фактори впливу та інформаційні втручання по вторинним каналам із метою їх врахування та компенсації. Проведене комп'ютерне моделювання показало на практиці результати і характер впливу кіберзагроз на інформаційну безпеку МК. Модель дозволяє визначати та оцінювати вплив домінуючих кіберзагроз на основні аналізу основних ризиків у мікроконтролерах, які працюють в складі складних систем та систем Інтернету речей. В роботі також наведено розвиток основних положень по створенню векторної математичної моделі оцінки загроз та впливів у МК, що може бути використано при формуванні повної векторної моделі та методу оцінки впливів і загроз на стан інформаційної безпеки і стабільності функціонування МК. Це може дати змогу оцінити основні показники стабільності роботи як окремих блоків, так і всієї інформаційної системи мікроконтролера. Модель також може дозволити проводити оцінку усереднених значень впливів інформаційних втручань на стабільність функціонування МК, оцінювати величину усереднених кіберзагроз і вразливостей інформаційної системи мікроконтролера. Запропонована модель призначена і може бути використана при розробці методу підвищення рівня інформаційної захищеності мікроконтролерів та суміжних схем для забезпечення їх більш стабільного і безпечного функціонування.

Ключові слова: кіберзахист, кіберзагроза, інформаційна безпека, вразливість, мікроконтролер, модель.

Abstract. The paper presents the research materials of the analysis cyber threats and their influences on information processes in microcontrollers (MC). The optimization of the existing mathematical model of cyber threats influences (impacts) on the information assessment was carried out. Also was performed the evaluation and analysis of the main information risks of cyber threats in microcontrollers, which work as part of control and automation systems of various general and specialized devices. The mathematical model of cyber threats has been improved for the more data assessments of cyber threats in microcontrollers systems, taking into account the interference of factors of the informational influences. The main indicators of the risk assessment of cyber threats in microcontrollers are determined, which are taken into account in the mathematical model of cyber threats for the information system of microcontrollers. The improved mathematical model describes the total impact factors of information threats, its influences and the main vectors of cyber attacks in MC. This model also will describe and makes possible to evaluate additional harmful factors, and information influences through secondary channels on the data processes in MC's with the aim of its compensation compensating. The performed researches by computer simulations and modeling were shown in practice the results and their nature of the cyber threats influences on information security of the MC's. The model allows determine and assess the impact of dominant cyber threats and the main risks in microcontroller information systems, what work as part of complex automation systems or Internet of Things devices. The work also provides the development of the main principles of the creating a vector mathematical model which will describe and assesses the impacts of the cyber threats on MC's. Its results can be used for the formation of a complete vector mathematical model and method for precision assessing of the cyber threats effects in MC's for its more information security and stability. This can make it possible to evaluate the main stability indicators of entire information system of the microcontroller. The model can also make possible to estimate the average values of the effects of information influences on the stability of the functioning of the MC. It also can estimate of the averaged value of cyber threats impacts for determine of main vulnerabilities in information system of the microcontroller. The proposed model is designed and can be used for the future further development of a method for increasing of the information security level of microcontrollers and their adjacent circuits for ensure their more stable and safe functioning.

Key words: cyber protection, cyber threat, information security, vulnerability, microcontroller, model.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-69-82>.

Вступ

Сучасні технології інформаційних систем на базі мікроконтролерів та мереж досить активно набувають динамічного стрімкого розвитку в останні роки і впроваджуються у все ширші сфери людської діяльності. Новітні технології інформаційних систем на базі мікроконтролерів впроваджені і впроваджуються й досі у вже досить широке поле пристроїв у всіх сферах людської діяльності і продовжують розширюватись і еволюціонувати [1]. Мікроконтролери (МК) все більше входять до складу широкого спектру пристроїв як загального, так і спеціального призначення і посідають центральне місце в основних ланках систем управління, автоматики і робототехніки та забезпечують керування сучасними цифровими пристроями [1, 2]. МК керуються і програмуються із використанням сучасних середовищ розробки функціональних мікропрограм на базі гнучких алгоритмів у системних мовах програмування C, C++, Assembler, що дозволяє будувати достатньо гнучкі стабільні системи управління на базі МК.

МК набули особливо великих значень і темпів в останні роки: від впровадження в традиційні МК системи, і до впровадження МК в спеціалізовані системи, як працюють в складі цифрових систем із залученням високорівневих ІТ-технологій [1-2, 4].

Але існує проблема стабільності і кібербезпеки основних робочих циклів мікропрограми МК та проблема несанкціонованих зовнішніх інформаційних втручань та впливів у МК по основним інтерфей-

сам і побічним (стороннім) каналам [1]. Кіберзагрози і інформаційні втручання за рахунок несанкціонованих підключень по стороннім вторинним каналам у МК можуть стати причиною нестабільності і відмов функціонування підпрограм мікроконтролера і наслідком виведення із ладу всієї системи управління на базі МК [1-4]. Тому кібербезпека інтерфейсів і вторинних каналів, а також мікропрограми МК (прошивки мікроконтролерів) та їх основних інформаційних процесів – складна і до кінця не вирішена проблема, яка потребує оцінки і комплексного підходу та й досі актуальна [1].

Оцінка кіберзагроз і впливів по основним та вторинним каналам в МК – актуальна та необхідна проблема, яка потребує якісного і ефективного вирішення. Базовим у рішенні цієї проблеми на попередньому рівні є завдання розробки нової чи удосконалення існуючої математичної моделі оцінки факторів впливу на інформаційні процесів в МК. Це дозволить оцінити та врахувати ці фактори в основних процесах МК і дасть змогу отримати відповідь на питання «як протидіяти чи компенсувати впливи і кіберзагрози у сучасних мікроконтролерах?».

Метою статті є вдосконалення математичної моделі оцінювання кіберзахищеності інформаційної системи мікроконтролерів на основі розширення механізму оцінювання впливу інформаційних втручань і кіберзагроз на інформаційну стабільність процесів у мікроконтролерах, що враховує сумарний і окремі фактори впливу кіберзагроз.

Очікується, що математична модель буде достатньо точно оцінювати стан безпеки інформаційної системи мікроконтролера (МК), із врахуванням оцінки ризиків і сучасних кіберзагроз для мікропрограм та інформаційної системи МК.

Відомі підходи опису кіберзагроз та впливів у мікроконтролерах

Відома математична модель оцінки впливу кіберзагроз в інформаційних системах і схемах у вигляді математичної моделі порушника кібербезпеки інформаційної системи [5]. Ця модель досить добре описує процеси у взаємопов'язаних модульних комплексних інформаційних системах.

Також відомі моделі шкідливого впливу на відмовостійкість інформаційних систем [6] та моделі вразливостей апаратного забезпечення кіберфізичних систем [7], якими є системи із мікроконтролерами.

В контексті безпеки система управління із мікроконтролерами, перспективним є завдання вдосконалення і адаптування математичної моделі саме для мікроконтролерів із оцінкою впливу кіберзагроз та негативних факторів впливу по первинним та вторинним каналам у МК. Також модель повинна враховувати ризики для інформаційної системи самого МК. Для цього необхідно реалізувати синтез відомих моделей дестабілізуючих факторів кіберзагроз і впливів у МК.

Одним із супутніх завдань кіберзахисту МК і його підпрограми – є актуальні і точні оцінки впливу загроз, а також оцінки наслідків від їх впровадження у МК та супутні системи контролю. Для цього потрібна адаптація математичної моделі оцінки стану безпеки і оцінки кіберзагроз саме для інформаційної системи мікроконтролерів із врахуванням як факторів впливу, так і факторів захисту.

Проблематика аналізу і чисельної оцінки кібербезпеки системи мікроконтролера

Досить часто задачі аналізу стану локального захисту окремих ресурсів в архітектурі МК і захисту даних прирівнюються до завдання забезпечення повної кібербезпеки всієї системи мікро контролера [1]. Але досить часто це не відповідає реальному стану речей і необхідному рівню захисту, так як на локальному рівні можна захистити тільки конкретні ресурси. Наприклад, в кінцевих пристроях і інтерфейсах МК [1, 4, 6, 7] захист даних та інформаційних процесів в інформаційній системі мікроконтролера (ІС МК) не може гарантувати 100%-го захисту даних, що знаходяться у пам'яті та інших ресурсах МК. Тому аналітика локального захисту не вирішує завдання опису і моделювання повного комплексного захисту усєї системи інформаційної системи мікроконтролера. До того ж, неповнота, окремих функцій та аргументів в існуючих моделях та відсутність динамічних оцінок впливів призводять до низького рівня відповідності реальних процесів кіберзагроз у ІС МК та їх не вірної оцінювання. Тому завдання розробки математичної моделі для оцінки і врахування адекватного впливу повинно базуватись на:

- на аналізі самих інформаційних процесів кіберзагроз в МК;
- на оцінці впливів їх окремих компонент;
- на оцінці комплексного впливу багатьох факторів кіберзагроз в МК;
- на точному визначенню основних і супутніх факторів інформаційних втручань у МК;
- на оцінці вектору атаки і профілю захищеності МК – системи;
- на аналізі самих типів і факторів кіберзагроз і їх впливів на інформаційний процес МК системи.

Тому задача оцінки ризиків прояву кіберзагроз у МК зводиться до розроблення методики і математичної моделі оцінювання ризиків і опису процесів інформаційних впливів із максимальним врахуванням факторів впливу (факторів кіберзагроз) на МК-систему. Також важливо, щоб математична модель, яка буде вдосконалюватись враховувала вплив загроз «0-го» дня і найбільш впливові кіберзагрози, які можуть становити значні ризики і повинні бути враховані. Модель повинна бути максимально адекватною і простою в оперуванні, повинна дозволити проводити аналіз інформаційної МК системи.

Варіанти і типи кіберзагроз для МК продовжують збільшуватись [1]. Сьогодні додаються все більше варіацій застосувань взаємопов'язаних МК пристроїв, їх протоколів і інтерфейсів МК [1-7], це призводить до збіль-

шення кількість додаткових кіберзагроз і потенційних негативних інформаційних впливів по вторинним каналам МК. Сучасні засоби інформаційних втручань в промислові МК пристрої дозволяють успішно реалізовувати шкідливий функціонал дистанційно і втручатись у процеси МК шкідливим програмним забезпеченням (ШПЗ) [1, 4-7]. Наприклад, варіанти впливу ШПЗ: Stuxnet, Flame, miniFlame, Duqu, Gauss, Regin, Wiper, Shamoon, які експлуатують вразливості програмного коду МК Meltdown and Spectre [1] та інші складні шкідливі механізми із використанням обфускації, метаморфних перетворень виконавчого коду мікромодулів ШПЗ із приховуванням їх функціоналу і ознак. Окремі варіанти такого ШПЗ впроваджуються в системи індустріального контролю в складі автоматичних систем управління технологічними процесами (АСУ ТП) та інших електронних пристроїв на базі мікроконтролерів. Це дозволяє робити ін'єкції шкідливого коду і здійснювати інформаційні втручання із порушенням штатного режиму і функціоналу МК, суміжних засобів їх функціонування.

Модель оцінки кіберзагроз у МК дозволить оцінити ступінь впливу і може бути використана при оцінці наслідків в системах, підходах і методах захисту МК від кіберзагроз та інформаційних впливів. Особливо це стосується загрозу у формі ШПЗ у вигляді мікрокоду чи ініціації сторонніх шкідливих команд чи переривань, або мікромодулів ПЗ, спеціалізованого або вузько-орієнтованого шкідливого впливу по вторинним і первинним каналам в МК. Також загрозу представляють окремі мікромодулі ПЗ, які можуть бути викликані в самій мікропрограмі МК для МК систем, яке експлуатує вразливості МК.

Все це потребує адекватної оцінки і аналітики, що можна здійснити за допомогою математичної моделі оцінки загроз в мікро контролерах.

Розробка математичної моделі оцінки інформаційних впливів і кіберзагроз в ІС МК

Основними загрозами в сучасних архітектурах мікроконтролерів розглянуті в роботах [5, 7]. В роботі [5] проводився огляд математичних моделей для безпеки в інформаційних системах. Дані принципи та інтерпретація процесів частково справедлива і для МК систем із врахуванням окремих особливостей та конкретики і жорсткості опорної архітектури мікропроцесора із врахуванням моделей безпеки «Bell and LaPadulla», «Clarck Wilson Model», «Roscoe-Woodcock» «CSP-model» [5], в яких описані підходи безпеки моделі захисту складних інформаційних систем. При розробці моделі безпеки в МК повинні використовуватись підходи імітаційного моделювання, які ґрунтуються на ймовірностях для розв'язання проблем поширення інформаційних загроз в середовищах комплексних комунікацій і розподілених блоків і окремих взаємопов'язаних обчислювальних функцій.

Так у [5] представлено математичні модель кібербезпеки інформаційної системи:

$$i(x, y) = \sum_{k=1}^l i_k(x, y) = \sum_{k=1}^l g_k \cdot p_k \cdot q_k(x) \cdot f_k(x, y) \quad (1)$$

де, x та y – ресурси нападу і, відповідно, захисту, і при цьому справедливим є співвідношення $\sum_{k=1}^l x_k = X$; $\sum_{k=1}^l y_k = Y$; k – номер об'єкта в складі МК(до об'єктів можуть бути віднесені окремі периферійні блоки в МК: наприклад, АЛП, ОЗП, ПЗП, регістри, тощо); g_k – відносна вартість інформації на k -му об'єкті (через g_k також позначається сам об'єкт); p_k — імовірність нападу на k -й об'єкт; $q_k(x)$ — щільність імовірності виділення нападом ресурсів x на k -ий об'єкт; $f_k(x, y)$ — імовірність вилучення інформації з k -го об'єкту, яку розглядаємо як динамічну вразливість об'єкта.

Дана модель [5] досить точно дозволяє описати процеси впливу в ІС (інформаційних системах) та в тому числі й у МК, але при їх взаємодії в рамках кожного інформаційного об'єкта і в сукупності, що дозволить зручно і компактно при описі впливів та різних факторів (і захисту і нападу) на об'єкт, а також дозволяє відносно оцінити ступінь впливу і взаємодії різних процесів між собою у математичному вигляді.

Також модель враховує таку відносно важливу величину (параметр) як вартість ресурсів, що є важним чинником при виборі технологій і систем захисту, а також оцінки їх ефективності. Але, вказана математична модель не враховує специфіку і характер процесів в кожному конкретному об'єкті та/або елементі інформаційної системи, а також не враховує й інтенсивність впливу різних процесів (і процесів захисту інформації і процесів нападу/атак на інформаційні ресурси) і питому вагу інформації в системі (відносний показник якості інформаційних даних в кожній конкретній підсистемі та/або об'єкту, які входять до складу системи).

Тому очевидно, що при оцінці впливу ресурсів нападу і захисту x та y – в кожному конкретному об'єкті та/або інформаційній системі потрібно враховувати специфіку інформаційного впливу із відповідними коефіцієнтами h_x, f_y , і при цьому для всієї інформаційної системи, яка складається із l об'єктів справедливим є співвідношення:

$$\sum_{k=1}^l x_k = X; \sum_{k=1}^l y_k = Y; X > X'; Y > Y'; \sum_{k=1}^l x_k h_x = X'; \sum_{k=1}^l y_k h_y = Y', \quad (2)$$

Також модель (1) і модель (2) не враховує функції ефективності нападу, і захисту $f_d(X)$; $f_d(Y)$ і відповідні коефіцієнти ефективності захисту і відбиття атак μ_{ex} і їх щільності. Ці функції ефективності нападу і захисту є залежностями від комплексного аргумента, який залежить від багатьох умов і в т.ч. й особливостей побудови об'єкта. В такому випадку функція (1), яка представляє математичну модель оцінки кіберзахищеності ІС МК перепишеться як:

$$I(X, Y) = \sum_{k=1}^l i_k(x, y) = \sum_{k=1}^l g_k \cdot p_k \cdot q_k(x) \cdot f_k(x, y) \cdot \mu_{ex}(x, y) \cdot f^d_k(x, y), \quad (3)$$

де x та y – ресурси нападу і відповідно захисту, $\sum_{k=1}^l x_k h_x = X$; $\sum_{k=1}^l y_k h_y = Y$; k – позначення і індекс/номер системного об'єкта/системного елемента (наприклад, АЛП, RAM-ROM, інтерфесу, регістру, тощо і т.п.) в МК; $f^d_k(x, y)$ – функція співвідношення ефективності захисту до нападу і до атак у інформаційній системі МК відповідно; g_k – відносна ціна(вартість) інформації на k -му об'єкті – блоці МК (окремо через g_k – може бути умовно позначений і сам блок в системі МК: наприклад окремий блок в архітектурі МК); p_k – ймовірність реалізації кіберзагрози на k -й блок в архітектурі МК; $q_k(x)$ – щільність ймовірності кіберзагроз у ресурсі x на k -й блок; $f_k(x, y)$ – функція ймовірності втрат/пошкодження/витоків інформації із k -го блоку в архітектурі МК, яку розглядаємо як динамічну вразливість k -го блоку в архітектурі МК. Прояв $f_k(x, y)$ може бути різним і призводити до: втрат; пошкодження; витоку; вилучення; модифікації даних в k -го блоку в архітектурі МК. В залежності від типу реалізації кіберзагрози; $\mu_{ex}(x, y)$ – функція ефективності захисту та ідентифікації ресурсу (функція ефективності захисту і відбиття кібератак в системі МК), $\mu_{ex}(x, y) \approx n \cdot \sum_{k=1}^l \mu_{exk}(x, y)$. Причому n – питомі коефіцієнти пропорційності і адаптації; $\mu_{exk}(x, y)$ – функція ефективності захисту та ідентифікації ресурсу одиничного k -го блоку в архітектурі МК.

В залежності від типів кібератак може бути виконані різні прояви впливів в системі МК і зокрема сам процес впровадження може бути здійснений із різним ступенем адаптації та ефективності. Без врахування ефективності, в самому простому варіанті модель (3) може мати вигляд:

$$I(X, Y) \approx \sum_{k=1}^l i_k(x, y) = \sum_{k=1}^l g_k \cdot p_k \cdot q_k(x) \cdot f_k(x, y) \cdot f^d_k(x, y), \quad (4)$$

але модель (4) не може врахувати процес ефективності процесів впровадження інформаційних впливів, що важливим і у більшій мірі враховує конкретні практичні умови, максимально наближені до реаль-
є дуже

них. Тому модель (3) є більш точною і враховує додаткові показники ніж модель (4) за рахунок введення додаткових параметрів і показників, зокрема функції ефективності нападу, і захисту до атак у інформаційній системі МК відповідно. Але в окремих випадках, коли ефективність впровадження кібератак і їх умови не дуже важлива, або нею можна знехтувати (в окремих випадках для спрощення і ототожнення простих розрахунків) може бути використана модель (4).

Як правило функція співвідношення ефективності захисту до нападу і до атак у інформаційній системі МК $f^d_k(x, y)$ та сама – функції ймовірності втрат/пошкодження/витоків інформації або їх захисту $f_k(x, y)$, мають експоненційну або квадратичну залежність, тобто $f_i(x, y) = n \cdot k \cdot e^x \cdot e^y$, або $f_i(x, y) = n \cdot k \cdot (x^2 + y^2)$. В той ж час функція ефективності захисту $\mu_{exk}(x, y)$ – як правило лінійну залежність $y = n \cdot k \cdot (x + y) + b_k$.

Функції функція співвідношення ефективності захисту до нападу забезпечує певну адаптивність системи до умов впливу та інформаційних втручань. Тому можна говорити про забезпечення певного ступеню адаптації інформаційного захисту до умов впливів і втручань (в т.ч. кіберзагроз) в мікроконтролерах.

Математична модель (4) є більш ефективною за (3), та точніше дозволяє оцінювати вплив на інформаційні об'єкти і саме у підсистемі ІС МК, що входить до складу інформаційної системи МК. А також підходить для оцінки впливу і захисту від загроз і атак (в т.ч. інформаційних втручань по побічним каналам) для мікропроцесорних систем. Ресурси нападу ілюструють множину функціоналу інформаційних зовнішніх і внутрішніх втручань в роботу основного циклу мікропрограми МК в т.ч. в порядок команд структуру і запис даних у стек пам'яті, тощо.

Модель опису загроз в (4) забезпечує розгляд по значно ширшим і вищим показникам ефективності загроз і захисту критичних даних в МК і в тому числі і МК для пристроїв IoT (Internet of Things, Інтерне-

ту речей) порівняно з іншими, непрямыми, методами. Модель може використовуватись для швидкої оцінки рівня загроз і факторів для їх попереднього аналізу у мікропроцесорних системах, в т.ч. для оперативного блокування трафіку і інформаційних потоків команд по побічних сторонніх каналах у МК IoT – по основному вектору загрози. Це такі загрози як:

- прямий і опосередкований доступ до пам'яті, доступ до регістрів, буфера ОЗП, тощо;
- переповнення /буфера, зчитування буфера при несанкціонованому доступі до нього;
- віддалене виконання коду, та/або зовнішній доступ до ліній передачі даних у МК, зчитування із зовнішніх ліній передачі даних в МК;
- зміна порядку адресації в МК, зміна/підміна значень адрес;
- окремі вразливості ядра та інших компонент, вразливості архітектури, вразливості і вплив на процеси роботи арифметико-логічного пристрою (АЛП) мікроконтролера (в т.ч. і мікропроцесора);
- доступ до ресурсів МК та до окремих регістрів (в т.ч. конфігураційних із зовні), пряму втручання/пересилка команд керування і передачі даних;
- переповнення стеку адрес, переповнення пам'яті, пряма зчитування значень стека, злам та несанкціоноване втручання в ядро системи;
- несанкціоноване втручання і зчитування і надсилання команд і даних із ліній портів мікроконтролера;
- втручання у роботу спеціальних регістрів даних та індикації стану портів введення/виведення МК;
- зміна слідування порядку команд управління та/або перехоплення їх і потоків даних як у ядрі та/або області ядра мікропроцесорної системи, так і у зовнішній периферії;
- несанкціоноване зовнішнє втручання в роботу ліній передачі даних та/або вторинних ліній – зовнішніх ліній передачі інформації і інтерфейсів в мікроконтролері. Сюди також можна віднести несанкціоноване (стороннє) пересилання/ зчитування команд керування МК, зчитування інформаційних потоків та/або окремих послідовностей блоків даних прийому/передачі даних до/від МК;
- загрози і атаки, що полягають у блокуванні обчислювального процесу за сторонніми зовнішніми вхідним і вихідним каналами в т.ч. із втручанням по вторинним функціональним каналам, і такими як енергоживлення;
- загрози «нульового дня» і загрози запуску шкідливого коду шляхом впровадження в основну підпрограму (в т.ч. загрози запуску «сліпих/порожніх» циклів в підпрограмі, зміна і переповнення пам'яті МК шляхом запуску ресурсоємного програмного коду тощо);
- інші потенційні загрози фізичного і прямого електромагнітного впливу на мікропроцесорну систему.

Підходи із використанням векторних моделей

Також, додатково модель (3) і її частковий випадок – модель (4) опису кібербезпеки інформаційної системи МК на базі поєднання комплексу технологій і різних методик захисту функціональних блоків і вузлів МК може бути доповнена математичною моделлю опису інформаційних процесів у МК. Математична модель (4) описується функцією оцінки кіберзахищеності ІС МК, в той час векторні моделі на базі марківських ланцюгів [6] дозволяють відтворювати і описувати складні інформаційні процеси в мікроконтролерах із використанням теорії графів і інформаційних системах. Це виконується за допомогою функції графів параметрів із метаданими вкладеності в моделі взаємодії інформаційних процесів. Тобто, відтворення інформаційного процесу – як явища (наприклад, основного та шкідливого процесу (процесу кіберзагрози)) описується функцією графу – або просто графом із набором векторних параметрів.

Такі графи із X_n – вершинами у вигляді парної взаємодії описуються дискретними функціями взаємодії [6]:

$$G = (X_i, E_i) \quad (5)$$

де $X_i = \{x_1, x_2, \dots, x_n\}$ – множина вершин графу; $E_i = \{e_1, e_2, \dots, e_n\}$ – множина ребер графу.

Із врахуванням модульності архітектури МК складання його із k-блоків та i-зв'язків модель (5) перепишеться:

$$G = (X_i, Y_i, R'_i, n_i) \quad (6)$$

де $Y_i = \{y_1, y_2, \dots, y_n\}$ – множина ребер графу із врахуванням їх проєкцій, $Y_i = f(E_i)$; $R'_i = \{r_1, r_2, \dots, r_n\}$ – множина граней (які пов'язані через кути) графу (метаграфу); n_i – кінцева кількість елементів множин.

Кожне ребро метаграфу об'єднує дві підмножини вершин:

1. $X_i = \{x_1, x_2, \dots, x_n\}$ – множина вершин графу;
2. $E_i = \{e_1, e_2, \dots, e_n\}$ – множина ребер графу.

Метаграфом при цьому є граф із розширеними параметрами. Множина граней метаграфу саме для ІС МК і із врахуванням особливостей модульності архітектури МК дозволяє відтворити процес в ІС МК і може бути визначена як:

$$R_k' = f_k(r_i) \cdot G_k = f_k(r_i) \cdot (X_i, Y_i) \quad (7)$$

Сама графічне представлення рівня мета графу показує взаємовплив і взаємозв'язки векторів, що описують параметри, і більш детально розглянуто у роботах опису векторних моделей [6].

Векторна модель представляється у вигляді графу процесів обробки в МК із метаданими і комплексом зв'язків у МК.

Модель, що описується формулами (6) для n -рівневого обчислювального процесу в МК передбачає, що чіткі зв'язки між елементами системи МК (наприклад, МК в пристрої IoT) існують тоді, коли зв'язки між окремими обчислювальними блоками і стадіями мікропрограми існують та чітко встановлені на верхніх рівнях взаємодії між ними. Це ж правило стосується і процесів в комунікаціях і передачі блоків даних в трактах передачі даних МК (порти та інтерфейси вводу-виводу). І наприклад, для моделі МК із 3-ма інформаційними блоками (об'єктами в архітектурі МК) формула матиме вигляд:

$$G_{comm} = f\{X_1, X_2, X_3, R_1, R_2, R_3\} \quad (8)$$

Зв'язки ребер метаграфу e_i між елементами обчислювального процесу мікропрограми МК передбачають взаємодію між елементами будь-якого рівня і включають множини [6]: $R_i = \{r_i^1, r_i^2, \dots, r_i^k\}$.

Множина процесів виконання інструкцій в інформаційній системі МК (в ядрі АЛП МК) і представлена елементами x_i (припустимо, $i=6$, АЛП - 6-й блок в архітектурі МК) в множині $X_6 = \{x_6^1, x_6^2, \dots, x_6^k\}$ із зв'язками $R_6 = \{r_6^1, r_6^2, \dots, r_6^k\}$.

Тому сусідні множини зв'язків $R_5 = \{r_5^1, r_5^2, \dots, r_5^k\}$ і $R_7 = \{r_7^1, r_7^2, \dots, r_7^k\}$ є взаємопов'язаними з $R_6 = \{r_6^1, r_6^2, \dots, r_6^k\}$ і визначаються по пов'язаним значенням і певним визначеним правилам.

Із врахуванням комплексної і модельної будови ІС МК формула (8) конкретизується і переписується у вигляді сум функції векторного добутку:

$$G = F\{X_1R_1, X_2R_2, X_3R_3, \dots, X_iR_i, \dots, X_kR_k\} \rightarrow \sum_{i=1}^k \vec{F}\{X_iR_i\} \quad (9)$$

Враховуючи область і вектор взаємодії процесів і роботи сервісів у комунікаційних трактах та інтерфейсах ІС МК, можна визначити особливості функцій і параметрів для системи характеристик параметрів МК в результаті передачі даних в комунікаціях ІС МК. Враховуючи використання стеку різних спеціалізованих протоколів і інтерфейсів, а також інколи необхідність шифрування (в окремих випадках) за допомогою спеціальних протоколів захисту даних, які працюють на вищому рівні для захисту каналу і даних в них, можна вважати, що система ІС МК в складі IoT знаходиться під впливом різних факторів і в тому числі факторів інформаційних втручань і факторів загроз кібербезпеки. Основною проблемою в МК IoT є різна обчислювальна і передавальна взаємодія окремих частин блоків команд і спільне використання ресурсів архітектури МК, що робить доступними одні частини ресурсів одних процесів доступними для інших. А також інформаційна «прозорість» інформаційно-комунікаційних трактів різних за архітектурою МК пристроїв, що створює можливості для проходження і проникнення інформаційних загроз. Крім того, специфіка і особливості використання різних архітектур і високо різність побудови МК не дозволяє використовувати традиційні моделі і засоби безпеки, орієнтовані на мультифункціональні платформи застосовувати їх до МК. Тому вирішення задач інформаційної безпеки МК вимагає комплексного диференційованого підходу і захисту комунікаційних складових, особливості архітектур МК і впливів до зовнішніх інформаційних втручань – як основного вектору атак. Проблемою є також доступність та безпека зовнішніх комунікацій при дії невизначених процесів і роботою із неперевіреними потоками даних при взаємодії МК із зовнішньою периферією у складі електронних апаратних схем (рис. 1), які також можуть бути скомпрометовані. Місця основних загроз та впливів по стороні зовнішніх інтерфейсів і портів МК у зв'язаній архітектурі мікроконтролерної системи також показано на рисунку 1.

Напрямки суміжних інформаційних втручань (в т.ч. кіберзагроз несанкціонованого дистанційного доступу чи DDoS-атак в МК) у комплексній мікропроцесорній системі із різними взаємопов'язаними МК та іншими елементами, які показані на рис. 1 можуть бути комплексними і описуватись моделлю (8), за умови вірної побудови і врахування зв'язків між блоками і процесами. Наявність додаткових інформаційних комунікацій і блоків в інформаційній системі із МК є додатковим фактором загроз і ризиків інформаційної безпеки для МК системи ($i+1$), яка повинні бути враховані в моделях (5) та (8). По функції інформаційного впливу це наближено до оцінок, які дані у [5]. Це приблизно відповідає залежностям: $G_{comm} = f\{X_i, X_{i+1}, R_i, R_{i+1}\} = f(x, y)$.

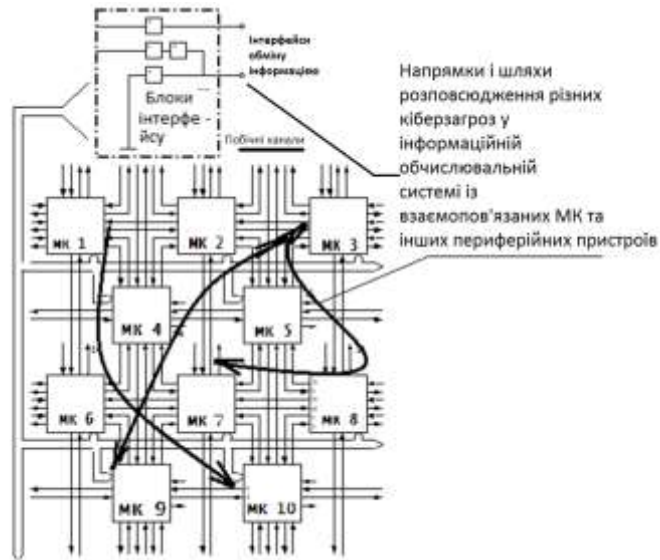


Рисунок 1 – Напрями розповсюдження потенційних інформаційних впливів (в т.ч. кіберзагроз) в комплексній та пов'язаній електронній системі на базі МК і окремих інформаційних блоків

Можна показати результати моделювання математичної моделі (4) і провести умовну оцінку характеру функції впливу для 3-х елементної системи, як це показано на рис. 2.

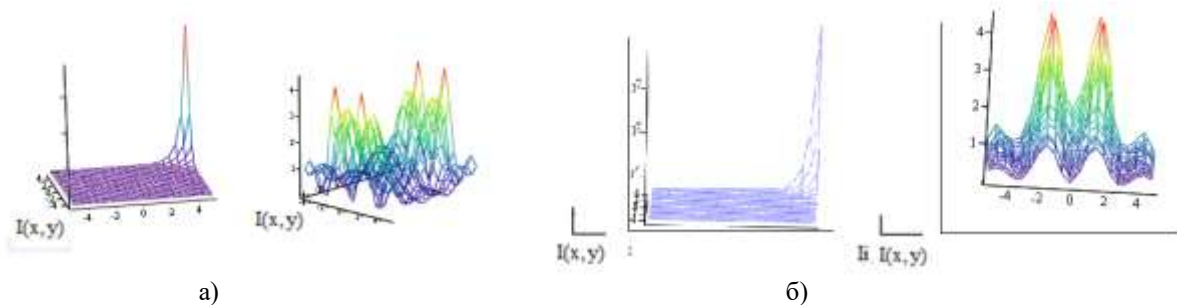


Рисунок 2 – Вигляд інтегральної функції комплексних впливів та втручань у інформаційний процес у мікропрограмі МК по моделі (4): а) вигляд функції поверхні (частковий випадок впливу загроз у ІС МК із 3-ма параметрами та частковим випадком ($k=3$; $d=1$; $i=3$); б) вигляд функції інтегрального впливу з іншого боку (під іншим кутом вигляду)

Оскільки за моделлю (3) та (4), інтегральна функція комплексних впливів та втручань у інформаційний процес у ІС МК є функцією 2-х змінних – фона формує графік поверхні. Результати моделювання (рис. 2) по моделі (3) свідчать, що цей графік поверхні має лавиноподібний пік, що характеризує різкий і стрімкий вплив інтегральних складових кіберзагроз на інформаційний процес у МК починаючи із деякого порогового значення. Це також і свідчить про суттєвий і швидкий стрибок у інформаційному процесі в ІС МК: різкий негативний вплив на функціонал інформаційного процесу МК, який значно зростає починаючи із деякого порогу. Починаючи із певного значення. Враховуючи баланс ресурсів моделі (3) - (4) та функції співвідношення ефективності захисту до нападу і до атак $f_k^d(x, y)$ у ІС МК, аналітично можна стверджувати, що відстань від початкової 0-ї точки координат до цього піку буде залежати від вхідних параметрів системи в моделі (3) - (4) і буде домінуючи залежати від самої функції ймовірності втрат/пошкодження/витоків інформації $f_k(x, y)$. Сам характер функції (рис. 2), як зазначалось вище, може мати нелінійний (експоненційний або квадратичний) прояв, в залежності від вхідних умов. Динаміка та експериментальні дослідження це підтверджують.

Як видно із рис. 2, комплексний вплив інформаційних впливів у ІС МК має узагальнюючий інтегральний нелінійно-наростаючий характер із пропорційним збільшенням величини амплітуди функції, в залежності від числа і значень факторів кіберзагроз у МК. Тобто, як видно із рис. 2: із ростом числа каналів впливів і загального числа факторів загроз, сумарна функція впливу збільшується пропорційно із їх збільшенням.

На рис. 3 показані графіки цієї ж інтегральної функції комплексних впливів та втручань у інформаційний процес у мікропрограмі МК по моделі (3)-(4), за умов певного спрощення і обмеження вхідних умов, коли функція моделі (4) представляється функцією однієї змінної $I(x, y) \rightarrow I(x)_{\lim_{f_k(x, y) \rightarrow 0}}$. Тобто в моделі (3)-(4) показано, що функція двох змінних в результаті деякого спрощення початкових умов замі-

нюється функцією однієї змінної ($df(x,y) \rightarrow df(x)/y \rightarrow const$) із зведенням цієї функції до одновимірної функції при числовому заданні другої змінної у вигляді кінцевої константи на скорочених вхідних проміжках даних. В таких умовах графік може бути представлена функцією однієї змінної для задачі спрощення моделювання і чисельних задач. Графік такої функції є вже двовимірним графіком і включає спрощення завдання моделювання моделі (3)-(4), і показаний на рис. 3.

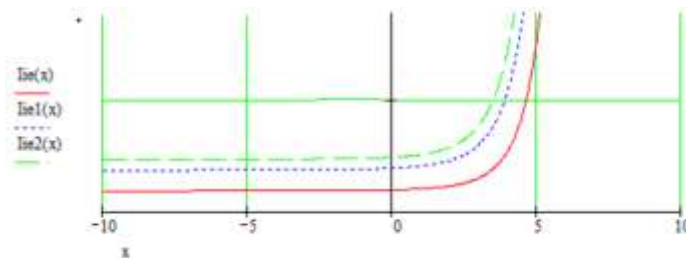


Рисунок 3 – Вигляд спрощеної інтегральної функції комплексних впливів та втручань у інформаційний процес в ІС МК по моделі (4): вигляд деякого числа спрощених функцій із 3-ма параметрами ($k=3; d=1; i=3$)

При побудові моделі у МК із моделюванням функцій розподіл зв'язків вкладень інформаційних процесів взаємодії у МК були враховані взаємозв'язки факторів множин e та X у моделях (3), (4), (6) та (8).

Математичні моделі що описуються формулами(3), (6) та (9) на відміну від існуючих враховують особливості модульності будови архітектури МК і безпековий вектор основних загроз – взаємопов'язані графи процесів в т. ч. вплив компонент графа із комунікаційні трактив МК та їх взаємозв'язки, а також множину піделементів взаємодії різних інформаційних процесів між собою в МК, а також і в його пам'яті.

Підходи до методу мінімізації ризиків кіберзагроз із врахуванням варіабельних факторів

Підходи до методу мінімізації ризиків полягають в тому, що якщо відома чи може бути простежена залежність між ресурсами нападу і ресурсами захисту, тобто $x=f(y)$, згідно (1), то можна згенерувати чи компенсувати негативний вплив ресурсів нападу $x \rightarrow x'$, $x' = f(y, x)$ та $y = f(x', x)$ та самої ефективності нападу(як показано у (4)), і таким чином зменшити вплив на інформаційний процес негативного фактору впливу ресурсів нападу: $f_k(x, y) \rightarrow f_{k \min}(x, y)$ у основному інформаційному процесі k -го блоку в архітектурі МК $i_k(x, y)$.

Основна ідея підходу методу мінімізації ризиків втручань в інформаційний процес МК полягає у тому, що якщо відома чи може бути визначена дія чи величина впливу кіберзагрози, відповідно може бути згенерована відповідна величина функції корекції в моделі (3) і (4), яка компенсує вплив:

$$f'_d(X) = F(f_d(Y)); f'_x(x,y) \rightarrow f_{x \min}(x,y); \mu_{ex}(y,x) \rightarrow \mu_{ex \max}(y,x); \quad (10)$$

Одними з найбільш поширених моделей для оцінювання інформаційної безпеки є стохастичні ймовірнісні моделі, що ґрунтуються на ризиках [7, 8]. Зокрема, до таких належать ті, що дозволяють оцінювання ймовірності подій, які відбуваються за певним сценарієм. Тоді використовується така формула для обчислення ймовірності небажаної події X та R :

$$P(X)_{MK} = \sum_i^n \overline{P(X | R_i)} \cdot \overline{P(R_i)}, \quad (11)$$

де $P(R_i)$ – ймовірність реалізації події кіберзагрози чи інформаційного втручання R_i ; $P(X/R_i)$ – ймовірність виникнення події кіберзагрози X внаслідок гіпотези R_i .

Для зручності при ресурсному підході до оцінювання інформаційної безпеки результати формалізують в таблиці (табл. 1).

Заповнення таблиці 1 і визначення ймовірностей і типу загроз для МК відбувається поблоково в залежності від його архітектури і наявності блоків по формулі (11), індивідуально в кожному окремому випадку.

При коректному визначенні інформаційних ресурсів в ІС МК – сума ймовірностей в останньому рядку таблиці повинна наближатись до одиниці: $P_{kSUM}(X_{SUM}) \rightarrow 1$, що описує повну групу подій. Відповідно на основі оцінок цих ймовірностей та ймовірностей виникнення загроз інформаційному ресурсу визначити ймовірність настання хоча б однієї з них, використовуючи формулу, наведену вище оцінюють інтегральну ймовірність для всього об'єкту.

Для оцінки рівня впливу загрози та інформаційних втручань в трактах МК і в його трактах комунікацій (побічний канал) для інформаційних систем МК запропоновано використовувати оцінку відповідності ДОС-стандартів CVSS, та отримувати інтегральні оцінки для МК-системи із орієнтованими на комплексну взаємодію факторів і взаємозв'язки різних інформаційних частин мікропрограми МК між собою (формули (3)-(7)). Так , рівень інформаційних втручань можна наближено оцінити за допомогою (4).

Таблиця 1 – Табличне представлення загроз і факторів впливу у моделі кібербезпеки МК

Назва і тип загрози та її ймовірність	Інформаційні блоки (системні об'єкти) в складі архітектури МК			
	Інформ. блок 1 (наприклад, АЛП)	Інформ. блок 2 (наприклад, ОЗП)	Інформ. блок і	Інформ. блок k (наприклад, ПЗП)
Загроза1, $P_1(X_1)=0.2$	0.22*	0.21*	...	0.24*
Загроза2, $P_2(X_2)=0.3$	0.31*	0.32*	...	0.34*
...
Загрозаі, $P_i(X_i)=0.1$	0.13*	0.12*	...	0.11*
Загроза k (k =i+1), $P_k(X_k)=0.05$	0.051*	0.052*	...	0.053*
Сумарно по всім загрозам $i=1 .. N$	По всім інформаційним блокам(об'єктам) МК: $k=1 .. N$, $P_{kSUM}(X_{SUM}) = 1$			

*-знак вказує на те, що значення ймовірностей введені для прикладу для окремого часткового випадку.

Запропонована модель оцінки фактору кіберзагроз і інформаційних втручань у ІС МК може з високою ефективністю і точністю використовуватись у діагностиці функціонального стану МК в т. ч. і на практиці.

На базі моделі рис. 2 враховуючи основний вектор загрози – напрямки каналної передачі даних по зовнішнім вторинним каналам та інтерфейсам МК, було запропоновано модель із врахуванням багатоканальності впливу і забезпеченням комплексного захисту даних на базі комутації каналів із використанням різних протоколів обміну, а також шифрування даних в МК у різні періоди часу із періодом T_b , в моделі захисту каналів інформаційних комунікацій ІС МК.

Схема впливу кіберзагрози на ІС МК може бути представлена як багатовекторна багатоканальна модель взаємодії – на рисунку 4.



Рисунок 4 – Умовна ілюстративна схема інформаційних впливів (впровадження кіберзагроз) по основним і вторинним каналам у багатомодульному середовищі ІС МК

Дана схема (рис. 4) ілюструє комплексний фактор реалізації та напрямки ризиків і інформаційних втручань в каналах і інформаційно-комунікаційних трактах реалізації передавання даних в МК системах. Також вона дозволяє надати орієнтовні оцінки ризиків і шляхи їх нейтралізації.

Об'єктивні показники моделі :

- Канальні загрози інформаційній безпеці, що характеризуються ймовірністю реалізації, пропорційною кількості комунікацій в системі і можуть бути візуально проілюстровані ;
- Вразливі точки (точки реалізації загроз інформаційної системи або системи запобігання загрозам (системи інформаційної безпеки враховуються);
- Враховується ризики – чинники, що відображає можливі наслідки від реалізації кіберзагроз і вплив їх на інформаційну безпеку МК. Зокрема фактори: втрати/ модифікації/ несанкціоноване зчитування інформації та ризики, що відображають вірогідні втрати - прямі та непрямі.

Як зазначено авторами у [1, 2], для нейтралізації і вчасного попередження кіберзагроз використовуються прогресивні практики:

– проведення аналізу процесів функціонування МК;

– нейтралізація кіберзагроз і шкідливих впливів;
 – використання комплексних підходів до інформаційного захисту в МК системі;
 – ізоляція області роботи МК і окремих алгоритмічних модулів в складі мікропрограми МК (прошивки);

– підходи моніторингу і використання криптостійких та надійних алгоритмів;
 – використання антивірусних платформ і мережевих систем аналізу трафіку.

Ефективність цих методів та підходів захисту ІС МК і досить часто й затрати на їх реалізацію не у повній мірі дозволяють отримати необхідний рівень безпеки інформаційної системи МК.

Співвідношення вартість/технічний функціональний рівень захисту систем і заходів захисту інформаційних систем МК не завжди відповідають необхідному і достатньому рівню, особливо враховуючи сучасні загрози «0»-го дня і рівень сучасного шпигунського і хакерського програмного забезпечення і методів запису /зчитування інформації для МК і суміжних із ними систем. А також недостатність і ґрунтовність оцінки впливу загроз за рахунок відсутності часто моделей і методик оцінювання інформаційних впливів на ІС МК.

Враховуючи складність вектору динамічність процесу впливу кіберзагроз в ІС МК, варіації їх рівня у часі t_i для складної і комплексної ІС МК системи, математична модель (3) – (4) можна представити у вигляді динамічної моделі оцінки загроз у різні моменти часу:

$$i_k(x, y, t) = \sum_{k=1}^l g_k \cdot p_k \cdot q_k(x) \cdot f_k(x, y, t_i, \frac{dj_i}{dt}); \quad (12)$$

$$I(X, Y, t) \approx \sum_{k=1}^l i_k(x, y, t) = \sum_{k=1}^l g_k \cdot p_k \cdot q_k(x) \cdot f_k(x, y, t_i, \frac{dj_i}{dt}) \cdot \mu_{ex}(x, y, t_i, \frac{dj_i}{dt}) \cdot f_d(X, t_i, \frac{dj_i}{dt}) \cdot f_d(Y, t_i, \frac{dj_i}{dt}).$$

де, $f_k(x, y, t_i, \frac{dj_i}{dt})$ – динамічна функція появи загроз і втручань, яка характеризує їх інтенсивність та динаміку прискорень $\frac{dj_i}{dt}$ у часі t_i ; j – показник усередненої швидкості впливів кіберзагроз.

Дана модель (12) враховує динамічний характер впливу кіберзагрози та інформаційні втручання по різним інформаційним каналам втручань та розвиток їх у часі, що забезпечує розгляд по значно ширшим і вищим показникам ефективності при аналізі загроз і вчасного реагування на них і як наслідок підвищення ймовірності і швидкості їх виявлення і забезпечення захисту критичних даних і процесів в архітектурі МК. Як результат дії вчасного і швидкого виявлення і ідентифікації загроз та впливів механізмами виявлення у комунікаційних трактах та інтерфейсах в МК можлива конкретна швидка дія по її нейтралізації – відсікання блокування цих каналів. Потім, на другій стадії передбачається запуск процесів відновлення гілок і даних алгоритмів мікропрограми МК або пере запуск окремих функцій чи всієї мікропрограми МК. При порівнянні із іншими моделями виявлення і захисту та іншими не прямими методами, дана модель (12) сумісно із моделями (5) та (8) може використовуватись для проведення швидкого динамічного аналізу і оцінки впливів, із подальшим прийняттям рішення про блокування інформаційного потоку із шкідливим фактором по i -му каналу в МК.

Запропонована модель оцінки впливу кіберзагроз та інформаційних впливів може із достатньою високою ефективністю використовуватись у практиці аналізу і захисту складових ІС МК (із різними архітектурами) в складі різних пристроїв як загального так і спеціального призначення, зокрема й пристроїв IoT. Саме різноманіття інформаційних загроз та потенційних шкідливих впливів в ІС МК може бути представлено у вигляді наступних логарифмічної залежності кількості загроз $N_{МК}$, що визначається кількістю всіх потенційно-можливих інформаційних загроз і впливів $m_{МК}$ та n -кількістю їх точок і каналів впровадження (і в т.ч. і потенційних вразливостей системи МК). Залежність, яка це описує може бути подана у вигляді:

$$I_{cyber} = \log N_{МК} = \log m_{МК}^n = n \log m_{МК} \quad (13)$$

В такому випадку кількість інформації, яка описує всі можливі потенційні ризики й самі кіберзагрози в МК із n -кількістю точок впровадження і повною кількістю загроз $m_{МК}$, та приблизною усередненою питомою ймовірністю появи кожної кіберзагрози (чи потенційного впливу) може бути описано як:

$$H_{cyberthreat} = -n \sum_i^{m_{МК}} p_{iМК} \log_2 p_{iМК} \quad (14)$$

Формула описує втрати ентропію можливих кіберзагроз в МК і може бути використана при побудові мапи кіберзагроз та моделі кіберзагроз в мікропроцесорі.

Орієнтовні втрати інформації при настанні кіберзагрози в МК можна оцінити по питомим ймовірностям появи кіберзагроз $P(y_i) \rightarrow p_{iМК}$ і ймовірностей самих подій $P(x_j|y_i) \rightarrow p_i$ основних ланок обчислювального процесу у внутрішній підпрограми МК (прошивці МК):

$$H_{MK}(X|Y) = -n \sum_{i=1}^{n_{mk}} \sum_{j=1}^{m_{mk}} \cdot P_{MK}(y_i) \times P_{MK}(x_j | y_i) \times \log_2 P_{MK}(x_j | y_i) \quad (15)$$

Модель оцінки інформаційних втручань у множині потенційних загроз точок обчислювального процесу ІС МК при захисті комунікацій в інформаційно-комунікаційних трактах ІС МК на базі комутації пакетів в різні часові інтервали T (із потенційним використанням шифрування) із використанням асинхронної передачі в різні інтервали часу :

$$F(T_{xi}Pr(t)) = f_i(t, IP_{r,i}(x), H_{cyberthreat}) \cdot N \rightarrow f_i(t, IP_{r,i}(x), H(X/Y)) \quad (16)$$

де, N – кількість всіх доступних машинних слів даних у біт/байт, враховуючи комбінацію їх формуванню по внутрішніми алгоритмам M ; T_{xi} – часовий проміжок зміни машинного слова при різному режимі кодування і перетворення (оброблення) при обробленні і передаванні в архітектурі ІС МК.

Даний підхід передбачає виконання синхронізації комутаторів сторони A із стороною B у ІС МК і синхронна комутація в часі із шифруванням даних в кожному новому вікні T_i іншим протоколом і з доступного пулу підтримуваних протоколів та забезпечення переключення кожен раз новим алгоритмом по циклу комутації.

На базі цієї моделі і підходу мінімізації (нейтралізації) і визначення кіберзагроз та шкідливих інформаційних втручань в ІС МК, можливий аналіз ризиків та кількісне оцінювання впливу кіберзагроз в ІС МК із врахуванням впливу різних негативних факторів, їх величини та динаміки у ІС МК. Різна їх інтенсивність та нестабільні і незавжди визначені умови кіберзагроз у МК, різна інтенсивність інформаційних втручань робить задачу їх аналізу важкою, а завдання їх нейтралізації і протидії – складним і важким на практиці. В подальшому планується розробити інноваційні модель і метод захисту інформаційних процесів у ІС МК від кіберзагроз, який буде базуватись на інноваційних підходах функціональних мікро- і нано- сервісах перевірки безпеки процесів і гілок мікропрограм, визначення (ідентифікації кіберзагроз) що працюють безпосередньо в складі основної мікропрограми (прошивки) МК у вигляді окремої функції/об'єкту наряду із основним функціоналом і основними функціями МК в складі мікропрограми. Також, даний підхід повинен передбачати перевірку зовнішніх підключень і порядку слідування команд керування та переривань у МК, для контролю безпеки і виявлення втручань по побічних каналах. Передбачається врахування взаємодії МК із іншими інформаційними елементами в складі апаратних засобів і пристроїв автоматизації. Даний підхід і положення методу планується адаптувати до центральної частини архітектури МК і до каналного рівня із захистом організації каналів інформаційної системи МК і суміжних підсистем та із організації моделі моніторингу ІС МК із різними інтенсивностями і декількома основними типами кіберзагроз у них.

Розроблена математична модель може стати основою для аналізу стабільності інформаційних процесів і бути використана при розробці зовнішніх засобів ІС МК, які послідовно підключаються до/або функціонують в складі основної архітектури ІС МК чи підсистем та засобів для прямого і непрямого аналізу та вимірювання шкідливих впливів і функціоналу мікро ПЗ (мікропрограм) мікро контролерів та кіберзагроз в їх коді.

Аналіз і нейтралізація сучасних кіберзагроз апаратного рівня [7-15] і шкідливого коду в мікропрограмах і трафіку в інтерфейсах МК і в складі обчислювального процесу повинна відбуватись в онлайн-режимі та в режимі реального часу (чи наближеному до реального часу). Використання комплексу технологій мережевого захисту основних мережевих протоколів і обчислювальних процесів, а також захисту трафіку передбачає умовно максимальну мінімізацію кіберзагроз та ризиків їх появи та дотримання критерію:

$$k \rightarrow \min R_t, \quad (17)$$

де R_t – узагальнена ймовірність появи інформаційних ризиків в системі МК ($R_t \in M_r$), де M_r – множина інформаційних ймовірностей загроз (мапа кіберзагроз), згідно (4) та (6).

Для побудови збалансованої системи інформаційної та кібербезпеки МК потрібно спочатку провести комплексний аналіз ризиків у сфері інформаційної безпеки біомедичної системи передачі даних. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику і заданого допустимого рівня інформаційного шкідливого впливу в ІС МК.

Висновки

В статті було розглянуто матеріали окремих досліджень, як власних так і досвіду закордонних вчених і спеціалістів, які ґрунтуються на роботах по аналізу ризиків мікроконтролерів, проведеної авторами раніше у [1]. В даній ж статті проведено розробку математичної моделі оцінки шкідливих впливів інформаційних втручань та кіберзагроз на основні аналізу домінуючих інформаційних ризиків і кіберзагроз у мікроконтролерах, які працюють в складі систем управління різноманітних як загальних так і спеціалізованих пристроїв. Приведене удосконалення математичної моделі саме для аналізу кіберзагроз у мікро

контролерах, із врахуванням різних факторів кіберзагроз та інформаційних впливів. Аналіз факторів приведено для мікроконтролерів, які працюють в складі систем управління різноманітних та спеціалізованих обчислювачів. Визначено основні показники моделі загроз та інформаційних впливів у МК, яка описує сумарний вплив інформаційних загроз і вектори кібератак у МК. В роботі також проведено оцінку і прогнози розвитку математичної моделі, проведено оцінку впливів базових типів кіберзагроз і факторів ризику для мікро контролерів. Це дає змогу оцінити основні усереднені сумарні впливи із боку кіберзагроз і вразливостей на стабільність функціонування МК і окремі місця в його архітектурі. Також модель може використовуватись при розробці підходів і методів стабільного і безпечного функціонування електронних систем на базі мікроконтролерів як загального, так і спеціального призначення.

Список літератури

- [1] В.І. Маліновський, Л.М. Куперштейн, Аналіз загроз безпеки мікроконтролерів, «Інформаційні технології та комп'ютерна інженерія», Вінниця, ВНТУ, №3(55), С. 21-32, 2022.
- [2] Маліновський В.І. Мінімізація факторів кіберзагроз і спеціалізовані підходи до інформаційного захисту мікропроцесорних систем індустріального Інтернету речей. Матеріали LI-ї Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії (ФІТКІ), Вінниця, Україна: ВНТУ, 2022. [Електронний ресурс]. Режим доступу URL: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000> . (Дата звернення 13.02.2024).
- [3] Cybersecurity Enablers in MSPM0 MCUs: Application Note / Texas instruments Incorporated, 19.p., 2023. [Електронний ресурс]. Режим доступу URL: https://www.ti.com/lit/an/slaae29/slaae29.pdf?ts=1708675272061&ref_url=https%253A%252F%252Fwww.google.de%252F . (Дата звернення 24.02.2024).
- [4] Шологон Ю. З. Вразливості апаратного забезпечення кіберфізичних систем. Репозитарій Національного університету «Львівська політехніка» (Lviv Polytechnic National University Institutional Repository), 12.с., 2023. [Електронний ресурс]. Режим доступу URL: <http://ena.lp.edu.ua> . (дата звернення 24.02.2024).
- [5] Ю.М. Щєбланін, Д.І. Рабчун, Математична модель порушника інформаційної безпеки. Кібербезпека: освіта, наука , техніка. №1(1), С.63-72, 2018, ISSN 2663-4023.
- [6] В. М. Савченко, О. В. Мнушка. Модель безпеки інформаційної системи на базі технологій IoT. Вісник Національного технічного університету "ХПІ". № 28(1353), 2019, ISSN 2079-0031.
- [7] Yuan Xiao, Yinqian Zhang, Radu Teodorescu. Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities. [Електронний ресурс]. Режим доступу URL: <https://arxiv.org/pdf/1912.00329.pdf>. (Дата звернення: 20.10.2023р.).
- [8] Meltdown and Spectre: Which systems are affected by Meltdown. [Електронний ресурс]. Режим доступу URL: <https://meltdownattack.com/#faq-systems-meltdown>. (Дата звернення: 20.10.2023р.).
- [9] Meltdown and Spectre: Which systems are affected by Meltdown. [Електронний ресурс]. Режим доступу URL: <https://meltdownattack.com/#faq-systems-meltdown>. (Дата звернення: 20.10.2023р.).
- [10] Speculative Processor Vulnerability. ARM Developer Forum. Specifications Updated, March 8, 2022. [Електронний ресурс]. Режим доступу URL: <https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor%20Vulnerability>. (Дата звернення: 20.10.2023р.).
- [11] Cache Speculation Side-channels white paper. ARM Developer Forum. Specifications Updated March 8, 2022. [Електронний ресурс]. Режим доступу URL: <https://developer.arm.com/documentation/102816/0205/>. (Дата звернення: 20.10.2023р.).
- [12] Kernel Side-Channel Attack using Speculative Store Bypass – CVE-2018-3639. [Електронний ресурс]. Режим доступу URL: <https://access.redhat.com/security/vulnerabilities/ssbd> . (Дата звернення: 20.10.2023р.).
- [13] Kakareka, Almantas, Y Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc., p. 393, ISBN 978-0-12-374354-1.
- [14] Serdar Yegulalp Rowhammer hardware bug threatens to smash notebook security / by Serdar Yegulalp// InfoWorld, March 9, 2015. [Електронний ресурс]. Режим доступу URL: <https://www.infoworld.com/article/2894497/rowhammer-hardware-bug-threatens-to-smash-notebook-security.html>. (Дата звернення: 20.10.2023р.).
- [15] Kuljit Vains et al. Patent US № 20140059287 A1: Row hammer refresh command. [Електронний ресурс]. Режим доступу URL: <https://patents.google.com/patent/US20140059287>. (Дата звернення: 20.10.2023р.).
- [16] Introduction to STM32 microcontrollers security. Application note. ST Microelectronics, 58 p., 2023. [Електронний ресурс]. Режим доступу URL:

https://www.st.com/resource/en/application_note/an5156-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf. (Дата звернення: 22.02.2024р.).

- [17] Automatic Microprocessor Performance Bug Detection / E. C. Barboza, S. Jacob, M. Ketkar, M. Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Електронний ресурс]. Режим доступу URL: <https://arxiv.org/pdf/2011.08781.pdf>. (Дата звернення: 22.02.2024р.).
- [18] Automatic Microprocessor Performance Bug Detection / Barboza, E. C., Jacob, S., Ketkar, M., Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Електронний ресурс]. Режим доступу URL: <https://doi.org/10.1109/hpca51647.2021.00053/>. (Дата звернення: 22.02.2024р.).

Стаття надійшла: 04.04.2024.

References

- [1] V.I. Malinov's'kyu, L.M. Kupershteyn, Analiz zahroz bezpeky mikrokontroleriv, «Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya», Vinnytsya, VNTU, №3(55), S. 21-32, 2022.
- [2] Malinov's'kyu V.I. Minimizatsiya faktoriv kiberzahroz i spetsializovani pidkhody do informatsiynoho zakhystu mikroprotsesornykh system industrial'noho Internetu rechey. Materialy LI-yi Naukovo-tekhnichnoyi konferentsiyi fakul'tetu informatsiynykh tekhnolohiy ta komp'yuternoyi inzheneriyi (FITKI), Vinnytsya, Ukrayina: VNTU, 2022. [Elektronnyy resurs]. Rezhym dostupu URL: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15000>.
- [3] Cybersecurity Enablers in MSPM0 MCUs: Application Note / Texas instruments Incorporated, 19.p., 2023. [Elektronnyy resurs]. Rezhym dostupu URL: https://www.ti.com/lit/an/slaae29/slaae29.pdf?ts=1708675272061&ref_url=https%253A%252F%252Fwww.google.de%252F. (Data zvernennya 24.02.2024).
- [4] Sholohon YU. Z. Vrazlyvosti aparatnoho zabezpechennya kiberfizychnykh system. Repozytariy Natsional'noho universytetu «L'viv's'ka politehnika» (Lviv Polytechnic National University Institutional Repository), 12.s., 2023. [Elektronnyy resurs]. Rezhym dostupu URL: <http://ena.lp.edu.ua>. (data zvernennya 24.02.2024).
- [5] YU.M. Shcheblanin, D.I. Rabchun, Matematychna model' porushnyka informatsiynoyi bezpeky. Kiberbez-peka: osvita, nauka , tekhnika. №1(1), S.63-72, 2018, ISSN 2663-4023.
- [6] V. M. Savchenko, O. V. Mnushka. Model' bezpeky informatsiynoyi systemy na bazi tekhnolohiy IoT. Visnyk Natsional'noho tekhnichnoho universytetu "KHPI". № 28(1353), 2019, ISSN 2079-0031.
- [7] Yuan Xiao, Yinqian Zhang, Radu Teodorescu. Speechminer: a Framework for investigating and measuring speculative execution vulnerabilities. [Elektronnyy resurs]. Rezhym dostupu URL: <https://arxiv.org/pdf/1912.00329.pdf>. (Data zvernennya: 20.10.2023r.).
- [8] Meltdown and Spectre: Which systems are affected by Meltdown. [Elektronnyy resurs]. Rezhym dostupu URL: <https://meltdownattack.com/#faq-systems-meltdown>. (Data zvernennya: 20.10.2023r.).
- [9] Meltdown and Spectre: Which systems are affected by Meltdown. [Elektronnyy resurs]. Rezhym dostupu URL: <https://meltdownattack.com/#faq-systems-meltdown>. (Data zvernennya: 20.10.2023r.).
- [10] Speculative Processor Vulnerability. ARM Developer Forum. Specifications Updated, March 8, 2022. [Elektronnyy resurs]. Rezhym dostupu URL: <https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor%20Vulnerability>. (Data zvernennya: 20.10.2023r.).
- [11] Cache Speculation Side-channels white paper. ARM Developer Forum. Specifications Updated March 8, 2022. [Elektronnyy resurs]. Rezhym dostupu URL: <https://developer.arm.com/documentation/102816/0205/>. (Data zvernennya: 20.10.2023r.).
- [12] Kernel Side-Channel Attack using Speculative Store Bypass – CVE-2018-3639. [Elektronnyy re-surs]. Rezhym dostupu URL: <https://access.redhat.com/security/vulnerabilities/ssbd>. (Data zvernennya: 20.10.2023r.).
- [13] Kakareka, Almantas, U Vacca, John. Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc., p. 393, ISBN 978-0-12-374354-1.
- [14] Serdar Yegulalp Rowhammer hardware bug threatens to smash notebook security / by Serdar Yegulalp// InfoWorld, March 9, 2015. [Elektronnyy resurs]. Rezhym dostupu URL: <https://www.infoworld.com/article/2894497/rowhammer-hardware-bug-threatens-to-smash-notebook-security.html>. (Data zvernennya: 20.10.2023r.).
- [15] Kuljit Bains et al. Patent US № 20140059287 A1: Row hammer refresh command. [Elektronnyy re-surs]. Rezhym dostupu URL: <https://patents.google.com/patent/US20140059287>. (Data zvernennya: 20.10.2023r.).

- [16] Introduction to STM32 microcontrollers security. Application note. ST Microelectronics, 58 p., 2023. [Elektronnyy resurs]. Rezhym dostupu URL: https://www.st.com/resource/en/application_note/an5156-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf. (Data zvernennya: 22.02.2024r.).
- [17] Automatic Microprocessor Performance Bug Detection / E. C. Barboza, S. Jacob, M. Ketkar, M. Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Elektronnyy resurs]. Rezhym dostupu URL: <https://arxiv.org/pdf/2011.08781.pdf>. (Data zvernennya: 22.02.2024r.).
- [18] Automatic Microprocessor Performance Bug Detection / Barboza, E. C., Jacob, S., Ketkar, M., Kishinevsky, M., Gratz, P., & Hu, J. IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE Publications, 2021. [Elektronnyy resurs]. Rezhym dostupu URL: <https://doi.org/10.1109/hpca51647.2021.00053/>. (Data zvernennya: 22.02.2024r.).

Відомості про авторів

Малиновський Вадим Ігорович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Vadim Malinovskyi – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia

Куперштейн Леонід Михайлович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Leonid Kupershtein – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia

Лукічов Віталій Володимирович – к.т.н., доц. каф. захисту інформації, Вінницький національний технічний університет, м. Вінниця

Vitalii Lukichov – PhD (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia

V. Malinovskyi, L. Kupershtein, V. Lukichov

MATHEMATICAL MODEL FOR ASSESSING CYBER THREATS AND INFORMATION IMPACTS IN MICROCONTROLLERS

Vinnytsia national technical university, Vinnytsia

УДК 004.7

Л.А. Савицька¹, Т.І. Коробейнікова², О.І. Костюк¹,
І. С. Колесник¹, О. В. Дудник¹

ЗАСОБИ ЗАХИСТУ INTERNET OF THINGS В КОРПОРАТИВНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

¹Вінницький національний технічний університет, Вінниця²Національний університет «Львівська політехніка»

Анотація. Дана робота стосується аналізу та удосконалення засобів захисту для Internet of Things (IoT) у корпоративних комп'ютерних мережах. Internet of Things охоплює широкий спектр даних, включаючи особисті відомості, що робить питання безпеки під час їх передачі вельми актуальним. Основна мета дослідження полягає в розробці вдосконаленого технологічного дизайну системи IoT для забезпечення високого рівня безпеки та конфіденційності інформації. Сучасний світ Інтернету речей вимагає аналізу та покращення захисту IoT в корпоративних комп'ютерних мережах. В процесі аналізу використано загальнодоступні джерела інформації та наукові підходи, включно із сучасними науково-практичними публікаціями, аналітичними звітами та ресурсами від провідних компаній, таких як Cisco, що спеціалізуються на мережевому обладнанні та налаштуванні корпоративних мереж. Такий підхід дозволяє враховувати найсучасніші тенденції та технологічні рішення в галузі безпеки IoT. Однією з ключових проблем, на яку звертається увага, розробці розширеного та вдосконаленого технологічного дизайну системи IoT. Враховуючи постійний розвиток технологій, необхідно забезпечити високий рівень адаптивності та гнучкості захисних засобів, щоб вони ефективно працювали в різних умовах та обставинах. Додатковий акцент робиться на вивченні впливу розширеного та вдосконаленого технологічного дизайну системи IoT. Важливо забезпечити синергію між новими технологічними рішеннями та вже існуючими структурами мережі, щоб досягти максимального ефекту в удосконаленні безпеки та ефективності. Отже, наукова робота зосереджена на комплексному аналізі та впровадженні новітніх захисних засобів для IoT в корпоративних мережах з урахуванням сучасних тенденцій та вимог до безпеки даних.

Ключові слова: Internet Of Things, інформаційна безпека, рівні стеку, безпековий технологічний дизайн системи IoT, модель безпечного дизайну системи Internet Of Things.

Abstract. This work pertains to the analysis and enhancement of security measures for the Internet of Things (IoT) in corporate computer networks. The Internet of Things encompasses a wide range of data, including personal information, making the issue of security during their transmission highly relevant. The primary goal of the research is the development of an advanced technological design for the IoT system to ensure a high level of security and confidentiality of information. The modern world of the Internet of Things demands an analysis and improvement of IoT security in corporate computer networks. In the process of analysis, publicly available information sources and scientific approaches were utilized, including contemporary scientific publications, analytical reports, and resources from leading companies, such as Cisco, specializing in network equipment and configuration of corporate networks. This approach allows for the consideration of the latest trends and technological solutions in the field of IoT security. One of the key issues addressed is the development of an extended and improved technological design for the IoT system. Considering the constant evolution of technologies, it is essential to ensure a high level of adaptability and flexibility of security measures to effectively operate in various conditions and circumstances. An additional emphasis is placed on studying the impact of an extended and improved technological design of the IoT system. It is crucial to establish synergy between new technological solutions and existing network structures to achieve maximum effectiveness in enhancing security and efficiency. Therefore, the scientific work focuses on a comprehensive analysis and implementation of cutting-edge security measures for IoT in corporate networks, taking into account contemporary trends and data security requirements.

Key words: Internet Of Things, information security, stack levels, secure technological design of the IoT system, model of secure design of the Internet Of Things system.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-83-93>.

Вступ та актуальність

Започаткування розвитку Internet of Things (IoT) та його використання відбулося у 2000-х роках. У цьому напрямку активно працюють численні відомі та інші компанії, такі як IBM, Intel, Google, Cisco, Microsoft, Amazon, і Siemens. [1-7]. Уже у період між 2018 і 2019 роками кількість пристроїв, які були підключені до мережі, вагомо перевищила населення Землі. Згідно з передбаченнями, до 2025 року кількість таких підключених пристроїв мала сягнути від 50 до 70 мільярдів одиниць. Це експоненційне зростання створює значні ризики для безпеки інформації, яка обробляється, передається та зберігається цими пристроями. Для запобігання цим ризикам необхідно дотримуватись вимог, включаючи ті, які встановлені Регламентом Європейського Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року щодо захисту особистих даних та вільного обігу таких даних, що відомий також як GDPR. [4, 8, 9]. Тому тема дослідження є актуальною.

Отже, потрібно провести аналіз та покращення захисту IoT в корпоративних комп'ютерних мережах. Основний акцент зроблено на розробці розширеного та вдосконаленого технологічного дизайну системи IoT.

Мета

Метою даного дослідження є підвищення безпеки та захисту пристроїв Internet Of Things всередині

корпоративної комп'ютерної мережі від несанкціонованого доступу. Це досягається за допомогою вдосконаленого технологічного дизайну системи IoT.

Задачі

1. Спроекувати вдосконалений технологічний дизайн системи Internet Of Things;
2. Запропонувати розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things;
3. Розробити модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things;

Архітектура та ключові елементи системи IoT

Поняття Internet Of Things відображає глобальну систему взаємно підключених та зв'язаних пристроїв різного типу, що призначені для поліпшення процесу прийняття рішень різного характеру, заснованого на аналізі величезних обсягів даних, які накопичуються цими пристроями. Іншими словами, Internet Of Things – це мережа, в якій об'єкти і пристрої спілкуються між собою та надсилають дані для покращення різноманітних рішень.

Система Internet Of Things складається з багатьох компонентів і складових. До цього переліку входять пристрої виконання, сервіси і технології, які використовуються для оптимальної роботи цієї перспективної галузі. В цей перелік включаються різні типи сенсорів, пристроїв для збору даних, засоби передавання інформації, хмарні обчислення, аналітичні інструменти та багато інших компонентів. Усі вони спільно працюють, щоб забезпечити надійну і ефективну роботу Internet Of Things та підтримувати вирішення різних завдань та завдань у різних галузях та сферах життя [10, 11].

Перелічимо засоби, сервіси і технології:

- Сенсори (розумні датчики/виконавчі механізми): це вбудовані системи, які мають операційні системи реального часу та використовуються для збору даних. Вони також обладнані джерелами безперебійного живлення і використовують мікро-електромеханічні системи (MEMS).
- Вбудовані системи зв'язку з датчиками: ці системи забезпечують зв'язок між датчиками. Зона охоплення бездротових персональних мереж може варіюватися від нульової відстані до 100 метрів. Для обміну даними між датчиками використовуються низькошвидкісні малопотужні інформаційні канали, які не завжди базуються на протоколі IP.
- Локальні обчислювальні мережі (LAN): зазвичай це системи обміну даними на базі протоколу IP, такі як 802.11 Wi-Fi, що використовуються для швидкої бездротової радіозв'язку. Ці мережі можуть бути як піринговими (Peer-to-peer), так і зірковими.
- Агрегатори, маршрутизатори, шлюзи (gateways), пограничні пристрої (Edge Device): ці пристрої служать постачальниками вбудованих систем і включають в себе різні компоненти, такі як процесори, динамічна оперативна пам'ять і системи зберігання даних. Вони також можуть бути виробниками модулів, пасивних компонентів, тонких клієнтів і радіосистем, а також надавати послуги з міжплатформного програмного забезпечення.
- Глобальна обчислювальна мережа: в цю категорію входять оператори стільникового зв'язку, оператори супутникового зв'язку, і оператори малопотужних глобальних мереж (Low-Power Wide-Area Network, LPWAN). Для IoT зазвичай використовуються транспортні протоколи Інтернету, такі як MQTT, CoAP, і навіть HTTP;
- Хмарна інфраструктура: хмарні ресурси виступають в ролі постачальників різноманітних послуг і платформ для системи Internet Of Things. Вони також надають інфраструктуру для обробки поточкових і пакетних даних, баз даних і аналізу даних. Крім того, хмарні постачальники надають інструменти для аналізу та розробки програмного забезпечення, а також сервіси машинного навчання.
- Сервіси аналізу даних: величезні обсяги інформації передаються в хмару для проведення подальшого аналізу. Робота з великими даними і отримання конкретних результатів вимагають комплексної обробки даних та використання методів аналізу та машинного навчання.
- Забезпечення безпеки: під час інтеграції всіх компонентів архітектури в єдину систему постає питання забезпечення кібербезпеки. Безпека є критичним аспектом на всіх рівнях, від фізичних датчиків до центральних обчислювальних систем, включаючи системи зв'язку та протоколи передавання даних. На кожному рівні необхідно гарантувати конфіденційність, доступність та цілісність даних. У цьому ланцюжку не може бути слабких точок, оскільки екосистема Internet Of Things стає об'єктом атак з боку хакерів у всьому світі.

Ця архітектура Internet Of Things об'єднує різноманітні компоненти та послуги, щоб забезпечити збір, обробку, зберігання та аналіз даних. Вона включає в себе різні типи пристроїв, мереж і сервісів і

вимагає високого рівня безпеки для захисту інформації від потенційних загроз. На рисунку 1 наведено схематичне зображення архітектури Internet Of Things за версією компанії CISCO [4, 10].

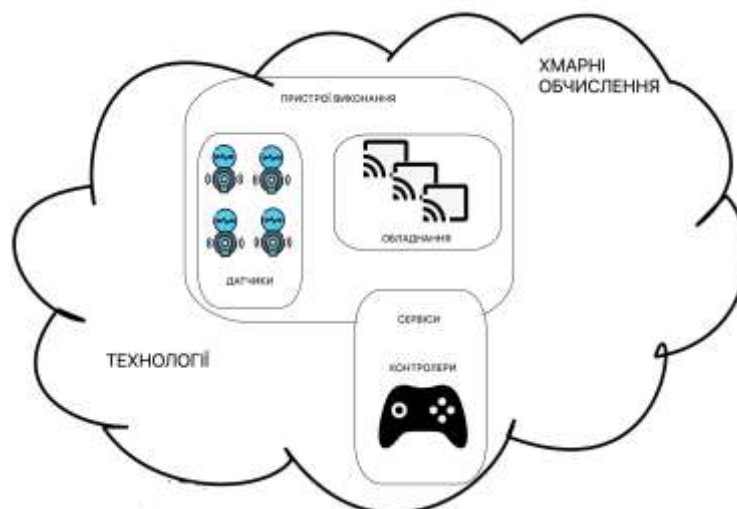


Рисунок 1 – Складові архітектури системи Internet Of Things

З різних поглядів компаній і спеціалізованих організацій архітектурна модель Internet Of Things може включати в себе різні рівні обслуговування та подання. Наприклад, Міжнародний союз електрозв'язку (МСЕ-Т) вивів 4-х рівневу модель архітектури IoT, тоді як Всесвітній форум IoT (IoT World Forum, IWF) розробив еталонну модель, яка складається з 7 рівнів [12,13,14]. Відмінність між цими моделями полягає в їхній конкретній реалізації. У загальних рисах вони нагадують архітектуру традиційних систем автоматизації управління технологічними процесами.

Вдосконалений технологічний дизайн системи Internet Of Things

У таблиці 1, наведеній нижче, представлена одна з прикладних 3-рівневих моделей архітектури системи Internet Of Things, яка розглядає питання безпеки на кожному рівні та можливі варіанти їх вирішення. Наслідком цього є більш глибоке розуміння аспектів безпеки в контексті Internet Of Things [15, 16, 17].

Таблиця 1 – Складові тривірневої моделі системи Internet Of Things

РІВЕНЬ ВИКОНАВЧИХ ПРИСТРОЇВ	Безпека IoT	RFID-пристрої, бездротові сенсорні пристрої, GPS-пристрої
	Безпека мережі IoT	
ТРАНСПОРТНИЙ РІВЕНЬ	Доступ до мережі IoT	WIFI-мережі, Ad hoc-мережі
	WAN	Мобільний Інтернет, Інтернет
	LAN	Безпека локальної мережі
ПРИКЛАДНИЙ РІВЕНЬ	IoT Applications	Інформаційна логістика, інтелектуальна мережева безпека, моніторинг середовища
	IoT Application support	Безпека середовища розробки, платформи хмарних обчислень, поміжні технології безпеки

Як вже було відзначено в даній роботі, остаточний вигляд структури Internet Of Things залежить від багатьох факторів, включаючи потреби та особливості конкретного проекту і реальні можливості для їх впровадження. Розподіл функцій системи на її рівнях також є важливим аспектом, який потребує чіткості та розуміння.

Для поліпшення розподілу функцій автором пропонується розширений дизайн системи IoT (порівняно із див. Таблиця 1) з додатковим рівнем інтерфейсів, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA). На рисунку 2 нижче наведено розширений дизайн системи IoT, що складається з 4 рівнів. Цей дизайн дозволяє краще розуміти та оптимізувати функціональний розподіл в контексті системи Internet Of Things.

3-LAYER MODEL	4-LAYER MODEL
Прикладний рівень	Службовий рівень
Транспортний рівень	Рівень корпоративної комп'ютерної мережі
Рівень виконавчих пристроїв	Рівень локальних інтерфейсів
	Рівень датчиків

Рисунок 2 – Запропонований розширений технологічний дизайн системи IoT

Кожен з вказаних компонентів на цьому ілюстрації виконує свою конкретну функцію. Рівень датчиків займається збором даних. Рівень локальних інтерфейсів відповідає за забезпечення взаємодії між різними учасниками системи, рівень корпоративної комп'ютерної мережі відповідає за передачу даних, і службовий рівень дозволяє створювати та управляти різними сервісами.

Ця ілюстрація демонструє, що кожен з компонентів в мережі має свою важливу функцію. Рівень датчиків відповідає за збір великої кількості різноманітних даних, рівень локальних інтерфейсів виконує роль посередника, який дозволяє різним частинам системи спілкуватися та обмінюватися інформацією. Рівень корпоративної комп'ютерної мережі відповідає за ефективну передачу цих даних між різними пристроями та підсистемами. Нарешті, службовий рівень включає в себе можливість створення, налагодження та керування різними сервісами та функціоналом мережі. Кожен із цих рівнів є важливою ланкою в цій складній системі, і їх спільна робота дозволяє Internet Of Things працювати ефективно та надійно.

Технологічний дизайн системи Internet Of Things

Відповідно до моделі сервіс-орієнтованої архітектури (Service-oriented architecture, SOA) технологічний дизайн системи Internet Of Things буде містити 4 чотири рівні, згідно досліджень (рис. 2). Відобразимо відкриту модель OSI, відомий протокольний стек TCP/IP, прототипну 3-рівневу модель та модель технологічного дизайну системи Інтернету речей за принципами SOA (рис. 3).

OSI	TCP/IP	3-LAYER Sec.IOT DESIGN	4-LAYER Sec.IOT DESIGN
7 Application	Application	Прикладний рівень	Службовий рівень
6 Presentation			
5 Session	Transport Network	Транспортний рівень	Рівень корпоративної комп'ютерної мережі
4 Transport			
3 Network			
2 Data Link	Network Access	Рівень виконавчих пристроїв	Рівень локальних інтерфейсів
1 Physical			
			Рівень датчиків

Рисунок 3 – Приведення технологічного дизайну системи Internet Of Things до відомих стандартів

Така архітектура забезпечує взаємодію між великою кількістю різних пристроїв. Кожен з цих рівнів має такі функції:

- Рівень датчиків взаємодіє з апаратними засобами та датчиками для визначення стану системи Інтернету речей та безпосередньо збирання даних (рівень 1);
- Рівень локальних інтерфейсів надає різні методи та засоби взаємодії системи Інтернету речей з безпечною мережею (LAN) (рівень 2);
- Рівень корпоративної комп'ютерної мережі надає повноцінну мережеву інфраструктуру, яка для стабільної підтримки з'єднань у корпоративній комп'ютерній мережі (рівень 3);
- Службовий рівень дає можливість керувати засобами та сервісами між користувачам та додатками (рівень 4).

За використання запропонованого технологічного дизайну, ця система розбивається на підсистеми, які взаємодіють між собою та можуть бути використані для підтримки функціонування новоствореної системи. Цей підхід гарантує безперебійну роботу, оскільки при відмові одного компонента інші продовжать функціонувати. У випадках, коли надійність та доступність є ключовими завданнями у проектуванні, ця модель виявляється найкращим вибором.

Цей підхід спрощує взаємодію з протоколами передавання даних та різними рівнями системи, оскільки сприяє покращенню взаємодії між об'єктами та спрощує процес керування. Модель технологічного дизайну системи Інтернету речей організована на основі принципів SOA, дає Інтернету речей можливість повністю реалізувати свій потенціал і показати всі свої переваги. Ця модель дозволяє створювати складні сервіси, де для виконання різних завдань можна виділити окремі об'єкти системи [19].

Розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things

У кожній системі є своя власна структура, або інакше кажучи, дизайн, що визначає, як взаємодіють всі її складові. Система Інтернету речей не є винятком. Після аналізу джерел було прийнято рішення зобразити взаємозв'язок компонентів системи IoT з аспектами безпеки. Цю залежність можна побачити на рисунку 4.

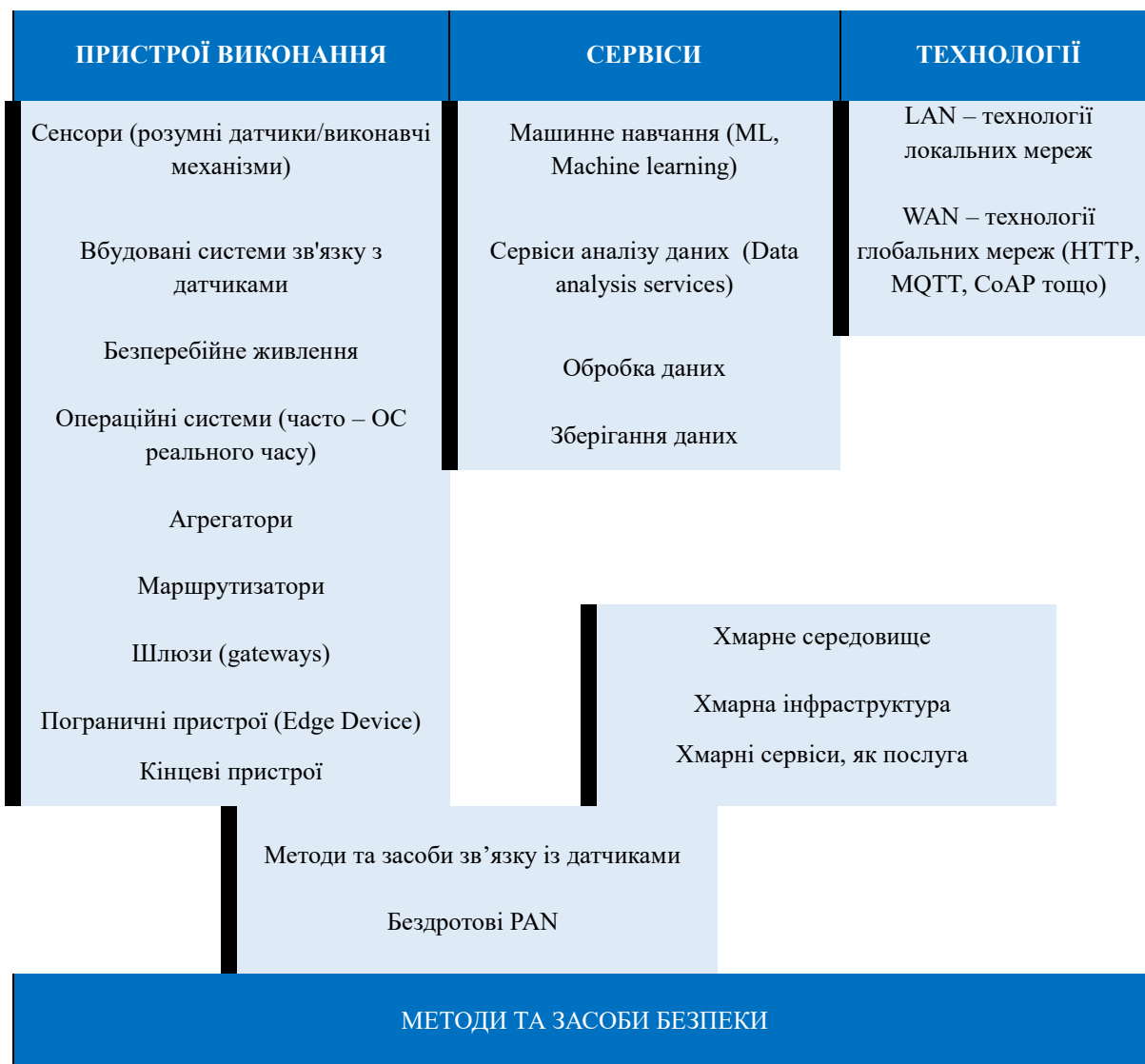


Рисунок 4 – Безпековий технологічний дизайн системи Internet Of Things

Нині цифрові технології проникають у всі сфери життя, запити до безперебійної роботи програмних чи апаратних продуктів стають все актуальнішими. Несанкціоноване втручання на різних рівнях таких

систем може завдати збитків. Тому під час розробки будь-якого програмного чи апаратного продукту, включно з цільовою системою Інтернету речей, забезпечення безпеки стає надзвичайно важливим [11].

На рисунку 5 зображено відповідність рівнів стеку системи IoT і проблем безпеки, притаманних цим рівням.

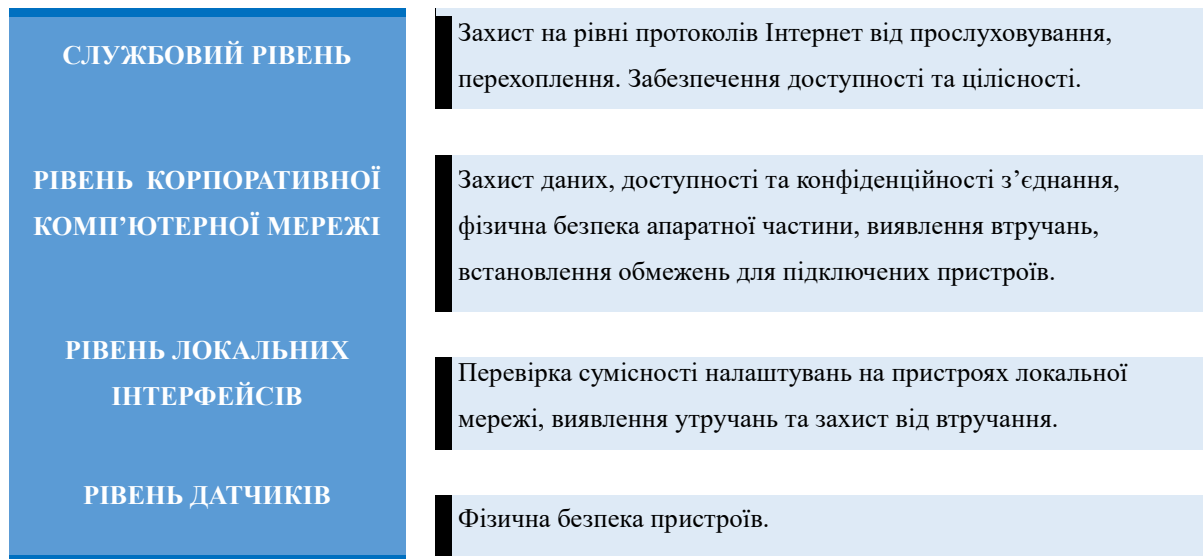


Рисунок 5 – Розподіл загроз безпеці по рівнях технологічного дизайну системи Internet Of Things

З урахуванням зростаючої мобільності, сучасна архітектура системи повинна бути високою у рівні адаптабельності для ефективної обробки різноманітних динамічних взаємодій на всіх рівнях її структури. Надання більш високого рівня абстракції, який може приховати деякі деталі реалізації, є безперечною перевагою стандартних архітектурних рішень і моделей.

Такий безпековий технологічний дизайн системи IoT є інтегрованою системою і гарантує надійну роботу своїх компонентів та забезпечує зв'язок між фізичними та віртуальними складовими.

Для створення цілісної системи обов'язково важливим є докладний підхід до проектування, з особливою увагою до процедур відновлення системи після виникнення неполадок. Враховуючи, що створення безпечного середовища має велике значення, важливо враховувати масштабність системи.

Модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things

Якщо враховувати використання відкритих стандартів, тоді запропонуємо вирішення питань безпеки на різних рівнях технологічного дизайну системи Internet Of Things. З метою підвищення загальної захищеності системи IoT, кожен рівень стеку використовує різні протоколи, послуги та механізми безпеки. Отже, кожен рівень прагне досягти важливих цілей, включаючи забезпечення безпеки інформації, фізичної безпеки та стійкого функціонування системи управління безпекою, як окремо, так і в цілому. Розподілимо рівні технологічного дизайну системи Internet Of Things відповідно їх функціональним елементам та розпишемо кожен згідно архітектури IoT та з погляду безпеки та аналізу літературних джерел у вигляді таблиці 2.

У таблиці 2 наведені складові та задачі для окремого рівня моделі безпечного дизайну системи Internet Of Things із відображенням атак та вимоги безпеки, які необхідні для кожного з них. Подана таблиця 2.1 ілюструє перелік методів для вирішення проблем безпеки під час безпечного дизайну системи Internet Of Things [16-18].

Для того, щоб продемонструвати вимоги до безпеки в дизайні Internet Of Things на прикладі, використаємо запропонований розширений технологічний дизайн системи IoT, яка складається з рівнів: датчиків, локальних інтерфейсів, корпоративної комп'ютерної мережі та службового. Кожен з них має забезпечити сприяння чіткому процесу управління безпекою корпоративної комп'ютерної мережі, це забезпеченню контролю доступу, автентифікації та цілісності даних, також їх конфіденційності і наявності інструментів для захисту системи IOT від вірусів та атак.

Тож створена модель безпечного дизайну системи Internet Of Things повинна мати можливість відстежувати кожен пристрій корпоративної комп'ютерної мережі, контролювати трафік та бути спроможною захистити або тимчасово обмежити використання пристрій/-оїв аби значно зменшити (в

ідеалі – унеможливити, пом'якшити) критичні наслідки для цілої екосистеми корпоративної комп'ютерної мережі, що містить IoT. Тепер коротко розглянемо запропонований розширений технологічний дизайн системи IoT.

Таблиця 2 – Модель безпечного дизайну системи Internet Of Things

SI	TCP/IP	ДИЗАЙН ІОТ	ОБ'ЄКТ ЗАХИСТУ (ПРОТОКОЛ, ТЕХНОЛОГІЯ, ТОЦО)	МЕТОД ЗАХИСТУ	ОПИС
7	Додатків	СЛУЖБОВИЙ РІВЕНЬ	DHCP, SSH, CoAP, AMQP, XMPP, masquerad	DHCP snooping, RSA, ACL, IPS, брандмауер, шифрування,	Хмарні послуги, сервіси аналізу даних, машинне навчання, зв'язок з пристроями (частково), безпека додатків
6					
5					
4	Транзит оргтний	РІВЕНЬ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	DDoS, DoS, IPv4, IPv6, MQTT та DDS, TLS / SSL, MITM, TCP, UDP	SYN protection, 6LowPAN,	Зв'язок з пристроями, провідні та безпроводні мережі, протоколи передавання даних (частково), корпоративні мережні пристрої (частково)
3	Інтернету				
2	Мережевого доступу	РІВЕНЬ ЛОКАЛЬНИХ ІНТЕРФЕЙСІВ	MAC, MIM, DNS, ARP, Адресні spoofing, STP, RFID, WSN, PKI, VLAN	PortSecurity, DAI, BPDU Guard, IPSG, PortFast	Мережні пристрої (частково), протоколи передавання даних (частково), міжплатформне ПЗ
1		РІВЕНЬ ДАТЧИКІВ	selfish загроза, фізична безпека, порушення цілісності даних, зловмисне ПЗ	IPsec, IEEE 802.11 AH	Датчики, безперебійне живлення, ОС реального часу, безпека, GPS, Bluetooth

Безпека на рівні датчиків

Даний рівень розширений технологічний дизайн системи IoT можна охарактеризувати як сполучення трьох ланок, які забезпечують дані від: пристроїв збору інформації; місця розташування (функціонування) пристрою; безпосередньо від людей.

Для повноцінної реалізації функцій безпеки необхідно передбачене виробником виконання елементів безпеки в пристроях, тобто можливість аутентифікації, шифрування даних та обмеження в локальному збереженні зібраної інформації. Зі сторони корпоративної комп'ютерної мережі та персоналу, що їх конфігурує – врахування особливостей роботи підприємства.

Складними питаннями безпеки на рівні датчиків технологічного дизайну системи IoT є:

1. Фізична безпека та захист пристроїв збору даних. Найкраще – це коли передбачено ускладнений або неможливий доступ до пристрою.
2. Недостатня модернізація апаратної частини та програмної складової, що обслуговує пристрій (наприклад, версії ОС або прошивка). Часто в пристроях (іноді адміністратори роблять це навмисно) немає передбаченої можливості для їх оновлення чи переналаштування. Нові вразливості можуть виникати постійно, тож якщо пристрій не буде мати доступу для оновлення своїх налаштувань, це може послабити безпеку системи.

Безпека на рівні локальних інтерфейсів

Цей рівень є посередником між IoT системою в місцях розташування датчиків і мережевими службами, додатками. Він надає підтвердження того що взаємодія між додатками і системою є легітимною. Потенційними проблемами на цьому рівні є:

1. Необхідність однотипних (часто – подібних) налаштувань конфігурації на всіх пристроях для досягнення сумісності з точки зору конфігурації.
2. Забезпечення безпеки зібраних даних на цьому рівні технологічного дизайну системи IoT.

3. Створення ефективних програмно-апаратних рішень безпеки задля оптимізації процесу взаємодії з легальними користувачами і зловмисниками.

Рекомендаціями для вирішення проблем безпеки даного рівня є дотримання конфіденційності, цілісності та доступності, регулярне оновлення ПЗ, аутентифікація та авторизація користувачів та адміністратора.

Безпека на рівні корпоративної комп'ютерної мережі

Мережевий рівень є надважливою частиною розширеного технологічного дизайну системи IoT, оскільки є каналом передавання даних між іншими рівнями. Зважаючи на те, що екосистема IoT складається з великої кількості побічних гібридних систем, фактор проблеми масштабованості корпоративної комп'ютерної мережі, її складності та безпеки передавання даних є значним.

Серед проблем, які виникають тут можуть бути:

1. Забезпечення класичних вимог інформаційної безпеки – конфіденційності, цілісності та доступності.
2. Фізична безпека (якщо пристрої які забезпечують передавання даних можуть бути у вільному доступі).
3. Надмірна кількість підключень до корпоративної комп'ютерної мережі, що створює додаткові складнощі в обслуговуванні, надмірні витрати мережевих ресурсів (як програмного, так і апаратного гатунку) та збільшення вразливостей внаслідок ймовірного зловмисного впливу.
4. Можливість запобігання зловмисного роду атак, на зразок «Man-In-The-Middle» для перехоплення інформації, що передається між об'єктами корпоративної комп'ютерної мережі.

Основними викликами до безпеки на рівні корпоративної комп'ютерної мережі в розумінні розширеного технологічного дизайну системи IoT є мінімізація можливості впливу зловмисників на екосистему та збільшення ефективності її роботи та, водночас, покращення якості обслуговування (Qos).

Безпека на службовому рівні

Службовий рівень розширеного технологічного дизайну системи IoT забезпечує ефективну взаємодію використання апаратних та програмних ресурсів і можливість повторного використання цих ресурсів. На службовому рівні відбувається аналіз отриманих даних від рівня датчиків, тож тут присутні служби обробки подій, служби інтеграції і аналітики тощо, які дозволяють обмін інформацією між сервісами та додатками, а також забезпечують виконання необхідних дій.

Виклики, які притаманні службовому рівню:

1. Забезпечення конфіденційності, цілісності та доступності.
2. Можливість недоброчесних маніпуляцій даними від служб та додатків службового рівня.
3. Створення захисту від різноманітних атак (на кшталт DoS та DDoS-атак).
4. Забезпечення аналізу трафіку для адміністраторів і обмеження для неавторизованих користувачів задля недопущення жодних маніпуляцій з даними.

Класичним підходом до вирішення і убезпечення від проблем на службовому рівні є відповідність стандартам та протоколам під час проектування та впровадженні дизайну системи IoT.

Висновки

У даній роботі досягнуто підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп'ютерної мережі від несанкціонованого доступу за допомогою вдосконаленого технологічного дизайну системи IoT. В результаті аналітичного дослідження вдалося проаналізувати архітектуру і ключові компоненти екосистеми Internet Of Things та особливості роботи технології IoT з точки зору взаємодії, обробки даних та розподілу інформації в системах IoT і виконати ґрунтовний аналіз загроз інформаційній безпеці IoT. Внаслідок вдалося спроектувати 4-рівневий технологічний дизайн системи Internet Of Things із урахуванням запропонованого рівня інтерфейсів, що надає подібність до принципів побудови сервіс-орієнтованої архітектури.

Запропоновано розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things та вмонтовано цю ідею в модель безпечної дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things. В результаті спроектовано модель корпоративної комп'ютерної мережі в програмному середовищі Packet Tracer з захистом у відповідності до запропонованого технологічного дизайну системи IoT.

Зокрема, результат полягає у такому:

1. Вдосконалена відома трирівнева модель системи Internet Of Things за рахунок приведення її до архітектури IoT від CISCO, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA);
2. Запропоновано розширений технологічний дизайн системи IoT, що містить такі рівні:

- датчиків, локальних інтерфейсів, корпоративної комп'ютерної мережі та службовий і це дає можливість поглибити безпекові аспекти в контексті IoT;
3. Розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп'ютерної мережі за рахунок приведення технологічного дизайну системи Internet Of Things до відомих стандартів;
 4. Розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп'ютерної мережі за рахунок розподілу загроз безпеці по рівням технологічного дизайну системи IoT;
 5. Запропоновано вдосконалену модель безпечного дизайну системи Internet Of Things.

Список літератури

- [1] Сайт компанії IBM [Електронний ресурс] – Режим доступу: https://www.ibm.com/cloud/internet-of-things?mhsrc=ibmsearch_a&mhq=iot
- [2] Сайт компанії Intel [Електронний ресурс] – Режим доступу: <https://www.intel.com/content/www/us/en/internet-of-things/overview.html>
- [3] Сайт компанії Google [Електронний ресурс] – Режим доступу: <https://cloud.google.com/iot-core>
- [4] Сайт компанії Cisco [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html>
- [5] Сайт компанії Microsoft [Електронний ресурс] – Режим доступу: <https://azure.microsoft.com/en-us/services/iot-central/>
- [6] Сайт компанії Amazon [Електронний ресурс] – Режим доступу: <https://aws.amazon.com/iot-core/>
- [7] Сайт компанії Siemens [Електронний ресурс] – Режим доступу: <https://new.siemens.com/global/en/products/automation/topic-areas/industrial-iot.html>
- [8] Цифрова трансформація бізнесу / Інтернет речей [Електронний ресурс] – Режим доступу: <https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iotXXX>
- [9] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року, (GDPR) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
- [10] Introduction to IoT. [Електронний ресурс] – Режим доступу: <https://lms.netacad.com/course/view.php?id=744659>.
- [11] Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.
- [12] Комп'ютерні мережі: навчальний посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки (НУЛП), 2022. – 228 с.
- [13] Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки (НУЛП), 2021. 232 с.
- [14] Інтернет речей: мережева архітектура та архітектура безпеки [Електронний ресурс] – Режим доступу до ресурсу: <https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html>.
- [15] Литвиненко Д. С. Модель безпеки інформаційної системи на базі технологій IoT : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 123 Комп'ютерна інженерія / Д. С. Литвиненко ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2021. – 81 с.
- [16] Коробейнікова Т.І. Організація архітектури системи IoT в протокольному стекові. / Т. І. Коробейнікова, Т. В. Іськович // International scientific journal «Grail of Science» – 2023. – № 27 (May, 12, 2023). – С. 341–346. ISSN: 2710–3056. ISBN 979-8-88955-792-0. <https://doi.org/10.36074/grail-of-science.12.05.2023.053>
- [17] Коробейнікова Т.І. Безпековий технологічний стек IoT / Коробейнікова Т.І., Іськович Т. В. // International periodical scientific journal «SWorldJournal» – 2023. – № 19 (part 1) (May, 2023). – С. 24–32. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-19-01-020. www.sworldjournal.com/index.php/swj/article/view/swj19-01-020
- [18] Jing, Qi & Vasilakos, Athanasios & Wan, Jiafu & Lu, Jingwei & Qiu, Dechao. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*. 20. 2481-2501. 10.1007/s11276-014-0761-7.
- [19] Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
- [20] Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп'ютерна інженерія 2021: - №1 (50). - С. 31–35

[21] Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // Інформаційні технології та комп'ютерна інженерія. – 2023. – № 1. – С. 66-74.

Стаття надійшла: 04.03.2024.

References

- [1] IBM website [Online]. Available: https://www.ibm.com/cloud/internet-of-things?mhsrc=ibmsearch_a&mhq=iot
- [2] Website Intel [Online]. Available: <https://www.intel.com/content/www/us/en/internet-of-things/overview.html>
- [3] Website Google [Online]. Available: <https://cloud.google.com/iot-core>
- [4] Website Cisco [Online]. Available: <https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html>
- [5] Website Microsoft [Online]. Available: <https://azure.microsoft.com/en-us/services/iot-central/>
- [6] Website Amazon [Online]. Available: <https://aws.amazon.com/iot-core/>
- [7] Website Siemens [Online]. Available: <https://new.siemens.com/global/en/products/automation/topic-areas/industrial-iot.html>
- [8] Tsyfrova transformatsiya biznesu / Internet rechey [Online]. Available: <https://www.it.ua/knowledge-base/technology-innovation/internet-veshej-internet-of-things-iotKHKHKKH>
- [9] Rehlament Yevropeys'koho Parlamentu i Rady (YES) 2016/679 vid 27 kvitnya 2016 roku, (GDPR) [Online]. Available: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
- [10] Introduction to IoT. [Online]. Available: <https://lms.netacad.com/course/view.php?id=744659>.
- [11] Tekhnolohii internetu rechey. Navchal'nyy posibnyk [Elektronnyy resurs]: navch. posib. dlya stud. spetsial'nosti 126 «Іnformatsiyni systemy ta tekhnolohii», spetsializatsiya «Іnformatsiyne zabezpechennya robototekhnichnykh system» / B. YU. Zhurakovs'kyy, I.O. Zeniv; KPI im. Ihorya Sikors'koho. – Elektronni tekstovi dani (1 fayl: 12,5Mbayt). – Kyiv: KPIim. Ihorya Sikors'koho, 2021. – 271 s.
- [12] Komp'yuterni merezhi: navchal'nyy posibnyk / T. I. Korobeŭnikova, S. M. Zakharchenko. – L'viv: Vydavnytstvo L'vivs'koï politekhniki (NULP), 2022. – 228 s.
- [13] Tekhnolohii zakhystu lokal'nykh merezh na osnovi obladnannya CISCO : navch. posibnyk / T. I. Korobeŭnikova, S. M. Zakharchenko. – L'viv: Vydavnytstvo L'vivs'koï politekhniki (NULP), 2021. 232 s.
- [14] Internet rechey: merezheva arkhitektura ta arkhitektura bezpeky [Online]. Available: <https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html>.
- [15] Lytvynenko D. S. Model' bezpeky informatsiynoyi systemy na bazi tekhnolohiy IoT : poyasnyval'na zapyska do kvalifikatsiynoyi roboty zdobuvacha vyshchoyi osvity na druhomu (mahisters'komu) rivni, spetsial'nist' 123 Komp'yuterna inzheneriya / D. S. Lytvynenko ; M-vo osvity i nauky Ukrainy, Kharkiv. nats. un-t radioelektroniky. – Kharkiv, 2021. – 81 s.
- [16] Korobeŭnikova T.I. Orhanizatsiya arkhitektury systemy IoT v protokol'nomu stekovi. / T. I. Korobeŭnikova, T. V. Is'kovych // International scientific journal «Grail of Science» – 2023. – № 27 (May, 12, 2023). – S. 341–346. ISSN: 2710–3056. ISBN 979-8-88955-792-0. <https://doi.org/10.36074/grail-of-science.12.05.2023.053>
- [17] Korobeŭnikova T.I. Bezpekovyy tekhnolohichnyy stek IoT / Korobeŭnikova T.I., Is'kovych T. V. // International periodical scientific journal «SWorldJournal» – 2023. – № 19 (part 1) (May, 2023). – S. 24–32. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-19-01-020. www.sworldjournal.com/index.php/swj/article/view/swj19-01-020
- [18] Jing, Qi & Vasilakos, Athanasios & Wan, Jiafu & Lu, Jingwei & Qiu, Dechao. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*. 20. 2481-2501. 10.1007/s11276-014-0761-7.
- [19] Pobudova zakhyshchenykh merezh na bazi obladnannya kompaniyi Cisco. // Zakharchenko S.M., Troyanovs'ka T. I., Boyko O.V. Navchal'nyy posibnyk. Vynnytsya : VNTU, 2017. – 133 s.
- [20] Savyts'ka L.A., Korobeŭnikova T.I. Udoskonalenny metod rozrobky ARI pidvyshchenoyi shvydkodiyi Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya 2021: - №1 (50). - S. 31–35
- [21] Savyts'ka L. A. Prohramnyy modul' poperedn'oho diahnostuvannya patsiyentiv na osnovi neyronnoyi merezhi Kokhonena [Tekst] / L. A. Savyts'ka, N. V. Dobrovols'ka, V. O. Kondratyuk // Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya. – 2023. – № 1. – S. 66-74.

Відомості про авторів

Савицька Людмила Анатоліївна, к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Savytska Liudmyla, PhD, associate professor of computing engineering department, Vinnytsya national technical university

Коробейнікова Тетяна Іванівна, к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana, PhD, associate professor of information technology security department, National university "Lvivska Politechnika"

Костюк Олег Віталійович, магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Kostiuk Oleh Vitaliyovych, magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering

Колесник Ірина Сергіївна, к.т.н. доцент, доцент кафедри обчислювальної техніки

Kolesnyk Iryna Sergiivna, PhD candidate of engineering sciences, associate professor of department of the computing engineering, Vinnytsya national technical university

Дудник Олександр Вікторович, к.т.н., ст. викладач кафедри обчислювальної техніки

Dudnyk Oleksandr Viktorovich, PhD, senior lecturer of department of the computing engineering, Vinnytsya national technical university

L. Savytska¹, T. Korobeinikova², O. Kostiuk¹, I. Kolesnyk¹, O. Dudnyk¹

INTERNET OF THINGS PROTECTION MEANS IN THE CORPORATE COMPUTER NETWORK

¹Vinnytsya national technical university, Vinnytsya

²National university "Lvivska Politechnika"

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 00467

В.І Манжула, М.П. Дивак, А. М. Мельник

МЕТОД СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ НЕЛІНІЙНИХ
МОДЕЛЕЙ СТАТИЧНИХ СИСТЕМ НА ОСНОВІ
ІНТЕРВАЛЬНИХ ДАНИХ

Західноукраїнський національний університет, м. Тернопіль

Анотація. У статті розглянуто важливу наукову задачу подальшого розвитку методів ідентифікації інтервальних нелінійних моделей статичних характеристик складних об'єктів на основі використання процедур, які знижують обчислювальну складність. Запропонований підхід до математичного моделювання статичних характеристик нелінійних об'єктів, що ґрунтується на інтервальному аналізі даних, забезпечує побудову адекватних моделей з гарантованими прогностичними властивостями. Процес побудови інтервальних нелінійних моделей статичних характеристик складних об'єктів ґрунтується на оптимізаційній задачі з нелінійною функцією мети, яка забезпечує мінімізацію середньоквадратичного відхилення між значеннями модельованої статичної характеристики складного об'єкта та значеннями які належать до експериментальних інтервалів. Такий підхід призводить до розширення простору параметрів нелінійних інтервальних моделей за рахунок введення додаткових коефіцієнтів α у функцію мети, але в той же час уможливує зведення оптимізаційної задачі з системою нелінійних обмежень до задачі без обмежень. Основним результатом проведених досліджень є новий метод синтезу структури моделі на підставі аналізу градієнта цільової функції оптимізаційної задачі для різного набору структурних елементів. В основі розроблення цього методу є нова процедура вибору структурних елементів моделей, яка уможливує зменшення кількості ітерацій параметричної ідентифікації на етапі формування структур претендентів. У статті визначено та обґрунтовано необхідні та достатні умови вичерпаності чи оптимальності набору структурних елементів на основі аналізу градієнта цільової функції та сформульовано основні правила формування набору цих елементів у моделі. На основі теоретичних та практичних міркувань запропоновано алгоритм реалізації нового методу структурної ідентифікації та продемонстровано його збіжність на прикладі моделювання об'єктів малої гідроенергетики. Запропонований метод ідентифікації нелінійних моделей на основі аналізу інтервальних даних забезпечує розвиток прикладних досліджень у сферах оборони країни, охорони довкілля, медицини та інших галузях, де основою для прийняття рішень є математичні моделі.

Ключові слова: інтервальні дані, інтервальна нелінійна модель, структурна ідентифікація, оптимізаційна задача, цільова функція, градієнт

Abstract. The article considers an important scientific task of further development of methods for identifying interval nonlinear models of static characteristics of complex objects based on the use of procedures that reduce computational complexity. The proposed approach to mathematical modeling of static characteristics of non-linear objects, based on interval data analysis, ensures the construction of adequate models with guaranteed prognostic properties. The process of constructing interval nonlinear models of the static characteristics of complex objects is based on an optimization problem with a nonlinear objective function that ensures the minimization of the mean square deviation between the values of the simulated static characteristics of the complex object and the values belonging to the experimental intervals. This approach leads to the expansion of the parameter space of nonlinear interval models due to the introduction of additional α coefficients into the objective function, but at the same time, it makes it possible to reduce the optimization problem with a system of nonlinear constraints to a problem without constraints. The main result of the conducted research is a new method of synthesis of the model structure based on the analysis of the gradient of the objective function of the optimization problem for a different set of structural elements. The basis of the development of this method is a new procedure for selecting structural elements of models, which makes it possible to reduce the number of iterations of parametric identification at the stage of forming candidate model structures. The article defines and substantiates the necessary and sufficient conditions for the completeness or optimality of a set of structural elements based on the analysis of the gradient of the objective function and formulates the basic rules for forming a set of these elements in the model. Based on theoretical and practical considerations, an algorithm for implementing a new method of structural identification is proposed, and its convergence is demonstrated in the example of modeling of small hydropower facilities. The proposed method of identifying nonlinear models based on the analysis of interval data ensures the development of applied research in the fields of national defense, environmental protection, medicine, and other fields where mathematical models are the basis for decision-making.

Keywords: interval data, interval nonlinear model, structural identification, optimization problem, objective function, gradient

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-94-104>.

Вступ

Задача структурної ідентифікації інтервальних моделей виникає у випадку необхідності встановлення та відображення причинно-наслідкових зв'язків між чинниками управління та характеристиками об'єкта. Такі задачі розв'язувалися для великої кількості сфер застосування зокрема екології, медицини, енергетики тощо [1-3]. Як правило, задачу формулюють у вигляді оптимізаційної задачі, в якій невідомими є як структурні елементи, так і параметри моделей. Для розв'язування задачі ідентифікації використовують експериментальні дані, при цьому необхідно враховувати похибки. Якщо похибки мають випадковий характер, то у цьому випадку використовують методи стохастичної оптимізації, які переважно ґрунтуються на методах групового урахування аргументів [4, 5]. У випадку, коли маємо не велику вибірку даних, але можемо визначити граничні межі похибок спостережень, то використовують аналіз інтервальних даних. Оптимізаційні задачі структурної ідентифікації, які формулюють для випадку інтервальних даних, мають комбінаторну складність [6, 7]. При цьому функція мети, яка використовується в таких за-

дачах є нелінійною або дискретною. В цьому випадку необхідне застосування методів глобального пошуку [7].

Останнім часом, для розв'язування цієї задачі використовують методи, що ґрунтуються на ройовому інтелекті, зокрема на поведінкових моделях бджолиної колонії [8-12]. Ці методи є універсальними і достатньо ефективними. Але, у випадку побудови статичних моделей на основі аналізу інтервальних даних, їх застосування є недоцільним через надмірно високу складність [13]. Аналіз зазначених методів, а також аналіз можливих варіантів постановки задачі структурної ідентифікації в працях показує, що через певну модифікацію функції мети, з метою приведення її до гладкої функції, для розв'язання таких задач також можуть застосовуватися комбінації градієнтних методів [14-16]. Таким чином, у статті розглянуто метод структурної ідентифікації інтервальних моделей на основі комбінації градієнтних методів при розв'язуванні оптимізаційної задачі.

Мета

Метою праці є розробка нового методу ідентифікації структури інтервальних нелінійних моделей статичних систем.

В основу методу покладено підхід вибору структурних елементів при синтезі структури моделі на основі аналізу градієнта функції мети в поточній точці.

Постановка задачі

Статичні об'єкти, як правило, описують функціональними залежностями між значеннями вхідних факторів та вихідними значеннями характеристик об'єкта у вигляді алгебраїчного виразу:

$$y(X) = f_1(\vec{\beta}, X) + f_2(\vec{\beta}, X) + \dots + f_m(\vec{\beta}, X), \quad (1)$$

де

$y(X)$ – модельоване значення характеристики статичного об'єкта;

$\vec{\beta}$ – вектор параметрів моделі, значення яких потрібно оцінити на основі експериментальних даних;

$\lambda_m = \{f_1(\vec{\beta}, X), f_2(\vec{\beta}, X), \dots, f_m(\vec{\beta}, X)\}$ – множина базисних функцій від вхідних змінних X та від вектора параметрів $\vec{\beta}$ моделі.

В якості базисних функцій в залежності від специфіки досліджуваних статичних об'єктів можуть використовуватися нелінійні функції [16]:

показникові:

$$f(\vec{\beta}, X) = \beta_1 \cdot X^{\beta_2};$$

гаусові моделі:

$$f(\vec{\beta}, X) = \beta_1 \cdot e^{\left[-\frac{(X-\beta_2)^2}{\beta_3}\right]};$$

тригонометричні ряду Фур'є

$$f(\vec{\beta}, X) = \beta_1 \cdot \cos(\beta_3 \cdot X) + \beta_2 \cdot \sin(\beta_3 \cdot X)$$

m – задана кількість базисних функцій моделі, тобто її структурних елементів.

Результати експерименту, які необхідні для ідентифікації нелінійних (в загальному вигляді) моделей (1) отримують у такому вигляді:

$$\vec{X}_i \rightarrow [y_i^-; y_i^+], i = 1, \dots, N, \quad (2)$$

де

$[y_i^-; y_i^+]$ – нижня та верхня межі експериментально отриманих значень характеристики статичного об'єкта в i -му спостереженні, $i = 1, \dots, N$;

\vec{X}_i – значення факторів впливу (вхідних змінних) на систему або характеристику об'єкта в i -му спостереженні;

N – загальна кількість спостережень (вимірювань) в експерименті.

Якщо для заданої моделі на основі множини базисних функцій λ_m отримані інтервальні оцінки вектора параметрів $[\vec{\beta}^m]$, то інтервальна модель для опису залежності характеристики статичного об'єкта від вхідних змінних матиме вигляд інтервального нелінійного алгебраїчного виразу:

$$[\hat{y}(X)] = f_1([\vec{\beta}^m], X) + f_2([\vec{\beta}^m], X) + \dots + f_m([\vec{\beta}^m], X), \quad (3)$$

де

$[\hat{y}(X)] = [\hat{y}^-(X); \hat{y}^+(X)]$ – обчислені інтервальні оцінки модельованої характеристики, відповідно до структури λ_m та вхідних даних X ;

$[\vec{\beta}^m] = ([\beta_1^m], [\beta_2^m], \dots, [\beta_m^m])$ – вектор інтервальних оцінок параметрів моделі.

На підставі умови, що обчислені інтервальні оцінки $[\hat{y}(X)]$ належать числовим інтервалам експериментальних даних

$$[\hat{y}^-(\vec{X}_i); \hat{y}^+(\vec{X}_i)] \in [y_i^-; y_i^+], i = 1, \dots, N \quad (4)$$

для цієї характеристики об'єкта, які отримані експериментально, отримуємо математичну задачу для обчислення інтервальних оцінок вектора параметрів $[\vec{\beta}^m]$ моделі для заданої структури λ_m [13].

$$\{y_i^- \leq f_1([\vec{\beta}], \vec{X}_i) + f_2([\vec{\beta}], \vec{X}_i) + \dots + f_m([\vec{\beta}], \vec{X}_i) \leq y_i^+, i = 1, \dots, N. \quad (5)$$

Отримана система (5) є інтервальною системою нелінійних алгебраїчних рівнянь (ІСНАР) для невідомих інтервальних оцінок вектора параметрів $[\vec{\beta}^m]$ моделі на основі λ_m . Функціональна залежність у формі виразу (3) називається інтервальною моделлю об'єкта, що розглядається як статична система.

Множина розв'язків ІСНАР Ω визначає вектор інтервальних оцінок параметрів $[\vec{\beta}^m]$ моделі. Через високу (комбінаторну) обчислювальну складність розв'язку цієї ІСНАР, на практиці обчислюються лише точкові оцінки параметрів $\vec{\beta}^m$. У цьому випадку, для оцінки параметрів розв'язують оптимізаційну задачу такого вигляду [2]:

$$\delta(\vec{\beta}^m) \xrightarrow{\vec{\beta}^m, \alpha_i} \min \quad (6)$$

$$\lambda_m \in \lambda_s, \quad (7)$$

$$\alpha_i \in [0,1], i = 1, \dots, N \quad (8)$$

де

λ_s – множина всіх можливих елементів структури інтервальної моделі;

s – кількість всіх можливих елементів структури;

α_i – коефіцієнти лінійної комбінації для визначення точки в межах експериментальних даних $[y_i^-; y_i^+]$.

У виразі (6), цільова функція $\delta(\vec{\beta}^m)$ формується на основі врахування обмежень, які задає інтервальна система нелінійних алгебраїчних рівнянь (5) [2].

Цільова функція є критерієм мінімізації квадратичної похибки, точкової моделі вигляду:

$$\hat{y}_i(\vec{X}_i) = f_1(\vec{\beta}_1, \vec{X}_i) + f_2(\vec{\beta}_2, \vec{X}_i) + \dots + f_m(\vec{\beta}_m, \vec{X}_i), i = 1, \dots, N, \quad (9)$$

та має такий вигляд [2]:

$$\delta(\vec{\beta}^m) = \sum_{i=1}^N (\hat{y}_i(\vec{X}_i) - P([y_i^-; y_i^+], \alpha_i))^2, i = 1, \dots, N, \quad (10)$$

де

$$P([y_i^-; y_i^+], \alpha_i) = \alpha_i \cdot y_i^- + (1 - \alpha_i) \cdot y_i^+, i = 1, \dots, N. \quad (11)$$

Запропонований в праці [17] підхід до параметричної ідентифікації інтервальних нелінійних моделей статичних систем, полягає у приведенні цієї задачі ідентифікації до розв'язування стандартної задачі мінімізації середньоквадратичного відхилення між значеннями модельованої характеристики статичного об'єкта та значеннями які належать до експериментальних інтервалів. Такий підхід призводить до розширення простору параметрів нелінійних моделей за рахунок введення додаткових коефіцієнтів α у функції мети, які забезпечують узгодженість обчислених на основі моделі та експериментальних даних. Таким чином отримуємо задачу багатовимірної оптимізації з нелінійною багатоекстремальною функцією мети.

В той же час, задача структурної ідентифікації полягає у необхідності визначення як структури моделі $\lambda_m \in \lambda_s$, тобто множини структурних елементів, так і параметрів моделі $\vec{\beta}^m$ на її основі.

Запишемо задачу структурної ідентифікації на основі задачі (6) у такому вигляді:

$$\delta(\vec{\lambda}_m, \vec{\beta}^m) \xrightarrow{\vec{\lambda}_m, \vec{\beta}^m, \alpha_i} \min \quad (12)$$

$$\lambda_m \in \lambda_s, \quad (13)$$

$$\alpha_i \in [0,1], i = 1, \dots, N. \quad (14)$$

В якості критерію зупинки оптимізації використовують умову (4) для випадку точкової моделі [17]:

$$\hat{y}_i(\lambda_m, \vec{X}) \in [y_i^-; y_i^+], i = 1, \dots, N. \quad (15)$$

Істинність такого твердження гарантує адекватність та задану точність побудованої моделі.

Складність даної задачі полягає в тому, що дана функція є дискретною, оскільки оптимізації відбувається на основі дискретних значень вектора $\vec{\lambda}_s$ – дискретні значення елементів множини λ_s якого отримуються на основі певної системи кодування. Тому її розв'язок будують на основі багаторазового розв'язку задачі параметричної ідентифікації (6) з напрямленим перебором множин λ_m на основі елементів множини λ_s .

Огляд літературних джерел

На сьогоднішній день розроблено ряд методів параметричної ідентифікації інтервальних моделей

як для динамічних об'єктів так і для статичних [18,19]. Треба відзначити, що оптимізаційна задача параметричної ідентифікації інтервальних моделей є обчислювальною NP-складною задачею. Особливостями задачі параметричної та структурної ідентифікації інтервальних нелінійних моделей статичних систем є те що в процесі оптимізації доводиться здійснювати пошук глобального мінімуму функції мети і при цьому здійснювати обхід чи вихід з багаточисленних локальних мінімумів. Тому для їх розв'язування переважно застосовують метаевристичні методи стохастичного пошуку. Зокрема, на сьогоднішній день найбільш ефективними з обчислювальної точки зору є методи, які побудовано на основі ройового інтелекту [10-22]. Для їх реалізації роблено ряд спеціалізованих програмних засобів, наведених, наприклад у працях [6, 18, 23]. Разом з тим, дослідниками таких оптимізаційних задач широко використовуються відомі програмні рішення, наведені в ряді стандартних пакетів прикладних програм, зокрема у Global Optimization Toolbox ППП MATLAB [24].

Аналіз методів структурної ідентифікації нелінійних інтервальних моделей продемонстрував, що основною проблемою, яка породжує комбінаторну або стохастичну складову оптимізації, є вибір структурних елементів з множини λ_s для формування вектора $\vec{\lambda}_m$. Основний підхід базується на оціненні (оптимізації параметрів на основі задачі (6-8)) для кожного вектора $\vec{\lambda}_m$ який був сформований внаслідок комбінації, селекції або мутації.

Тому стоїть завдання розробки процедур ідентифікації як параметрів так і структури інтервальних нелінійних моделей зі зниженням обчислювальної складності. Це досягається на основі розроблення методу вибору структурних елементів, який би уможливив зменшення кількості процедур параметричної ідентифікації на етапі формування структур моделей-претендентів.

Метод структурної ідентифікації інтервальних нелінійних моделей на основі аналізу градієнта цільової функції

Оскільки цільова функція (12) є гладкою для деякого фіксованого вектора $\vec{\lambda}_m$, то для її дослідження можна використати градієнтні методи.

Нехай задано деяку модель-претендент зі структурою на основі вектора $\vec{\lambda}_k$ та вектора параметрів $\vec{\beta}^m$. Для дослідження якості структури моделі-претендента запропоновано використовувати антиградієнт цільової функції $\delta(\vec{\lambda}_m, \vec{\beta}^m)$ в точці $\vec{\beta}^k$. Для моделі-претендента на основі вектора $\vec{\lambda}_m$, із розмірністю m величина вектора антиградієнту $-\nabla$ відносно вектора параметрів $\vec{\beta}^m$ вказує на напрям мінімізації цільової функції $\delta(\vec{\lambda}_m, \vec{\beta}^m)$. Відповідно, для структури $\vec{\lambda}_m$ заданого розміру m вектор антиградієнту позначимо так:

$$-\nabla \delta(\vec{\lambda}_m, \vec{\beta}^m) = \left(\frac{d\delta(\vec{\lambda}_m, \vec{\beta}^m)}{d\beta_1^m}, \frac{d\delta(\vec{\lambda}_m, \vec{\beta}^m)}{d\beta_2^m}, \dots, \frac{d\delta(\vec{\lambda}_m, \vec{\beta}^m)}{d\beta_m^m} \right). \quad (16)$$

Спираючись на властивість похідних багатовимірної функції по її змінних, можемо стверджувати, що необхідною та достатньою умовою оптимальності набору структурних елементів $\vec{\lambda}_m$ моделі-претендента в сенсі задачі (12-14) є мінімум норми вектора антиградієнта $\|-\nabla \delta(\vec{\lambda}_m, \vec{\beta}^m)\|$ цільової функції (2.12) в точці $\vec{\beta}^m$.

Спираючись на цю умову запропоновано наступні правила вибору структурних елементів в ході синтезу структури при реалізації методу структурної ідентифікації на основі градієнта цільової функції.

Правило 1. Необхідною та достатньою умовою оптимальності набору структурних елементів $\vec{\lambda}_k$ моделі-претендента в сенсі задачі (12-14) для фіксованої кількості параметрів m_k є мінімум норми вектора антиградієнта $\|-\nabla \delta(\vec{\lambda}_m, \vec{\beta}^m)\|$ цільової функції (12) в точці $\vec{\beta}^m$.

У випадку виконання цієї умови виконуємо одну з двох дій: якщо умова (5) виконується, то зупинка алгоритму, оскільки знайдено розв'язок задачі (12-14), в протилежному випадку, маємо «вичерпаність» розмірності моделі і відповідно збільшуємо кількість структурних елементів $m + 1$.

Правило 2. (випадок невиконання правила 1.) Найбільш придатним кандидатом серед усіх структурних елементів для структури $\vec{\lambda}_m$ є той який забезпечує найкращу мінімізацію цільової функції (12), що визначається віддаленістю її мінімуму для моделі з вибраним структурним елементом на основі норми антиградієнта.

Для кількісної оцінки придатності нових структурних елементів запропоновано використовувати значення похідної цільової функції $\frac{d}{d\beta_v} \delta(\vec{\beta}_v^m, f_w^s(\vec{\beta}^m, X)) \Big|_{\beta=\vec{\beta}_v^m, \delta=\min \delta(\vec{\lambda}_m, \vec{\beta}^m)}$ на основі моделі для якої визначено мінімум цільової функції та із врахуванням нових структурних елементів $f_w^s(\vec{\beta}^m, X)$, $w = m + 1, \dots, s$.

На рисунку 1 проілюстровано приклад, який демонструє, що такий підхід забезпечує відкидання структурних елементів, що погіршують якість моделі, оскільки для них не існує значення похідної в заданій точці та можливість вибору найкращого структурного елемента для поточної моделі. При цьому числове значення похідної в точці буде свідчити про здатність структурного елемента забезпечити мінімізацію цільової функції. Відповідно, необхідно вибирати структурний елемент із максимальним значенням похідної в точці.

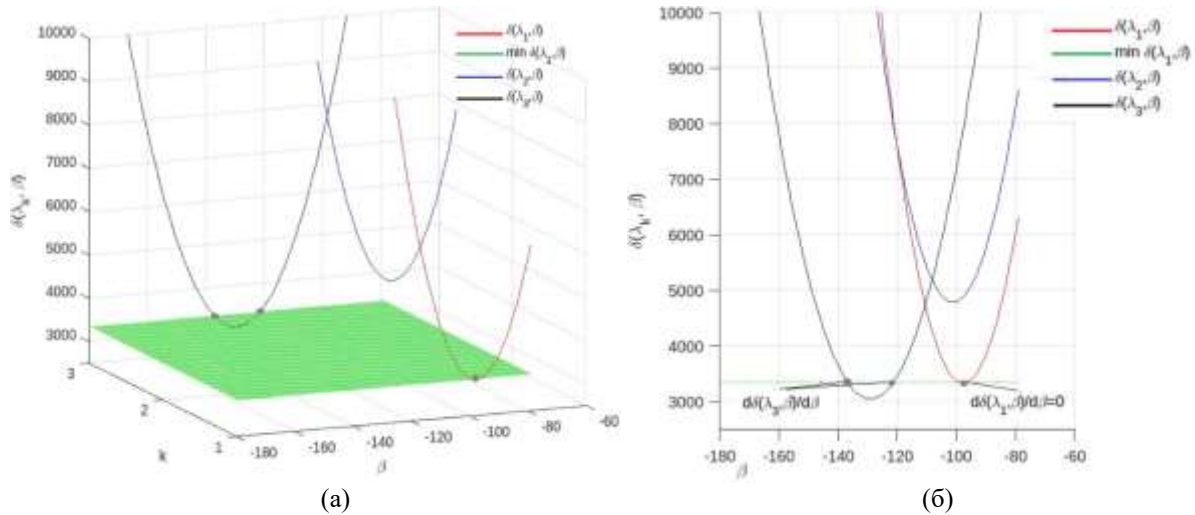


Рисунок 1 – Ілюстрація вибору структурного елемента на основі оцінки градієнта цільової функції.

На рисунку 1(а) відображено графіки цільової функції на основі трьох моделей із структурою $\lambda_1, \lambda_2, \lambda_3$. При цьому на основі моделі із структурою λ_1 визначено глобальний мінімум цільової функції $\delta(\vec{\lambda}_1, \vec{\beta}^1)$. Значення мінімуму використовується для пошуку похідної цільової функції з метою вибору нових структурних елементів, які забезпечать її мінімізацію. Як бачимо на рисунку 1(б), структурний елемент, який формує структуру λ_2 не забезпечує мінімізацію цільової функції та, відповідно, не враховується для формування поточної структури. Відповідно, структурний елемент, що формує структуру λ_3 , є претендентом для вибору.

На основі теоретичних та практичних міркувань алгоритм структурної ідентифікації нелінійних інтервальних моделей базується на мінімізації функції мети в просторі параметрів із напрямленим вибором дискретних значень структури моделі.

Псевдокод алгоритму структурної ідентифікації наведено нижче:

```

Stop_Criterion = FALSE;
Сформувати множину можливих структурних елементів,  $\lambda_s$ ;
s = length( $\lambda_s$ );
k=1;
Задати початкову структуру:
 $\lambda_k = \{f_1^k(\hat{\beta}_1^k, \vec{X}), \dots, f_{m_k}^k(\hat{\beta}_{m_k}^k, \vec{X})\}$ ;
Поки Stop_Criterion == FALSE:
    m = length( $\lambda_k$ );
    Обчислити вектор оцінок параметрів  $\vec{\beta}^k$  моделі на основі  $\lambda_k$ ;
    Якщо модель адекватна:
        Stop_Criterion = TRUE;
    В іншому випадку:
        Для v від 1 до m
            Для w від 1 до s
                Обчислити похідну функції мети по v-му параметру для w-го структурного
                елемента,  $\frac{d}{d\beta_v} \delta(\hat{\beta}_v^k, f_w^s(\hat{\beta}^k, X))$ ;
            Кінець для w
        Кінець для v
    
```

Знайти вектор антиградієнта на основі k -ї структури, $-\nabla \delta(\vec{\lambda}_k, \vec{\beta}^k)$;

Якщо $\|-\nabla \delta(\vec{\lambda}_k, \vec{\beta}^k)\| \neq 0$

Для v від 1 до m

Якщо $\left\| \frac{d}{d\beta_v} \delta(\vec{\beta}^k, f_w^s(\vec{\beta}^k, X)) \right\| > 0$:

Замінити у структурі λ_k згідно з правилом 2 елемент $f_v^k(\vec{\beta}^k, X)$ на $f_w^s(\vec{\beta}, X)$;

Кінець якщо

Кінець для v

В іншому випадку:

$k=k+1$;

Додати у структуру λ_k новий елемент $f_w^s(\vec{\beta}, X)$;

Кінець якщо

Кінець якщо

Кінець поки

Для обчислення антиградієнта можна використовувати чисельний метод або аналітичний вираз для значень часткових похідних в точці $\vec{\beta}^k$ на основі заданих структурних елементів:

$$\begin{aligned} \frac{d}{d\beta_v^k} \delta(\beta_v^k, f_w^s(\vec{\beta}^k, X)) &= \frac{d}{d\beta_v} \sum_{i=1}^N \left(\frac{\hat{y}_i(\lambda_k, \vec{\beta}^k) - P([y_i^-, y_i^+], \alpha_i) +}{f_v^k(\vec{\beta}^k, \vec{X}_i)} \right)^2 = \\ &2 \cdot \sum_{i=1}^N \left(\frac{\hat{y}_i(\lambda_k, \vec{\beta}^k) - P([y_i^-, y_i^+], \alpha_i) +}{f_v^k(\beta_v^k, \vec{X}_i)} \right) \cdot \frac{d}{d\beta_v} \sum_{l=1}^N f_v^s(\beta_v^k, \vec{X}_l), \end{aligned} \quad (17)$$

де

$$\hat{y}_i(\lambda_k, \vec{\beta}^k) = \sum_{q=1}^{m_k} f_q(\vec{\beta}_q, \vec{X}_i), q \neq v;$$

β_v^k – параметр моделі за яким здійснюється диференціювання цільової функції, $\beta_v^k \in \vec{\beta}^k$;

$f_v^s(\beta_v^k, \vec{X}_i)$ – структурний елемент, що не є елементом моделі-претендента, $f_v^s(\beta_v^k, \vec{X}_i) \in \lambda_s \wedge f_v^s(\beta_v^k, \vec{X}_i) \notin \lambda_k$.

Експерименти, результати та обговорення

Моделювання генерованої потужності МГЕС

Завдання відновлення існуючих та створення нових малих гідроелектростанцій (МГЕС) є нагальними, враховуючи потенціал гідроресурсів в Україні. У той же час доцільно розробити математичні моделі характеристик гідроелектростанції з метою дослідження та забезпечення максимальної ефективності використання гідроенергетичних ресурсів. За приклад таких досліджень обрано МГЕС «Топольки», яку побудовано на річці Стрипа в Тернопільській області. Зазначена МГЕС має дві турбіни, які з'єднано з генераторами з потужністю 70 та 90 кВт. Робота генераторів в системі вимагає постійної оцінки стану характеристик гідроресурсів та прогнозування можливої генерованої електроенергії з метою заощадливого використання обладнання станції. Зокрема, необхідним є прогнозування кожен раз при зміні погодних умов та сезонних коливань наявних гідроресурсів, з метою прийняття рішень про доцільність використання двох турбін одночасно, або використання однієї з двох турбін є доцільним. В такому випадку, одну із турбін можемо виводити на ремонт. Таким чином, виникає необхідність розробки та використання моделі, яка пов'язує кількість потенційно можливої згенерованої електроенергії в залежності від характеристик гідротехнічного обладнання та наявних гідроресурсів. Для ідентифікації цієї математичної моделі використаємо розроблений метод структурної та параметричної ідентифікації нелінійних моделей.

Експериментальні дані

У результаті досліджень цієї МГЕС було отримано експериментальні дані [25].

Як бачимо з таблиці 1, кількість виробленої за добу електроенергії представлено в інтервальному вигляді внаслідок похибок оцінювання цієї величини технічними засобами.

Апробація методу та обговорення

Сформована множина усіх потенційних структурних елементів для моделі залежності генерованої потужності від умов функціонування МГЕС:

$$\lambda_s = \{x_1, x_2, x_3, x_1^{\beta_1}, x_2^{\beta_1}, x_3^{\beta_1}, x_1 \cdot x_2^{\beta_1}, x_1 \cdot x_3^{\beta_1}, x_2 \cdot x_3^{\beta_1}, x_1^{\beta_1} \cdot x_2^{\beta_2}, x_1^{\beta_1} \cdot x_3^{\beta_2}, x_2^{\beta_1} \cdot x_3^{\beta_2}\}$$

Із використанням методу структурної ідентифікації, наведеного вище, отримано таку структуру інтервальної моделі добового генерування електроенергії:

$$y(\lambda_5, X) = \beta_1 \cdot x_1 \cdot x_2^{\beta_2} + \beta_2 \cdot x_3^{\beta_4} \quad (18)$$

та оцінки параметрів для отриманої моделі:

$$\hat{\beta} = (88.619, 0.4256, 2.5533, 0.4914)$$

$$\hat{\alpha} = (0.1985, 0.273, 0.1713, 0.0865, 0.6162, 0.9991, 0.8814, 0.397, 0.7368, 0.5845, 0.5823, 0.4998, 0.4427, 0.5582, 0.2692, 0.1964, 0.0002, 0.9202, 0.675, 0.3728, 0.4643, 0.7596, 0.9164, 0.9667, 0.2294, 0.9564, 0.7288, 0.3038, 0.9127, 0.1438).$$

Таблиця 1 – Експериментальні дані генерування електроенергії МГЕС

№	Реактивна потужність, Вт	Напір (різниця б'єфів), м	Рівень води на гідропості, м	Вироблена електроенергія, кВт
1	182,5	4,6	6,5	[1096,4; 1202,1]
2	182,7	4,7	5,5	[1078,1; 1182,1]
3	182,7	4,7	4,97	[1078,1; 1182,1]
4	182,7	4,7	5,45	[1096,4; 1202,1]
5	182,9	4,7	7,5	[1078,1; 1182,1]
6	183	4,7	11,9	[1096,4; 1202,1]
7	183,1	4,7	12,5	[1114,6; 1222,1]
8	183,1	4,7	9,8	[1132,9; 1242,2]
9	183,1	4,55	10,4	[1096,4; 1202,1]
10	183,1	4,6	13,7	[1151,2; 1262,2]
11	184,6	4,6	14,9	[1169,5; 1282,2]
12	184,6	4,6	14	[1169,5; 1282,2]
13	184,6	4,7	12,8	[1169,5; 1282,2]
14	184,7	4,65	12,5	[1151,2; 1262,2]
15	184,8	4,6	11,6	[1169,5; 1282,2]
16	184,8	4,7	10,4	[1169,5; 1282,2]
17	184,8	4,7	10,1	[1187,7; 1302,3]
18	184,8	4,8	7,3	[1059,8; 1162]
19	187,2	4,8	7,5	[1096,4; 1202,1]
20	187,2	4,7	7,1	[1114,6; 1222,1]
21	187,2	4,8	7,3	[1114,6; 1222,1]
22	187,2	4,75	8,3	[1096,4; 1202,1]
23	187,2	4,7	8,3	[1078,1; 1182,1]
24	189,1	4,6	7,24	[1059,8; 1162]
25	189,1	4,7	5,74	[1114,6; 1222,1]
26	189,2	4,7	4,64	[1023,3; 1122]
27	189,4	4,6	4,78	[1041,6; 1142]
28	189,4	4,8	5,74	[1114,6; 1222,1]
29	189,4	4,8	4,11	[1023,3; 1122]
30	189,5	4,75	5,01	[1114,6; 1222,1]

Відповідно, побудовано математичну модель на основі інтервальних даних та структури (18) у такому вигляді:

$$y(X) = 88.619 \cdot x_1 \cdot x_2^{0.4256} + 2.5533 \cdot x_3^{0.4914}. \quad (19)$$

Графічне представлення виконання умови (15) для отриманої моделі, тобто включення прогнозованих на основі моделі (19) значень у експериментальний коридор, що отриманий на основі вимірювань, наведено на рисунку 2.

Ефективність запропонованого підходу та алгоритму його реалізації демонструє збіжність даного алгоритму в ході структурної ідентифікації моделі (19). Графік збіжності цільової функції наведено на рисунку 3.

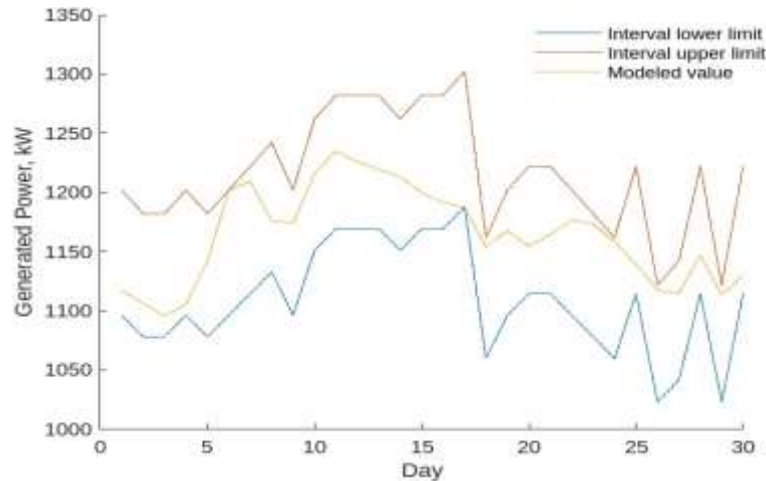


Рисунок 2 – Графічне представлення виконання умови (15) для отриманої моделі

Як бачимо, для вхідної множини λ_s із 12 структурних елементів кількість оцінених моделей склала п'ять, що свідчить про ефективність даного методу не зважаючи на додаткові обчислювальні затрати щодо аналізу похідної цільової функції.

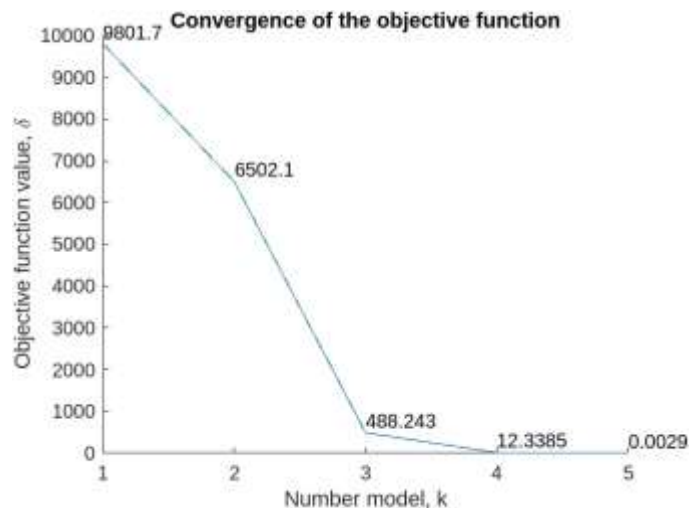


Рисунок 3 – Ілюстрація збіжності алгоритму структурної ідентифікації для моделі (19)

Висновки.

Отже, в роботі запропоновано новий метод структурної ідентифікації інтервальних нелінійних моделей, який ґрунтується на виборі структурних елементів для синтезу структури моделі із використанням аналізу градієнта цільової функції. Визначено та обґрунтовано необхідні та достатні умови «вичерпаності» чи оптимальності набору структурних елементів на основі аналізу градієнта цільової функції та сформульовано основні правила вибору структурних елементів. Реалізовано алгоритм структурної ідентифікації та проведено дослідження його збіжності.

Апробація запропонованого методу та алгоритму його реалізації показала ефективність запропонованого підходу до структурної ідентифікації інтервальних нелінійних моделей. На прикладі показано, що вигравш від застосування процедур аналізу похідної цільової функції переважає додаткові обчислювальні затрати на них.

Список літератури

[1]M. Dyvak, I. Voytyuk, N. Porplytsya and A. Pukas, "Modeling the process of air pollution by harmful emissions from vehicles," 2018 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Slavske, 2018, pp. 1272-1276, doi: 10.1109/TCSET.2018.8336426.

[2]M. Dyvak, V. Manzhula, Yu. Trufanova. Interval Non-linear Model of Information Signal Characteristics Distribution for Detection of Recurrent Laryngeal Nerve during Thyroid Surgery. In: Proceedings of

the 5th International Conference on Informatics & Data-Driven Medicine (IDDM-2022), CEUR Workshop Proceedings, 2022, 3302, pp. 99–107

[3] Dyvak, M., Papa, O., Melnyk, A., Pukas, A., Porplytsya, N., Rot, A. Interval model of the efficiency of the functioning of information web resources for services on ecological expertise (2020) *Mathematics*, 8 (12), art. no. 2116, pp. 1-12.

[4] A. Ivakhnenko, G. Ivakhnenko, “The Review of Problems Solvable by Algorithms of the Group Method of Data Handling (GMDH)”, *Pattern Recognition and Image Analysis*, 5 (4), pp. 527-535, 1995.

[5] O. G. Moroz, V. S. Stepashko, Combinatorial algorithm of MGUA with genetic search of the model of optimal complexity, Proceedings of the International Conference on Intellectual Systems for Decision Making and Problems of Computational Intelligence, 2016, pp. 297–299.

[6] M. Dyvak, I. Spivak, A. Melnyk, V. Manzhula, T. Dyvak, A. Rot, M. Hernes, “Modeling Based on the Analysis of Interval Data of Atmospheric Air Pollution Processes with Nitrogen Dioxide due to the Spread of Vehicle Exhaust Gases”, *Sustainability*, 15(3):2163, 2023. <https://doi.org/10.3390/su15032163>

[7] M. Dyvak; N. Porplytsya; Y. Maslyiak and N. Kasatkina. Modified artificial bee colony algorithm for structure identification of models of objects with distributed parameters and control. 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, 2017, pp. 50-54.

[8] A. Petrowski, S. Ben-Hamida, *Evolutionary Algorithms (Computer Engineering: Metaheuristics Book 9)*, 1st ed. Wiley-ISTE: Hoboken, NJ, USA, 2017.

[9] S. Katoch, S.S. Chauhan, V. Kumar, “A review on genetic algorithms: Past, present, and future”, *Multimed. Tools Appl.*, 80, 8091–8126, 2021. [CrossRef] [PubMed]

[10] I.T. Christou, W.L. Darrell, K. De Long, W. Martin, *Evolutionary Algorithms*”, Springer-Verlag: New York, NY, USA, 2021.

[11] A. Slowik, *Swarm Intelligence Algorithms: Modification and Applications*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2020.

[12] A. Abraham, R.K. Jatoth, A. Rajasekhar, “Hybrid differential artificial bee colony algorithm”, *J. Comput. Theor. Nanosci.*, 9, 249–257, 2012.

[18] S. Alshattnawi, L. Afifi, A.M. Shatnawi, M.M. Barhoush, “Utilizing Genetic Algorithm and Artificial Bee Colony Algorithm to Extend the WSN Lifetime”, *Int. J. Comput.*, 21, 25-31, 2022.

[13] N.P. Dyvak, V.I. Manzhula, “Structural Identification of Interval Models of the Static Systems” *Journal of Automation and Information Sciences*, 40 (4), pp. 49-61, 2008.

[14] Bubeck, S. (2015). Stochastic gradient descent and related optimization methods. *Foundations and Trends in Machine Learning*, 8(3-4), 179-364

[15] Anders Forsgren, Philip E. Gill, Margaret H. Wright, “Interior methods for nonlinear optimization”, *SIAM review*, 44.4, pp. 525-597, 2002.

[16] A. Beck, *Introduction to nonlinear optimization: Theory, algorithms, and applications with MATLAB*, Society for Industrial and Applied Mathematics, 2014.

[17] Manzhula, V., Dyvak, M., & Zabchuk, V. (2024). The Improved Method for Identifying Parameters of Interval Nonlinear Models of Static Systems. *International Journal of Computing*, 23(1), 19-25. <https://doi.org/10.47839/ijc.23.1.3431>

[18] M. Dyvak, N. Porplytsya, I. Borivets, M. Shynkaryk, “Improving the computational implementation of the parametric identification method for interval discrete dynamic models”, in Proc. 12th International Conference on International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), pp. 533-536, Lviv, Ukraine, 5-8 September 2017.

[19] N. Porplytsya, M. Dyvak, I. Spivak, and I. Voytyuk, “Mathematical and algorithmic foundations for implementation of the method for structure identification of interval difference operator based on functioning of bee colony”, in Proc. 13th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), pp. 196-199, Lviv, Ukraine, 24-27 February 2015.

[20] B. Akay, D. Karaboga, B. Gorkemli, E. Kaya, “A survey on the artificial bee colony algorithm variants for binary, integer and mixed integer programming problems”, *Appl. Soft Comput.*, 106, 107351, 2021.

[21] B. Akay, D. Karaboga, “A survey on the applications of artificial bee colony in signal, image, and video processing”, *Signal Image Video Process*, 9, 967–990, 2015.

[22] Slowik A. *Swarm Intelligence Algorithms: modification and applications*. 1st edition. CRC Press. 2020. 378 p.

[23] Dyvak M., Porplytsya N., Maslyiak Y., Kasatkina N. Modified artificial bee colony algorithm for structure identification of models of objects with distributed parameters and control. The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM): Proceedings of the 2017 14th International Conference. Lviv, Ukraine. 21–25 February 2017. P. 50–54.

[24] Global Optimization Toolbox, <https://www.mathworks.com/products/global-optimization.html>.

[25] Пукас А. В. Методи та засоби побудови математичних моделей характеристик складних об'єктів в умовах інтервальної невизначеності: дисертація на здобуття наукового ступеня доктора технічних наук : 01.05.02 – математичне моделювання та обчислювальні методи / Андрій Васильович Пукас ; Міністерство освіти і науки України, Національний університет «Львівська політехніка». – Львів, 2021. – 292 с.

Стаття надійшла: 12.04.2024

References

- [1] M. Dyvak, I. Voytyuk, N. Porplytsya and A. Pukas, "Modeling the process of air pollution by harmful emissions from vehicles," 2018 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Slavske, 2018, pp. 1272-1276, doi: 10.1109/TCSET.2018.8336426.
- [2] M. Dyvak, V. Manzhula, Yu. Trufanova. Interval Non-linear Model of Information Signal Characteristics Distribution for Detection of Recurrent Laryngeal Nerve during Thyroid Surgery. In: Proceedings of the 5th International Conference on Informatics & Data-Driven Medicine (IDDM-2022), CEUR Workshop Proceedings, 2022, 3302, pp. 99–107
- [3] Dyvak, M., Papa, O., Melnyk, A., Pukas, A., Porplytsya, N., Rot, A. Interval model of the efficiency of the functioning of information web resources for services on ecological expertise (2020) *Mathematics*, 8 (12), art. no. 2116, pp. 1-12.
- [4] A. Ivakhnenko, G. Ivakhnenko, "The Review of Problems Solvable by Algorithms of the Group Method of Data Handling (GMDH)", *Pattern Recognition and Image Analysis*, 5 (4), pp. 527-535, 1995.
- [5] O. G. Moroz, V. S. Stepashko, Combinatorial algorithm of MGUA with genetic search of the model of optimal complexity, *Proceedings of the International Conference on Intellectual Systems for Decision Making and Problems of Computational Intelligence*, 2016, pp. 297–299.
- [6] M. Dyvak, I. Spivak, A. Melnyk, V. Manzhula, T. Dyvak, A. Rot, M. Hernes, "Modeling Based on the Analysis of Interval Data of Atmospheric Air Pollution Processes with Nitrogen Dioxide due to the Spread of Vehicle Exhaust Gases", *Sustainability*, 15(3):2163, 2023. <https://doi.org/10.3390/su15032163>
- [7] M. Dyvak; N. Porplytsya; Y. Maslyiak and N. Kasatkina. Modified artificial bee colony algorithm for structure identification of models of objects with distributed parameters and control. 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, 2017, pp. 50-54.
- [8] A. Petrowski, S. Ben-Hamida, *Evolutionary Algorithms (Computer Engineering: Metaheuristics Book 9)*, 1st ed. Wiley-ISTE: Hoboken, NJ, USA, 2017.
- [9] S. Katoch, S.S. Chauhan, V. Kumar, "A review on genetic algorithms: Past, present, and future", *Multimed. Tools Appl.*, 80, 8091–8126, 2021. [CrossRef] [PubMed]
- [10] I.T. Christou, W.L. Darrell, K. De Long, W. Martin, *Evolutionary Algorithms*", Springer-Verlag: New York, NY, USA, 2021.
- [11] A. Slowik, *Swarm Intelligence Algorithms: Modification and Applications*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2020.
- [12] A. Abraham, R.K. Jatoth, A. Rajasekhar, "Hybrid differential artificial bee colony algorithm", *J. Comput. Theor. Nanosci.*, 9, 249–257, 2012.
- [18] S. Alshatnawi, L. Afifi, A.M. Shatnawi, M.M. Barhoush, "Utilizing Genetic Algorithm and Artificial Bee Colony Algorithm to Extend the WSN Lifetime", *Int. J. Comput.*, 21, 25-31, 2022.
- [13] N.P. Dyvak, V.I. Manzhula, "Structural Identification of Interval Models of the Static Systems" *Journal of Automation and Information Sciences*, 40 (4), pp. 49-61, 2008.
- [14] Bubeck, S. (2015). *Stochastic gradient descent and related optimization methods. Foundations and Trends in Machine Learning*, 8(3-4), 179-364
- [15] Anders Forsgren, Philip E. Gill, Margaret H. Wright, "Interior methods for nonlinear optimization", *SIAM review*, 44.4, pp. 525-597, 2002.
- [16] A. Beck, *Introduction to nonlinear optimization: Theory, algorithms, and applications with MATLAB*, Society for Industrial and Applied Mathematics, 2014.
- [17] Manzhula, V., Dyvak, M., & Zabchuk, V. (2024). The Improved Method for Identifying Parameters of Interval Nonlinear Models of Static Systems. *International Journal of Computing*, 23(1), 19-25. <https://doi.org/10.47839/ijc.23.1.3431>
- [18] M. Dyvak, N. Porplytsya, I. Borivets, M. Shynkaryk, "Improving the computational implementation of the parametric identification method for interval discrete dynamic models", in *Proc. 12th International Conference on International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*, pp. 533-536, Lviv, Ukraine, 5-8 September 2017.

[19] N. Porplytsya, M. Dyvak, I. Spivak, and I. Voytyuk, "Mathematical and algorithmic foundations for implementation of the method for structure identification of interval difference operator based on functioning of bee colony", in Proc. 13th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), pp. 196-199, Lviv, Ukraine, 24-27 February 2015.

[20] B. Akay, D. Karaboga, B. Gorkemli, E. Kaya, "A survey on the artificial bee colony algorithm variants for binary, integer and mixed integer programming problems", Appl. Soft Comput., 106, 107351, 2021.

[21] B. Akay, D. Karaboga, "A survey on the applications of artificial bee colony in signal, image, and video processing", Signal Image Video Process, 9, 967-990, 2015.

[22] Slowik A. Swarm Intelligence Algorithms: modification and applications. 1st edition. CRC Press. 2020. 378 p.

[23] Dyvak M., Porplytsya N., Maslyiak Y., Kasatkina N. Modified artificial bee colony algorithm for structure identification of models of objects with distributed parameters and control. The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM): Proceedings of the 2017 14th International Conference. Lviv, Ukraine. 21-25 February 2017. P. 50-54.

[24] Global Optimization Toolbox, <https://www.mathworks.com/products/global-optimization.html>.

[25] A. V. Pukas. Methods and means of constructing mathematical models of the characteristics of complex objects under conditions of interval uncertainty: dissertation for obtaining the scientific degree of Doctor of Technical Sciences: 05.01.02 - mathematical modeling and computational methods / Andriy Vasyliovych Pukas; Ministry of Education and Science of Ukraine, Lviv Polytechnic National University. - Lviv, 2021. - 292 p.

Відомості про авторів

Манжула Володимир Іванович – кандидат технічних наук, доцент, докторант кафедри комп'ютерних наук

Дивак Микола Петрович – доктор технічних наук, професор, проректор з наукової роботи, ЗУНУ, м. Тернопіль

Мельник Андрій Миколайович – доктор технічних наук, професор, професор кафедри комп'ютерних наук, ЗУНУ

V.I. Manzhula, M.P. Dyvak, A. M. Melnyk

STRUCTURAL IDENTIFICATION METHOD OF NONLINEAR MODELS OF STATIC SYSTEMS BASED ON INTERVAL DATA

West Ukrainian National University, Ternopil

УДК 004.9

В. М. Михалевич, Л. О. Майданевич

ВИКОРИСТАННЯ СИСТЕМИ MAPLE В МАТЕМАТИЧНИХ ЗАДАЧАХ КРИПТОГРАФІЇ. ПОВІДОМЛЕННЯ 1. ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ.

Вінницький національний технічний університет, Вінниця

Анотація. На основі аналізу літературних джерел зроблено висновок про актуальність використання середовища системи комп'ютерної математики Maple з метою створення програмного забезпечення для проведення наукових досліджень та створення навчально-методичних матеріалів з розв'язання типових математичних задач криптографії. Зазначено, що найбільш відомий та поширений криптографічний алгоритм з відкритим ключем RSA базується на низці задач елементарної теорії чисел, що можуть бути розв'язані за допомогою стандартних засобів системи Maple. В цій роботі розглянуто вказані стандартні команди з демонстрацією прийомів їх застосування на спеціально розроблених прикладах. Розглянуто команди для розв'язання задач за такими розділами, як подільність цілих чисел, прості числа; найважливіші функції в теорії чисел: функції виділення цілої та дробової частин числа та мультиплікативні функції; конгруенції та системи конгруенцій першого порядку, квадратичні лишки. Наведено простий та ефективний алгоритм і програма визначення за допомогою стандартних команд Maple простих чисел Мерсенна. Вказаний алгоритм базується на необхідній умові простоти чисел Мерсенна. Продемонстровано роботу авторських навчальних Maple-тренажерів обчислення: за розширеним алгоритмом Евкліда; функції Ейлера; символу Лежандра; символу Якобі. Роботу навчального тренажера з обчислення функції Ейлера продемонстровано під час обчислення відповідного значення для простого числа, складеного числа, що є добутком двох простих, складеного числа, що є натуральним степенем простого числа, а також складених натуральних чисел довільної структури. За допомогою фрагментів програмного коду, що можуть бути покладені в основу розробки навчальних тренажерів продемонстровано визначення повної системи найменших невід'ємних лишків; повної системи абсолютно найменших та зведеної системи лишків за простим та складеним модулями.

Ключові слова: математичні задачі криптографії, теорія чисел, Maple, навчальні Maple-тренажери, алгоритм Евкліда, функція Ейлера, конгруенції, квадратичні лишки, символ Якобі.

Abstract. On the basis of the analysis of literary sources, a conclusion was made about the relevance of using the environment of the Maple computer mathematics system for the purpose of creating software for conducting scientific research and creating educational and methodological materials for solving typical mathematical problems of cryptography. It is noted that the most famous and widespread cryptographic algorithm with a public key RSA is based on a number of problems of elementary number theory that can be solved using standard tools of the Maple system. This work examines the specified standard commands with a demonstration of their application techniques on specially developed examples. The commands for solving problems in such sections as divisibility of whole numbers, prime numbers are considered; the most important functions in number theory: functions for selection of integer and fractional parts of a number and multiplicative functions; congruences and systems of congruences of the first order, quadratic remainders. A simple and effective algorithm and program for determining prime Mersenne numbers based on standard Maple commands is given. This algorithm is based on the necessary condition of simplicity of Mersenne numbers. The work of the author's educational Maple calculation simulators is demonstrated: according to the extended Euclid algorithm; Euler functions; symbol of Legendre; Jacobi symbol. The operation of the Euler function training simulator is demonstrated when calculating the corresponding value for a prime number, a composite number that is the product of two primes, a composite number that is a natural power of a prime number, as well as composite natural numbers of arbitrary structure. With the help of fragments of the program code, which can be used as a basis for the development of training simulators, the determination of the complete system of the smallest integral residues is demonstrated; of the complete system of the absolute smallest and the reduced system of remainders by simple and composite modules.

Key words: mathematical problems of cryptography, number theory, Maple, educational Maple simulators, Euclid's algorithm, Euler's function, congruences, quadratic remainders, Jacobi symbol.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-105-118>.

Вступ

Світова наукова спільнота постійно працює в напрямі пошуку, формування та вдосконалення принципово нових технологій навчання, що базуються на використанні інформаційних технологій [1, 2, 3, 4, 5, 6]. Розв'язання математичних задач криптографії, що в значній мірі базуються, зокрема, на задачах елементарної теорії чисел, звичайно передбачають проведення громіздких рутинних обчислень [1, 2, 3, 4, 6]. Такі обчислення можна проводити з використанням багатьох сучасних середовищ. Одним з найкращих представників таких середовищ є системи комп'ютерної математики (СКМ), зокрема, Maple - система, що спрямована на автоматизацію символічних та числових обчислень, аналіз і візуалізацію даних та навчальної інформації [7, 8, 9]. Ця система надає можливість швидко оволодіти основами методів для вирішення математичних задач та широко використовується в академічних та наукових галузях. Пошуки ефективних шляхів та прийомів застосування СКМ Maple під час розв'язання задач теорії чисел, лінійної й абстрактної алгебри, математичного аналізу, теорії ймовірностей та криптографічних перетворень розпочалися декілька десятків років тому [10, 11, 12, 13, 14]. З часом спостерігається посилення інтенсивності подібних пошуків [15, 16, 17, 18].

До суттєвих переваг таких систем можна також віднести простоту їх освоєння, у порівнянні, наприклад, з освоєнням середовища мови Python.

Актуальність

В той же час, серед численних публікацій, що присвячені описанню доволі ефективних прийомів використання СКМ Maple до розв'язання широкого кола математичних задач, подібних праць, в яких розглядаються задачі елементарної теорії чисел, лінійної алгебри, теорії ймовірностей, що безпосередньо пов'язані із математичними задачами криптографії, залишається недостатньо. До найбільш вдалих та ґрунтовних праць в цій галузі можна віднести працю [15]. Однак в цій праці увага акцентується на застосуванні стандартних команд СКМ Maple та обмежуються тільки розглядом задач елементарної теорії чисел. Створення навчальних Maple-тренажерів в цій праці не розглядається взагалі. На наш погляд, створення та використання вказаних тренажерів є одним з найефективніших напрямків впровадження СКМ в навчальному процесі здобувачів вищої освіти галузі знань 12 - Інформаційні технології, зокрема, спеціальності 125 - Кібербезпека.

Мета та задачі дослідження

Метою даної статті є розгляд основних прийомів розв'язання з використанням СКМ Maple широкого кола задач теорії чисел, лінійної алгебри, теорії ймовірностей, що мають криптографічні застосування.

Для досягнення поставленої мети вирішувались такі задачі:

- визначити основні розділи та задачі теорії чисел, що мають бути розглянуті в матеріалах досліджень, а також найбільш наочну форму подачу цих матеріалів.
- розробити компактні приклади застосування стандартних команд Maple, що відображують, як математичну сутність відповідних задач, так і особливості синтаксису програмного середовища.
- продемонструвати на окремих характерних прикладах роботу навчальних Maple-тренажерів розв'язування окремих типових задач елементарної теорії чисел.

Виклад основного матеріалу

Частина команд для розв'язання задач елементарної теорії чисел знаходяться в ядрі системи Maple. Такі команди є доступними зразу після запуску цієї системи. Інша частина команд знаходиться в пакеті *numtheory* і стає доступною тільки після підключення. Всі команди цього пакету можна підключити за допомогою командного рядка

```
with (numtheory) ;
```

```
[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral_basis, invfrac, invphi, issqrfree, jacobi, kronecker, lambda, legendre, mcombine, mersenne, migcdex, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, phi, pi, pprimroot, primroot, quadres, rootsunity, safeprime, sigma, sq2factor, sum2sq, tau, thue];
```

Якщо в поточному сеансі роботи в середовищі Maple планується використовувати тільки окремі команди пакету, їх можна підключити за допомогою такого командного рядка

```
with (numtheory, divisors, factorset, fermat, jacobi, legendre, phi, pi, sigma) ;  
[divisors, factorset, fermat, jacobi, legendre,  $\phi$ ,  $\pi$ ,  $\sigma$ ]
```

В той же час, доступ до будь-якої команди цього пакету може бути отриманий за допомогою синтаксису

```
numtheory [phi] (35) ;
```

24,

що може бути зручним, якщо не планується застосування інших команд пакету і не планується повторного використання цієї команди.

Надалі, звертаючись до команд цього пакету будемо саме за таким синтаксисом, щоб підкреслити належність команди до вказаного пакету.

Аналіз форм подачі матеріалів досліджень, подібних до цієї роботи надає можливість припустити, що найбільш наочним є використання таблиць з декількома колонками під час описання широкого кола стандартних команд та однієї колонки - для описання прикладів розв'язування деяких відомих математичних задач з криптографічним застосуванням, також під час демонстрації роботи Maple-тренажерів.

Команди, що будемо описувати, групуватимемо за різними тематичними розділами, безпосереднє пов'язаними з криптографічним алгоритмом з відкритим ключем RSA – найбільш відомим та широко-зповсюдженим в різних додатках для шифрування та цифрового підпису.

Ці розділи визначені на основі низки праць наукового та навчально-методичного характеру [1, 2, 4, 6, 17, 18, 19, 20, 21].

1.1. Подільність цілих чисел. Прості числа.

Команда або оператор	Стисле описання	Приклади застосування*
irem(m, n) irem(m, n, 'q') ; iquo(m, n)	Якщо m і n є натуральними числами, тоді <i>irem</i> повертає таке ціле число r (<i>iquo</i> повертає таке ціле число q), що $m = n \cdot q + r$,	m:=23:n:=4: r:=irem(m, n, 'q'); m=` `(q)*n+` `(rhs(%)); r=3

<p><code>%</code> <code>rhs</code></p>	<p>$0 \leq r < n$; Якщо присутній третій аргумент, йому буде присвоєно значення частки (остачі). Посилання на останнє обчислене значення права частина рівняння</p>	$23 = 4 (5) + (3)$ <pre>m:=7:n:=16: r:=irem(m,n,'q'); m=` `(q)*n+` `(rhs(%)); r=7 7=16(0)+(7) m:=33:n:=3: r:=irem(m,n,'q'); m=` `(q)*n+` `(rhs(%)); r=0 33=3(11)+(0) m:=23:n:=4: iquo(m,n); 5</pre>
<p><code>isprime(n)</code> <code>nextprime(n)</code>, <code>prevprime(n)</code> <code>ithprime(n)</code></p>	<p>Здійснює перевірку цілого додатного числа на простоту Знаходження найближчого більшого (меншого) простого числа Знаходження простого числа з порядковим номером n;</p>	<pre>isprime(7),isprime(15); true,false prevprime(7),nextprime(7); 5,11 ithprime(7); 17</pre>
<p><code>ifactor(n)</code></p>	<p>Канонічний розклад числа. Канонічним розкладанням натурального числа на прості множники називають таке його розкладання, коли множники записуються в порядку зростання</p>	<pre>n:=728:n=ifactor(n); 728=(2)^3(7)(13) n:=101:n=ifactor(n); 101=(101) n:=18!: `(18)!=ifactor(n); (18)!= (2)^16(3)^8(5)^3(7)^2(11)(13)(17) n:=3195007177:n=ifactor(n); 3195007177=(58217)(54881)</pre>
<p><code>factorset(n)</code></p>	<p>обчислює множину простих дільників числа n</p>	<pre>numtheory[factorset](18!); {2,3,5,7,11,13,17}</pre>
<p><code>divisors(n)</code></p>	<p>обчислює множину всіх додатних дільників числа n:</p>	<pre>numtheory[divisors](128); `+`(%[]); {1,2,4,8,16,32,64,128} 255</pre>
<p><code>igcd</code> <code>ilcm</code></p>	<p>знаходять найбільший спільний дільник (найменше спільне кратне) двох або більше цілих чисел;</p>	<pre>[[15,35],[5,11],[15,35,45]]; igcd,map(z->igcd(z[]),%); ilcm,map(z->ilcm(z[]),%%); [[15,35],[5,11],[15,35,45]] igcd,[5,1,5] ilcm,[105,55,315]</pre>
<p><code>igcdex(m,n,'s','t')</code>;</p>	<p>роширений алгоритм Евкліда: обчислює такі цілі числа g, s, t, що, $s m + t n = g, g = (m, n)$;</p>	<pre>m:=11:n:=21: igcdex(m,n,'u','v'): ` `(u)*m+` `(v)*n=%; 11(2)+21(-1)=1</pre>
<p style="text-align: center;">НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР з обчислень за розширеним алгоритмом Евкліда [6]</p> <pre>My_Euclid:=proc(a1,b1) local aa,bb,ri_1,ri,ri1,qi,xi_1,xi,xil,yi_1,yi,yil,i,i_1; if type(a1,posint) and type(b1,posint) then if a1>=b1 then aa:=a1;bb:=b1;ri_1:=a1;ri:=b1 else aa:=b1;bb:=a1;ri_1:=b1;ri:=a1 end if; print(a=ri_1,b=ri); qi:=floor(ri_1/ri); xi_1:=1;xi:=0;yi_1:=0;yi:=1;</pre>		

```

i_1:=0:
print('r'[i_1]=ri_1,'x'[i_1]=xi_1,'y'[i_1]=yi_1,[ri_1=xi_1*` (aa)+y
i_1*` (bb)]);
for i while ri1<>0 do
  qi:=floor(ri_1/ri);#print('qi'=qi);
  ri1:=ri_1-qi*ri;
  xi1:=xi_1-qi*xi;
  yi1:=yi_1-qi*yi;

print('q'[i]=qi,'r'[i]=ri,'x'[i]=xi,'y'[i]=yi,[ri=xi*` (aa)+yi*`
(bb)]);
  ri_1:=ri;ri:=ri1;xi_1:=xi;xi:=xi1;yi_1:=yi;yi:=yi1;
end do
else
  'procname( args )'
end if;
print(gcd=ri_1,xi_1*` (aa)+yi_1*` (bb)=ri_1);
xi_1,yi_1
end proc:
My_Euclid(26, 21):

```

$$\begin{aligned}
 & a = 26, b = 21 \\
 & 'r'_0 = 26, 'x'_0 = 1, 'y'_0 = 0, [26 = (26)] \\
 & 'q'_1 = 1, 'r'_1 = 21, 'x'_1 = 0, 'y'_1 = 1, [21 = (21)] \\
 & 'q'_2 = 4, 'r'_2 = 5, 'x'_2 = 1, 'y'_2 = -1, [5 = (26) - (21)] \\
 & 'q'_3 = 5, 'r'_3 = 1, 'x'_3 = -4, 'y'_3 = 5, [1 = -4 (26) + 5 (21)] \\
 & \text{gcd} = 1, -4 (26) + 5 (21) = 1 \\
 & \quad -4, 5
 \end{aligned}$$

```
My_Euclid(11,21):
```

$$\begin{aligned}
 & a = 21, b = 11 \\
 & 'r'_0 = 21, 'x'_0 = 1, 'y'_0 = 0, [21 = (21)] \\
 & 'q'_1 = 1, 'r'_1 = 11, 'x'_1 = 0, 'y'_1 = 1, [11 = (11)] \\
 & 'q'_2 = 1, 'r'_2 = 10, 'x'_2 = 1, 'y'_2 = -1, [10 = (21) - (11)] \\
 & 'q'_3 = 10, 'r'_3 = 1, 'x'_3 = -1, 'y'_3 = 2, [1 = -(21) + 2 (11)] \\
 & \text{gcd} = 1, -(21) + 2 (11) = 1 \\
 & \quad -1, 2
 \end{aligned}$$

```
My_Euclid(70, 98):
```

$$\begin{aligned}
 & a = 98, b = 70 \\
 & 'r'_0 = 98, 'x'_0 = 1, 'y'_0 = 0, [98 = (98)] \\
 & 'q'_1 = 1, 'r'_1 = 70, 'x'_1 = 0, 'y'_1 = 1, [70 = (70)] \\
 & 'q'_2 = 2, 'r'_2 = 28, 'x'_2 = 1, 'y'_2 = -1, [28 = (98) - (70)] \\
 & 'q'_3 = 2, 'r'_3 = 14, 'x'_3 = -2, 'y'_3 = 3, [14 = -2 (98) + 3 (70)] \\
 & \text{gcd} = 14, -2 (98) + 3 (70) = 14
 \end{aligned}$$

ЧИСЛА МЕРСЕННА

Числа Мерсенна мають вигляд $M_n = 2^n - 1$. Числа саме такого виду є найбільшими серед відомих простих чисел. Складемо програму для визначення всіх простих чисел Мерсенна серед першої тисячі натуральних чисел:

```

for n from 1 to 1000 do
  if isprime(2^n-1) then
    print(M[n]=2^n-1);
  end if;
end do;

```

$$M_2 = 3$$

$$M_3 = 7$$

$$\begin{aligned}
 M_5 &= 31 \\
 M_7 &= 127 \\
 M_{13} &= 8191 \\
 M_{17} &= 131071 \\
 M_{19} &= 524287 \\
 M_{31} &= 2147483647 \\
 M_{61} &= 2305843009213693951 \\
 M_{89} &= 618970019642690137449562111 \\
 M_{107} &= 16225927682921336339157801028812 \\
 M_{127} &= 17014118346046923173168730371588410572
 \end{aligned}$$

$$\begin{aligned}
 M_{521} &= \\
 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559 \\
 640661454554977296311391480858037121987999716643812574028291115057151
 \end{aligned}$$

$$\begin{aligned}
 M_{607} &= \\
 5311379928167670986895882065524686273295931177270319231994441382004035598608522427391625 \\
 0226522928566888932948624650101534657933765270723940951997876658735194383127083539321903 \\
 1728127
 \end{aligned}$$

Легко довести, що числа Мерсенна $M_k = 2^k - 1$, є складеними для будь-яких додатних складених чисел k - парних або непарних. Іншими словами простота числа k є необхідною умовою (проте, недостатньою) простоти числа Мерсенна $M_k = 2^k - 1$. В зв'язку з цим наведений простий алгоритм виявлення засобами СКМ Maple простих чисел Мерсенна серед натуральних чисел певного проміжку легко удосконалити шляхом введення двох додаткових умов. Перша умова – пропускати всі числа Мерсенна, що відповідають парним значенням номера k . Друга – для всіх непарних значень k перевіряти спочатку простоту самого числа k , і тільки в разі позитивної відповіді переходити до перевірки на простоту відповідного числа Мерсенна. Легко видно, що із зростанням натуральних чисел частота зустрічаємості серед них простих чисел Мерсенна різко знижується. Крім того із зростанням номера числа Мерсенна їх величина також різко зростає, що добре видно із демонстраційного графіка на рис. 1. Наприклад, значно простіше, тобто значно швидше, можна здійснити перевірку на простоту числа $k = 527$, ніж здійснити перевірку відповідного числа Мерсенна, десяткове представлення якого містить 159 цифр! Оскільки число $k = 527$ є складеним, відпадає необхідність перевірки відпові-

дного числа Мерсена. Наведемо удосконалену програму та приклад її роботи ($u(k) = \frac{k}{2^k - 1}$):

```

for n in [2, 2*k+1 $ k=1..500] do
  if isprime(n) then
    if isprime(2^n-1) then
      print(M[n]=2^n-1, u(n)=evalf(n/(2^n-1)))
    end if
  end if
end do:

```

$$\begin{aligned}
 M_2 &= 3, u(2) = 0.6666666667 \\
 M_3 &= 7, u(3) = 0.4285714286 \\
 M_5 &= 31, u(5) = 0.1612903226 \\
 M_7 &= 127, u(7) = 0.05511811024 \\
 M_{13} &= 8191, u(13) = 0.001587107801 \\
 M_{17} &= 131071, u(17) = 0.0001297006966 \\
 M_{19} &= 524287, u(19) = 0.00003623969315 \\
 M_{31} &= 2147483647, u(31) = 0.1443549991 \cdot 10^{-7} \\
 M_{61} &= 2305843009213693951, u(61) = 0.2645453301 \cdot 10^{-16} \\
 M_{89} &= 618970019642690137449562111, u(89) = 0.1437872549 \cdot 10^{-24} \\
 M_{107} &= 162259276829213363391578010288127, u(107) = 0.6594384130 \cdot 10^{-30}
 \end{aligned}$$

$$M_{127} = 170141183460469231731687303715884105727, u(127) = 0.7464389128 \cdot 10^{-36}$$

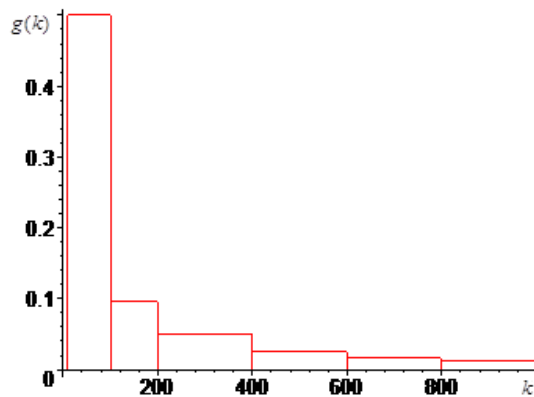


Рисунок 1 – Залежність відношення довжини номера числа Мерсена до довжини його значення

$$g(k) = \frac{\text{length}(k)}{\text{length}(2^k - 1)}$$

(length – кількість цифр в десятковому представленні числа) для різних значень номерів.

1.2. Найважливіші функції в теорії чисел: функції виділення цілої та дробової частин числа та мультиплікативні функції.

<p>round (n) floor (n) ceil (n) trunc (n) - frac (n) - evalf (x) map</p>	<p>округлює число <i>n</i> до найближчого цілого; округлює число <i>n</i> до найбільшого цілого числа, що менше або дорівнює цьому числу; округлює число <i>n</i> до найменшого цілого числа, що більше або дорівнює цьому числу; округлює дійсне число <i>n</i> до найближчого цілого в напрямку до 0. Стандартне математичне позначення: $[n]$. знаходить дробову частину числа <i>n</i>. Стандартне математичне позначення $\{n\}=n-[n]$: подає дійсне число <i>x</i> у формі числа з плаваючою точкою або у вигляді числа зі знаками після коми; застосовує процедуру до кожного елемента об'єкта</p>	<pre>L:=evalf([exp(1),3.9,-1.9,Pi,15]); `round(L)` ,map(t->round(t),L); `floor(L)` ,map(t->floor(t),L); `ceil(L)` *`-->`*map(t->ceil(t),L); `trunc(L)` ,map(t->trunc(t),L); `frac(L)` *`-->`*map(t->frac(t),L); L = [2.718281828 3.9, -1.9, 3.141592654 15.] round(L), [3, 4, -2, 3, 15] floor(L), [2, 3, -2, 3, 15] ceil(L) --> [3, 4, -1, 4, 15] trunc(L), [2, 3, -1, 3, 15] frac(L) --> [0.718281828 0.9, -0.9, 0.141592654 0.]</pre>
<p>numtheory[phi] (n)</p>	<p>Функція Ейлера для натурального числа <i>n</i>- визначається, як кількість натуральних чисел, що не перевищують <i>n</i> і взаємно прості з ним.</p>	<pre>[8, 11, 21, 25]; map(z->`phi`(z)=numtheory[phi](z),%); [8, 11, 21, 25] [φ(8) = 4, φ(11) = 10, φ(21) = 12, φ(25) = 20]</pre>
<p>tau (n) sigma (n)</p>	<p>обчислює кількість додатніх дільників числа <i>n</i>: обчислює суму додатніх дільників числа <i>n</i>.</p>	<pre>n:=15:numtheory[divisors](n); tau(15)=numtheory[tau](15); sigma(15)=numtheory[sigma](15); {1, 3, 5, 15} τ(15) = 4 σ(15) = 24</pre>

mobius (n)	Функція Мебіуса для натурального безквадратного числа $n > 1$ визначається, як $(-1)^s$, s – кількість простих дільників числа n ; $mobius(1)=1$, в інших випадках $mobius(n)=0$.	<pre>[6, 70, 50]; map(z->`mobi- us`(z)=numtheory[mobius](z),%); [6, 70, 50] [mobius(6) = 1, mobius(70) = -1, mobius(50) = 0]</pre>
lambda (n)	Функція Кармайкла для натурального числа обчислює значення функції Кармайкла, тобто найменшого числа $\lambda(n)$, такого, що $n \mid a^{\lambda(n)} - 1$ за умови $(n,a)=1$.	<pre>[5, 7, 3^3]; map(z->`lamb- da`(ifactor(z))=numtheory[lambda](z),%); map(z->numtheory[phi](z)- numtheory[lambda](z),%%); [5, 7, 27] [lambda(5) = 4, lambda(7) = 6, lambda(3^3) = 18] [0, 0, 0] [35, 3^3*5*11^2]; map(z->`lamb- da`(ifactor(z))=numtheory[lambda](z),%); map(z->numtheory[phi](z)- numtheory[lambda](z),%%); [35, 16335] [lambda(5)(7) = 12, lambda(3^3)(5)(11)^2 = 1980] [12, 5940]</pre>
numtheory[pi] (n)	обчислює кількість простих чисел на відрізку від 1 до n ;	<pre>map(z->numtheory[pi](z), [2, 3, 10, 100]); [1, 2, 4, 25]</pre>
<p style="text-align: center;">НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР з обчислень функції Ейлера [18]</p> <p>My_phi(17); Число $p=17$ є простим, отже значення функції Ейлера обчислюємо за формулою $\phi(p) = p - 1$ $[\phi(17) = (17) - 1] = 16$</p> <p>My_phi(35); Задане число є добутком простих чисел $35 = (5)(7)$ Отже, для обчислення функції Ейлера використовуємо властивість мультиплікативності цієї функції: $[[\phi(5)(7) = \phi(5)\phi(7)] = ((5) - 1)((7) - 1)] = 24$</p> <p>My_phi(27); В канонічній формі задане число має вигляд $27 = (3)^3$ Отже, для обчислення функції Ейлера використовуємо формулу $\phi(p^q) = p^{(q-1)}(p - 1)$ $[\phi(3^3) = (3)^{(3-1)}(3 - (1))] = 18$</p> <p>My_phi(17*19^2*31); В канонічній формі задане число має вигляд $190247 = (17)(19)^2(31)$ Отже, для обчислення функції Ейлера використовуємо найбільш загальну формулу $\phi((17)(19)^2(31)) = (190247) \left(\prod_{k=1}^3 \left(1 - \frac{1}{p_k} \right) \right)$</p>		

$$\left[(190247) \left(\prod_{k=1}^3 \left(1 - \frac{1}{p_k} \right) \right) = (190247) \left(1 - \frac{1}{(17)} \right) \left(1 - \frac{1}{(19)} \right) \left(1 - \frac{1}{(31)} \right) \right] = 164160$$

1.3. Конгруенції

Команда або оператор	Стисле описання	Приклади застосування*
a mod b modp (a, b) mods (a, b)	Здійснює обчислення за модулем цілого числа b : повертає найменший додатний лишок; повертає абсолютно найменший лишок;	19 mod 5; modp (19, 5); mods (19, 5); 4 4 -1
<pre>n:=7: printf(`повна система найменших невід'ємних лишків за модулем 7: `); k \$ k=0..n-1; printf(`повна система абсолютно найменших лишків за модулем 7: `); i:=((-1)^n-1)/2:seq(mods(k,n),k=0..n-1); printf(`зведена система лишків за модулем 7: `); select(x->is(igcd(x,n)=1),[k \$ k=0..n-1])[] повна система найменших невід'ємних лишків за модулем 7: 0, 1, 2, 3, 4, 5, 6 повна система абсолютно найменших лишків за модулем 7: 0, 1, 2, 3, -3, -2, -1 зведена система лишків за модулем 7: 1, 2, 3, 4, 5, 6 n:=12: printf(`повна система найменших невід'ємних лишків за модулем 12: `); k \$ k=0..n-1; printf(`повна система абсолютно найменших лишків за модулем 12: `); i:=((-1)^n-1)/2:seq(mods(k,n),k=0..n-1); printf(`зведена система лишків за модулем 12: `); select(x->is(igcd(x,n)=1),[k \$ k=0..n-1])[] повна система найменших невід'ємних лишків за модулем 12: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 повна система абсолютно найменших лишків за модулем 12: 0, 1, 2, 3, 4, 5, 6, -5, -4, -3, -2, -1 зведена система лишків за модулем 12: 1, 5, 7, 11 printf(`Перевірка належності двох чисел a, b до одного класу лишків за модулем 11: `); n:=11:[[3,36],[1,78],[2,14],[-1,11],[-12,12]]; map(z->z*`-->`*is(z[1]-z[2] mod n=0),%); Перевірка належності двох чисел a, b до одного класу лишків за модулем 11: [[3, 36], [1, 78], [2, 14], [-1, 11], [-12, 12]] [[3, 36] --> true, [1, 78] --> true, [2, 14] --> false, [-1, 11] --> false, [-12, 12] --> false]</pre>	<pre>printf(`Перевірка належності двох чисел a, b до одного класу лишків за модулем 11: `); n:=11:[[3,36],[1,78],[2,14],[-1,11],[-12,12]]; map(z->z*`-->`*is(z[1]-z[2] mod n=0),%); повна система найменших невід'ємних лишків за модулем 12: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 повна система абсолютно найменших лишків за модулем 12: 0, 1, 2, 3, 4, 5, 6, -5, -4, -3, -2, -1 зведена система лишків за модулем 12: 1, 5, 7, 11 printf(`Перевірка належності двох чисел a, b до одного класу лишків за модулем 11: `); n:=11:[[3,36],[1,78],[2,14],[-1,11],[-12,12]]; map(z->z*`-->`*is(z[1]-z[2] mod n=0),%); Перевірка належності двох чисел a, b до одного класу лишків за модулем 11: [[3, 36], [1, 78], [2, 14], [-1, 11], [-12, 12]] [[3, 36] --> true, [1, 78] --> true, [2, 14] --> false, [-1, 11] --> false, [-12, 12] --> false]</pre>	
msolve	Обчислює розв'язок конгруенції з однією змінною або системи конгруенцій з декілька невідомими за модулем n ;	<pre>msolve(5*x=29,18); {x=13} msolve(2*x=29,18); msolve(3*x=15,18); {x=5},{x=11},{x=17} msolve(14*x^3-6*x+36=0,7); {x=6} msolve({3*x-4*y=5,7*x+y=2},17); {y=4,x=7}</pre>
chrem	обчислює розв'язок лінійної системи конгруенцій з однією змінною і різними попарно	<pre>chrem([6,4],[7,17]); chrem([6,4,5],[7,17,6]); 55</pre>

	простими модулями	293
legendre	обчислює символ Лежандра	legendre (184, 347) ; 1 legendre (3, 7) ; -1
НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР обчислення символу Лежандра Символи Лежандра та Якобі використовуються для встановлення числа розв'язків модулярних квадратних рівнянь відповідно за простим та складеним модулем. Приклад. Дослідити, чи має розв'язки конгруенція $x^2 \equiv 184 \pmod{347}$. ► My_Lej (184, 347) ; Число "a" має такий канонічний розклад: $184 = (2)^3 (23)$ Отже, з використанням мультиплікативності символу Лежандра, отримаємо: $\left(\frac{184}{347}\right) = \left(\frac{2}{347}\right)^3 \left(\frac{23}{347}\right)$ Всі співмножники в парних степенях дорівнюють одиниці, отже: $\left(\frac{184}{347}\right) = \left(\frac{2}{347}\right) \left(\frac{23}{347}\right)$ My_Lej (2, 347) ; $\left(\frac{2}{347}\right) = (-1)^{\left(\frac{(347)^2-1}{8}\right)}$ $\left(\frac{2}{347}\right) = -1$ My_Lej (23, 347) ; КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА: для будь-яких простих непарних чисел p і q виконується рівність $\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$ В цьому випадку $\left(\frac{23}{347}\right) = (-1)^{\left(\frac{((23)-1)((347)-1)}{4}\right)} \left(\frac{347}{23}\right)$ Отже $\left(\frac{23}{347}\right) = -\left(\frac{347}{23}\right)$ -My_Lej (347, 23) ; $\left(\frac{347}{23}\right) = \left(\frac{347 \text{ ['mod' (23)]}}{(23)}\right)$ $-\left(\frac{347}{23}\right) = -\left(\frac{2}{23}\right)$ -My_Lej (2, 23) ; $\left(\frac{2}{23}\right) = (-1)^{\left(\frac{(23)^2-1}{8}\right)}$ $-\left(\frac{2}{23}\right) = -1$ `` (184/347) = (-1) * (-1) ; $\left(\frac{184}{347}\right) = 1$ Відповідь: конгруенція $x^2 \equiv 184 \pmod{347}$ має два розв'язки. ◀		
jacobi	обчислює символ Якобі	jacobi (1001, 9907) ; -1
НАВЧАЛЬНИЙ MAPLE-ТРЕНАЖЕР		

обчислення символу Якобі

Приклад. Дослідити, чи має розв'язки конгруенція $x^2 \equiv 1001 \pmod{9907}$.

► **Му_Яас(1001, 9907) ;**

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:

для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{1001}{9907}\right) = (-1)^{\left(\frac{((1001)-1)((9907)-1)}{(4)}\right)} \left(\frac{9907}{1001}\right)$$

Отже

$$\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right)$$

$$\left(\frac{9907}{1001}\right) = \left(\frac{9907 \text{ ['mod' (1001)] }}{(1001)}\right)$$

$$\left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right)$$

Оскільки число 898 - парне, подамо це число у вигляді

$$898 = 2' q$$

$$898 = (2) (449)$$

$$\left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right) \left(\frac{449}{1001}\right)$$

$$\left(\frac{2}{1001}\right) = (-1)^{\left(\frac{(1001)^2-1}{(8)}\right)}, \left(\frac{2}{1001}\right) = 1$$

$$\left(\frac{898}{1001}\right) = \left(\frac{449}{1001}\right)$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:

для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{449}{1001}\right) = (-1)^{\left(\frac{((449)-1)((1001)-1)}{(4)}\right)} \left(\frac{1001}{449}\right)$$

Отже

$$\left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right)$$

$$\left(\frac{1001}{449}\right) = \left(\frac{1001 \text{ ['mod' (449)] }}{(449)}\right)$$

$$\left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right)$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:

для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{103}{449}\right) = (-1)^{\left(\frac{((103)-1)((449)-1)}{(4)}\right)} \left(\frac{449}{103}\right)$$

Отже

$$\begin{aligned} \left(\frac{103}{449}\right) &= \left(\frac{449}{103}\right) \\ \left(\frac{449}{103}\right) &= \left(\frac{449 [\text{'mod'} (103)]}{(103)}\right) \\ \left(\frac{449}{103}\right) &= \left(\frac{37}{103}\right) \end{aligned}$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:

для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{37}{103}\right) = (-1)^{\left(\frac{((37)-1)((103)-1)}{(4)}\right)} \left(\frac{103}{37}\right)$$

Отже

$$\begin{aligned} \left(\frac{37}{103}\right) &= \left(\frac{103}{37}\right) \\ \left(\frac{103}{37}\right) &= \left(\frac{103 [\text{'mod'} (37)]}{(37)}\right) \\ \left(\frac{103}{37}\right) &= \left(\frac{29}{37}\right) \end{aligned}$$

КВАДРАТИЧНИЙ ЗАКОН ВЗАЄМНОСТІ ГАУССА:

для будь-яких непарних натуральних взаємнопростих чисел p і q виконується рівність

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(q-1)(p-1)}{4}\right)} \left(\frac{p}{q}\right)$$

В цьому випадку

$$\left(\frac{29}{37}\right) = (-1)^{\left(\frac{((29)-1)((37)-1)}{(4)}\right)} \left(\frac{37}{29}\right)$$

Отже

$$\begin{aligned} \left(\frac{29}{37}\right) &= \left(\frac{37}{29}\right) \\ \left(\frac{37}{29}\right) &= \left(\frac{37 [\text{'mod'} (29)]}{(29)}\right) \\ \left(\frac{37}{29}\right) &= \left(\frac{8}{29}\right) \end{aligned}$$

Оскільки число 8 - парне, подамо це число у вигляді

$$8 = 2^t q$$

$$8 = (2)^3 (1)$$

$$\begin{aligned} \left(\frac{8}{29}\right) &= \left(\frac{2}{29}\right)^3 \left(\frac{1}{29}\right) \\ \left(\frac{2}{29}\right)^3 &= (-1)^{\binom{(29)^2-1}{(8)}} \left(\frac{2}{29}\right)^3 = -1 \\ \left(\frac{8}{29}\right) &= -\left(\frac{1}{29}\right) \\ \left(\frac{1}{29}\right) &= 1 \\ \left(\frac{1001}{9907}\right) &= -1 \end{aligned}$$

Відповідь: не існує розв'язку конгруенції $x^2 \equiv 1001 \pmod{9907}$. ◀

Висновки

1. Розглянуто прийоми розв'язання за допомогою стандартних команд системи Maple основних задач елементарної теорії чисел, більшість з яких має безпосереднє відношення до криптографічного алгоритму RSA - одного з найпоширеніших асиметричних криптографічних методів, що використовується для шифрування і цифрового підпису.

2. Продемонстровано роботу авторських Maple-тренажерів, що разом з використанням інших прийомів застосування стандартних команд системи Maple до розв'язання математичних задач криптографічного характеру направлено на покращення ефективності, зокрема, наочності, висвітлення сутності розглянутих методів та ідей, покладених в їх основу.

3. Матеріали статті можуть бути використані здобувачами вищої освіти та викладачами ЗВО під час розв'язання типових математичних задач галузі знань 12 – Інформаційні технології. Особливо корисним представлені матеріали можуть виявитися в процесі вивчення дисципліни «Математичні основи криптографії».

Список літератури

- [1] Хорошко В.О., Азаров О.Д., Шелест М.Є., Андреев В.І., Мухачов В.А., Щербина В.П., Яремчук Ю.Є. Комп'ютерна криптографія. Лабораторний практикум. - Київ: НАУ, 2003. - 94 с.
- [2] Гулак Г.М. Основи криптографічного захисту інформації: підручник / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук / – Вінниця : ВНТУ, 2011. – 199 с. (ISBN 978–966–641–430–7).
- [3] Кветний Р.Н. Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ECC та RSA / Р.Н. Кветний, Є.О. Титарчук, А.А. Гуржій // Інформаційні технології та комп'ютерна інженерія. – 2016. – № 3. – С. 38-43.
- [4] Лужецький В. А. Інформаційна безпека : навчальний посібник / В.А.Лужецький, О. П. Войтович, А. В. Дудатьєв –Вінниця : УНІВЕРСУМВінниця, 2009. –240 с. –ISBN 978-966-641-265-53.
- [5] Лужецький В. А. Методи багатоканального керованого хешування для комп'ютерної криптографії /В. А. Лужецький, Ю. В. Баришев // Інформаційні технології та комп'ютерна інженерія. – 2011. – № 1. – С. 66-72.
- [6] Михалевич В. М. Навчальний Maple-тренажер з обчислень за розширеним алгоритмом Евкліда/ В. М. Михалевич, О. І. Тютюнник, О. Корінний // Матеріали Всеукраїнської науково-методичної конференції «Сучасні науково-методичні проблеми математики у вищій школі», 23 – 24 травня 2022 р. – К.: НУХТ, 2022р. – 133 с. – С. 80-83. <https://drive.google.com/file/d/1VlroDm7xDJuf9mjRYoWK2nsRX-cVqaSR/view>.
- [7] Лужецький В. А. Щільність заповнення ряду натуральних чисел членами окремої зворотної послідовності другого порядку/Лужецький В. А., Михалевич В. М., Михалевич О. В., Каплун В. А. // Інформаційні технології та комп'ютерна інженерія. – 2010. – №1(17) – С. 46-51.
- [8] Добрянюк Ю. В. Застосування СКМ Maple для побудови 3D графіків в задачах обчислення об'єму фігур/Добрянюк Ю. В., Михалевич В. М., Коломієць А. А., Козак О. М. // Інформаційні технології та комп'ютерна інженерія. – 2022. – № 2(17) – С. 115-123.
- [9] Mikhalevich V. M. Maximum Accumulated Strain for Linear Two-Link Triangle-Like Deformation Trajectories / Volodymyr Markusovych Mikhalevich, Igor Vasilyevich Abramchuk // International Applied Mechanics. – 2021. – No. 57(6). – P. 720–736, doi.org/10.1007/s10778-022-01121-w.
- [10] Cheung Y. L. Learning number theory with a computer algebra system/ Y. L. Cheungti // International Journal of Mathematical Education in Science and Technology. – 1996/ – 3(27), p. 379-385, doi:10.1080/0020739960270308.

- [11] Klima, R., Sigmon N., Stitzinger T. Applications of abstract algebra with Maple. CRC Press, Boca Raton, FL. 2000. 251 p. ISBN 0-8493-8170-3.
- [12] Baligaand A., Boztas S. Cryptography in the classroom using Maple. In W.Yang, S.Chu, Z.Karian, and G. Fitz-Gerald, editors. Proceedings of the Sixth Asian Technology Conference in Mathematics. – 2001. – p.343–350.
- [13] Михалевич В. М. Excel-VBA-Maple програма генерації задач з дисциплін математичного спрямування / В. М. Михалевич // Інформаційні технології та комп'ютерна інженерія. — 2005. — № 2. — С. 74–83.
- [14] Михалевич В. М. Захист Maple процедур/ В. М. Михалевич, І. В. Димніч, О. В. Михалевич // Інформаційні технології та комп'ютерна інженерія. – 2007. - № 3(10). – С. 159-165.
- [15] Бедратюк Л. П. Використання системи комп'ютерної алгебри Maple в елементарній теорії чисел / Л. П. Бедратюк, Г. І. Бедратюк // Восточно-Европейский журнал передовых технологий. - 2013. - № 6(4). - С. 10-13. - Режим доступу: http://nbuv.gov.ua/UJRN/Vejrpte_2013_6%284%29__3
- [16] Бедратюк Л. П. Використання системи комп'ютерної алгебри Maple в класичних криптосистемах / Л. П. Бедратюк, Г. І. Бедратюк // Вісник Хмельницького національного університету. – 2015. - № 231(6). - С. 148-153.
- [17] Михалевич В. М. Математичні моделі та програмні засоби генерування псевдовипадкових послідовностей для криптографічних застосувань [Електронний ресурс] / В. М. Михалевич, О. І. Тютюнник, Є. С. Дремлюга, К. В. Медведева // І Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії, м. Вінниця. – 2021. – Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/11617/9718>.
- [18] Михалевич В. М. Навчальний Maple-тренажер з обчислення функції Ейлера [Електронний ресурс] / В. М. Михалевич, Д. Б. Рогачевський, Д. Ю. Желнитський, Б. А. Балух // ІІ Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії, м. Вінниця. – 2022. – Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15034/12681>
- [19] Стасюк М. Елементи математичних основ криптографії : навчальний посібник / М. Стасюк / Навчальний посібник. Львів : ЛДУ БЖД, 2021. – 216 с.
- [20] Оглобліна О. І., Сушко Т.С., Шрамко Ю.В. Елементи теорії чисел : навч. посіб. Суми : Сумський державний університет, 2015. – 186 с.
- [21] Математичні методи криптології. Навчальний посібник. [Ел. ресурс] / А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко. – 2021. – . –Режим доступу: <https://duikt.edu.ua/ua/lib/1/category/2132/view/2220>.
- Стаття надійшла до редакції: 27.02.2024

References

- [1] Khoroshko V.O., Azarov O.D., Shelest M.Ie., Andreev V.I., Mukhachov V.A., Shcherbyna V.P., Yaremchuk Yu.Ie. Kompiuterna kryptohrafiia. Laboratorni praktykum. - Kyiv: NAU, 2003. – 94 s.
- [2] Hulak H.M. Osnovy kryptohrafichnoho zakhystu informatsii: pidruchnyk / H.M. Hulak, V.A. Mu-khachov, V.O. Khoroshko, Yu.Ie. Yaremchuk / – Vinnytsia : VNTU, 2011. – 199 s. (ISBN 978–966–641–430–7).
- [3] Kvietyni R.N. Metod ta alhorytm obminu kliuchamy sered hrup korystuvachiv na osnovi asyme-trychnykh shyfriv ECC ta RSA / R.N. Kvietyni, Ye.O. Tytarchuk, A.A. Hurzhii // Informatsiini tekhnolohii ta kompiuterna inzheneriia. – 2016. – № 3. – S. 38-43.
- [4] Luzhetskyi V. A. Informatsiina bezpeka : navchalnyi posibnyk / V.A.Luzhetskyi, O. P. Voitovych, A. V. Dudatiev –Vinnytsia : UNIVERSUMVinnytsia, 2009. –240 s. –ISBN 978-966-641-265-53.
- [5] Luzhetskyi V. A. Metody bahatokanalnoho kerovanoho ksheshuvannia dlia kompiuternoї kryp-tohrafiї /V. A. Luzhetskyi, Yu. V. Baryshev // Informatsiini tekhnolohii ta kompiuterna inzhe-neriia. – 2011. – № 1. – S. 66-72.
- [6] Mykhalevych V. M. Navchalnyi Maple-trenazher z obchyslen za rozshyrenym alhorytmom Ev-klida/ V. M. Mykhalevych, O. I. Tiutiunnyk, O. Korinnyi // Materialy Vseukrainskoi nauko-vo-metodychnoi konferent-sii «Suchasni naukovo-metodychni problemy matematyky u vyshchii shkoli», 23 – 24 travnia 2022 r. – K.: NUKhT, 2022r. – 133 s. – S. 80-83. <https://drive.google.com/file/d/1VlroDm7xDJuf9mjRYoWk2nsRX-cVqaSR/view>
- [7] Luzhetskyi V. A. Shchilnist zapovnennia riadu naturalnykh chysel chlenamy okremoi zvorotnoi posli-dovnosti druhoho poriadku/Luzhetskyi V. A., Mykhalevych V. M., Mykhalevych O. V., Kaplun V. A. // In-formatsiini tekhnolohii ta kompiuterna inzheneriia. – 2010. – №1(17) – S. 46-51.
- [8] Dobraniuk Yu. V. Zastosuvannia SKM Maple dlia pobudovy 3D hrafiiv v zadakh obchyslennia obiemu fihur/Dobraniuk Yu. V., Mykhalevych V. M., Kolomiets A. A., Kozak O. M. // Informatsiini tekhnolohii ta kompiuterna inzheneriia. – 2022. – № 2(17) – S. 115-123.

- [9] Mikhalevich V. M. Maximum Accumulated Strain for Linear Two-Link Triangle-Like Deformation Trajectories / Volodymyr Markusovych Mikhalevich, Igor Vasilyevich Abramchuk // International Applied Mechanics. – 2021. – No. 57(6). – P. 720–736, doi.org/10.1007/s10778-022-01121-w.
- [10] Cheung Y. L. Learning number theory with a computer algebra system/ Y. L. Cheungti // International Journal of Mathematical Education in Science and Technology. – 1996/ – 3(27), p. 379-385, doi:10.1080/0020739960270308.
- [11] Klima, R., Sigmon N., Stitzinger T. Applications of abstract algebra with Maple. CRC Press, Boca Raton, FL. 2000. 251 p. ISBN 0-8493-8170-3.
- [12] Baligaand A., Boztas S. Cryptography in the classroom using Maple. In W.Yang, S.Chu, Z.Karian, and G. Fitz-Gerald, editors. Proceedings of the Sixth Asian Technology Conference in Mathematics. – 2001. – p.343–350.
- [13] Mykhalevych V. M. Excel-VBA-Maple prohrama heneratsii zadach z dystsyplin matematychnoho spriamuvannia / V. M. Mykhalevych // Informatsiini tekhnolohii ta kompiuterna inzheneriia. — 2005. — № 2. — S. 74–83.
- [14] Mykhalevych V. M. Zakhyst Maple protsedur/ V. M. Mykhalevych, I. V. Dymnich, O. V. Mykhalevych // Infor-matsiini tekhnolohii ta kompiuterna inzheneriia. – 2007. - № 3(10). – S. 159-165.
- [15] Bedratiuk L. P. Vykorystannia systemy kompiuternoї alhebrы Maple v elementarnii teorii chysel / L. P. Bedratiuk, H. I. Bedratiuk // Vostochno-Evropeyskyi zhurnal peredovykh tekhnolohyi. - 2013. - № 6(4). - S. 10-13. - Режим доступу: http://nbuv.gov.ua/UJRN/Vejpte_2013_6%284%29_3
- [16] Bedratiuk L. P. Vykorystannia systemy kompiuternoї alhebrы Maple v klasychnykh kryptosystemakh / L. P. Bedratiuk, H. I. Bedratiuk // Visnyk Khmelnytskoho natsionalnogo universytetu. – 2015. - № 231(6). - S. 148-153.
- [17] Mykhalevych V. M. Matematychni modeli ta prohramni zasoby heneruvannia psevdovypadkovykh poslido-vnosteї dlia kryptohrafichnykh zastosovan [Elektronnyi resurs] / V. M. Mykhalevych, O. I. Tiutiunyk, Ye. S. Dremluha, K. V. Medvedieva // L Naukovo-tekhnichna konferentsiia fakultetu informatsiinykh te-khnolohii ta kompiuternoї inzhenerii, m. Vinnytsia. – 2021. – Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/11617/9718>.
- [18] Mykhalevych V. M. Navchalnyi Maple-trenazher z obchyslennia funktsii Eilera [Elektronnyi resurs] / V. M. Mykhalevych, D. B. Rohachevskyi, D. Yu. Zhelnytskyi, B. A. Balukh // LI Naukovo-tekhnichna konferentsiia fakultetu informatsiinykh tekhnolohii ta kompiuternoї inzhenerii, m. Vinnytsia. – 2022. – Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15034/12681>
- [19] Stasiuk M. Elementy matematychnykh osnov kryptohrafii : navchalnyi posibnyk / M. Stasiuk / Navcha-lnyi posibnyk. Lviv : LDU BZhD, 2021. – 216 s.
- [20] Ohloblina O. I., Sushko T.S., Shramko Yu.V. Elementy teorii chysel : navch. posib. Sumy : Sumskyi derzhavnyi universytet, 2015. – 186 s.
- [21] Matematychni metody kryptolohii. Navchalnyi posibnyk. [El. resurs] / A.D. Kozhukhivskyi, I.D. Horbenko, H.I. Haidur, O.A. Kozhukhivska, V.V. Marchenko. – 2021. – . –Rezhym dostupu: <https://duikt.edu.ua/ua/lib/1/category/2132/view/2220>.

Відомості про авторів

Михалеви́ч Володи́мир Маркусо́вич – д.т.н., професор, завідувач кафедри вищої математики Вінницького національно-го технічного університету, м. Вінниця

Майданеви́ч Леони́д Олекса́ндрови́ч – к. філос. н., асистент кафедри захисту інформації Вінницького національно-го технічного університету, м. Вінниця

Mykhalevych Volodymyr — D.Sc. Professor, head of the Chair for Higher Mathematics, Vinnytsia National Technical University

Maidanevych Leonid – Cand. Sc., assistant of the Department of Information Protection, Vinnytsia National Technical University

V. M. Mykhalevych, L. O. Maidanevych

USE OF THE MAPLE SYSTEM IN MATHEMATICAL PROBLEMS OF CRYPTOGRAPHY. PART 1. ELEMENTARY THEORY OF NUMBERS

Vinnytsia National Technical University, Vinnytsia

УДК 681.3:621.74:004.8:004.94

О. В. Бродовий¹, В. С. Дорошенко², О. Б. Янченко³

3D-ПРОЕКТУВАННЯ ПОРИСТИХ ЛИВАРНИХ МОДЕЛЕЙ В ПРОГРАМІ RHINOCEROS 8

¹Міжнародний ліцей «Михаїл», Київ²Фізико-технологічний інститут металів та сплавів НАН України, Київ³Вінницький національний технічний університет, Вінниця

Анотація. Впровадження в ливарне виробництво 3D-друку дозволяє з цифрових креслень ливарних моделей виготовляти металеві виливки нерідко зі складною геометрією, які було б складно або неможливо виготовити іншими методами. Особливо 3D-друк вигідний для лиття металу за моделями, що газифікуються (ЛГМ), в якому застосовують разові пінополімерні моделі, які випаровуються в піщаній формі від тепла металу, що заливається в цю форму. При виготовленні і застосуванні для ЛГМ-процесу легкових друкованих моделей, що за об'ємною вагою та газотвірністю приближаються до типових моделей з пінополістиролу, методи конструювання пористих вентильованих моделей та оптимізації процесу газифікації друкованих матеріалів запропоновано реалізувати за допомогою нових алгоритмів проектування легкових конструкцій, які інтегровані у діюче програмне забезпечення для тривимірного моделювання, зокрема у програму Rhinoceros. В роботі досліджено і випробувано недавно створений компанією Spherene Inc. алгоритм проектування 3D-друкованих конструкцій стосовно друкування ливарних моделей низької об'ємної ваги, призначених для ЛГМ-процесу. Цей алгоритм є прикладом новаторського впровадження в діючу програму тривимірного моделювання досягнень прикладної математики в галузі теорії тривимірних періодичних мінімальних поверхонь. Виконані нами перші приклади цифрового моделювання макропористих ливарних моделей для їх друку підтвердили доступність використання алгоритму від компанії Spherene Inc. і гармонійного включення пор чи порожнин сфероподібної конфігурації (які компанія називає «spherenes») в їх конструкцію як з можливістю підтримання їх достатньої міцності при мінімальній масі моделей, так і для друкування відкритих (трансляційних) пор заданої орієнтації для суцільної вентиляції і відкачування газів вакуумом ливарної форми.

Ключові слова: 3D-технології, 3D-друк, програмне забезпечення, ливарна модель, газифікація моделі, spherenes, ЛГМ.

Abstract. The introduction of 3D printing into foundry production makes it possible to produce metal castings, often with complex geometry, from digital drawings of foundry patterns, which would be difficult or impossible to produce by other methods. 3D printing is especially beneficial for metal casting by gasifying patterns (Lost Foam Casting, LFC process), which uses disposable foam polymer patterns that evaporate in a sand mold from the heat of the metal poured into the mold. In the manufacture and application of lightweight printed models for the LFC process, which in terms of volume weight and gas permeability are close to typical models made of polystyrene foam, it is proposed to implement the methods of constructing porous ventilated models and optimizing the process of gasification of printed materials with the help of new algorithms for the design of lightweight structures. These algorithms are integrated into existing 3D modeling software, including Rhinoceros. In the work, the recently created Spherene Inc. company was researched and tested. an algorithm for designing 3D-printed structures in relation to printing low-volume foundry patterns intended for the LFC process. This algorithm is an example of innovative introduction into the current program of 3D modeling of the achievements of applied mathematics in the field of the theory of three-dimensional periodic minimal surfaces. Our first examples of digital modeling of macro-porous foundry patterns for their printing confirmed the availability of using the algorithm from Spherene Inc. and the harmonious inclusion of pores or cavities of a sphere-derived configuration (which the company calls "spherenes") in their design, both with the possibility of maintaining their sufficient strength with a minimum mass of patterns, and for printing open (translational) pores of a given orientation for continuous ventilation and pumping out gases by vacuum of the foundry molds.

Keywords: 3D technologies, 3D printing, software, foundry pattern, pattern gasification, spherenes, Lost Foam Casting.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-119-126>.

Вступ

Цифровізація та автоматизація сьогодні стали вже не просто основою конкурентної переваги при виробництві товарів (робіт, послуг), у багатьох сферах вони сприймаються як необхідна умова організації виробничих процесів [1]. Зокрема, впровадження в ливарне виробництво 3D-друку (адитивного виробництва), як однієї з галузей цифровізації, дозволяє з цифрових креслень ливарних моделей виготовляти металеві виливки нерідко зі складною геометрією, які було б складно або неможливо виготовити іншими методами. Особливо 3D-друк вигідний для лиття металу за моделями, що газифікуються (ЛГМ-процес, Lost Foam Casting), в якому застосовують разові піно-полімерні (з пінополістиролу, ППС) моделі, які випаровуються в піщаній формі від тепла металу, що заливається в цю форму [2].

Автоматичний друк таких моделей покращить ефективність та якість особливо дрібносерійного, ремонтного та індивідуалізованого виробництва, підтримає конкурентоспроможність підприємств в сучасному ринковому середовищі. Взагалі, 3D-друк, як важливий елемент цифровізації виробництва, що дозволяє без паперових креслень з цифрової моделі за комп'ютерними програмами автоматично виготовляти полімерні моделі, відповідає концепції цифро-фізичного перетворення (з цифрового файлу – у матеріальну конструкцію), що названо терміном: digital-to-physical conversion [3].

Актуальність

Важливою перевагою 3D-технологій при ЛГМ являється можливість змінювати як конфігурацію ливарної металопродукції, так і конструкцію ливарних моделей шляхом внесення змін в цифрове креслення на етапі модельного виробництва без наступного переформатування решти складових діючого ливарного процесу. Проте, розкриття потенціалу впровадження 3D-друку на даному етапі знаходиться лише на початковому рівні. Виготовлення легковагих друкованих моделей, що за об'ємною вагою та газотвірністю приближаються до типових моделей з ППС поки є непростою задачею [2]. Тому розробка нових методів конструювання пористих моделей, придатних для друку, з удосконаленням процесу газифікації друкованих матеріалів та створенням нових алгоритмів проєктування легковагих конструкцій в складі діючого програмного забезпечення для тривимірного моделювання є актуальною темою досліджень. Зауважимо, що ЛГМ-процес не припиняє свого поширення в ливарництві, досягаючи в світовому вимірі, за оцінками експертів, до 4 % всього об'єму литва, що складає близько 4 млн тонн.

Мета

Мета статті полягає в дослідженні і опробуванні недавно створеного компанією Spherene Inc. (Швейцарія, <https://spherene.ch>) алгоритму проєктування 3D-друкованих виробів для ливарних моделей низької об'ємної ваги, придатних для ЛГМ-процесу. Цей алгоритм є прикладом новаторського впровадження досягнень прикладної математики в діючу програму тривимірного моделювання.

Критика способів 3D-друку для виробництва металопродукції і постановка задачі

Відомі способи 3D-друку тривимірних виробів із металу та тугоплавких матеріалів мають ті недоліки, що включають застосування високої вартості енергоємне обладнання. Високотемпературні плавлення чи спікання металовиробів у цих способах потребують значних витрат енергії та, як правило, захисної атмосфери для камери друку, а діючі стандарти контролю якості металопродукції (щодо відповідності марки металу) не розповсюджуються на друковані матеріали. Все це приблизно на порядок збільшує собівартість друку металовиробів порівняно з відпрацьованими ливарними способами [2].

Значно простішим напрямом впровадження 3D-технологій в ливарне виробництво є друкування для ЛГМ-процесу полімерних ливарних моделей, як разової оснастки. Такі друковані ливарні моделі призначені для розміщення (формування) в піску ливарної форми і газифікації їх при заливанні такої форми металом. Оскільки вилівок утворюється після випарування моделі, то контроль якості затверділого вилівка та відповідність марки його металу не відрізняється від традиційно застосовуваних і унормованих діючими стандартами операцій в ливарних цехах. Однак, бурхливий розвиток 3D-друку ще не настільки поширився в ливарні процеси, що може конкурувати з традиційними технологіями, наприклад щодо друку моделей, аналогічних за низькою густиною матеріалу ППС. Тому нові удосконалення 3D-друку і його програмного забезпечення є поточною проблемою в плані взаємної адаптації з діючим виробництвом, зокрема щодо оптимізації конструкторських рішень на основі математичних методів. Звідси, задача покращення якості тривимірних виробів на етапі проєктування, зменшення витрат та часу, необхідних для їх створення, і забезпечення високого рівня їх конкурентоспроможності полягала в дослідженні геометричних та топологічних принципів і алгоритмів для пошуку оптимальної конфігурації матеріалу в межах конструкції ливарних моделей з урахуванням функціональних вимог та обмежень.

Приклади розв'язання задачі на основі застосування нового алгоритму програмування

В процесі аналізу новітньої інформації нас зацікавив алгоритм, розроблений компанією Spherene Inc., який створює адаптивні поверхні (для) мінімальної щільності (Adaptive Density Minimal Surfaces, ADMS) як самопідтримуючу стратегію заповнення, яку можна використовувати для зменшення маси та керування властивостями матеріалу в 3D-друкованих деталях [4].

Тривимірні періодичні мінімальні поверхні (Triply Periodic Minimal Surfaces, TPMS) [5, 6], такі як гіроїд [6], стали звичайними елементами дизайну для 3D-друкованих деталей. Теорія мінімальних поверхонь (МП) - одна з класичних і в той же час галузей математики, що розвиваються (на стику геометрії, топології та варіаційного обчислення). Вона вивчає математичні властивості поверхонь, які мінімізують певні енергетичні функціонали. Основна ідея полягає в тому, що МП має найменшу можливу енергію серед усіх поверхонь, які обмежені заданим контуром або границею. Наочною реалізацією МП служить мильна плівка, вона затягує контури різної конфігурації та набуває форми, що відповідає мінімуму потенційної енергії (енергії поверхневого натягу), яка прямо пропорційна її площі.

Окремий клас МП утворюють періодичні поверхні TPMS, які можуть бути отримані нескінченним повторенням деякої елементарної комірки, а застосування їх для 3D-моделювання підвищує технологічність наступного виробництва модельованих конструкцій шляхом збирання останніх (в заданих просторових напрямках), зокрема з повторюваних серійно виготовлених (надрукованих) елементів моделей. Для фахівців з 3D-моделювання цікавим є застосування теорії TPMS, оскільки вона дозволяє створювати складні геометричні форми, які можуть бути використані для створення унікальних та ефективних конструкцій, зокрема в ливарному виробництві. Також ця теорія знаходить широкі застосування у різних

галузях, включаючи матеріалознавство, архітектуру та біологію.

Робота [5] містить важливі відомості про цю теорію і може бути корисною для розуміння її застосувань у 3D-моделюванні. Крім того, таке моделювання дозволить створювати поверхні "мінімальні" з точки зору таких складних функціоналів, як комбінація енергії поверхневого натягу, гравітаційної енергії, енергії деформації тощо, а також довільних поверхневих інтегралів, що задаються користувачем. Це дає можливість не лише отримувати на комп'ютері креслення моделі з МП, але і МП у поєднанні з заданими службовими характеристиками модельованих конструкцій, що потім будуть отримані 3D-друком. Аналітичність МП, кожна точка яких визначається у просторі аналітичною функцією, спрощує 3D-моделювання, технологічність виготовлення матеріальних виробів, а також контроль їхньої якості і подальшої обробки за допомогою сучасного устаткування з програмним забезпеченням.

Компанія Spherene Inc., зокрема наслідуючи коралоподібні природні структури, розробила дещо нову (порівняно з TPMS) геометрію метаматеріалів, засновану на іншому класі геометричних форм, що за рахунок мінімальних поверхонь (МП) мінімізують об'ємну масу матеріалу: сфери, або, точніше, інверсні сфери, які компанія називає «spherenes» [4]. Використанням МП для моделювання мінімальних енергетичних станів матеріалів у фізичних моделях досягають того, що структури Spherene Inc. рівномірно розподіляють напругу, мінімізуючи кількість використовуваного матеріалу. Приклади за методикою такого моделювання показано на рис. 1.

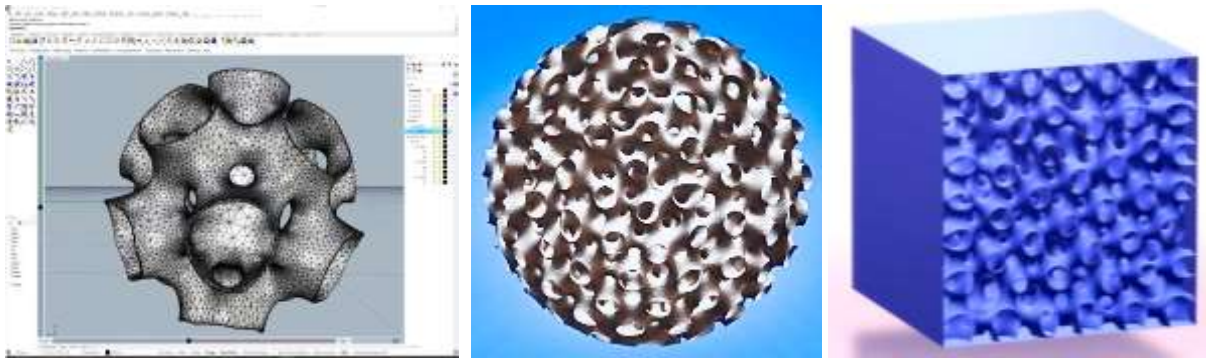


Рисунок 1 - Приклади структур типу spherenes, в тому числі в якості наповнювача в конструкціях з зовнішньою гладкою поверхнею у вигляді куба (моделі створено за методикою з сайту <https://spherene.ch>)

Компанія Spherene Inc. алгоритм заповнення друківаних конструкцій за допомогою інверсних сфер зробила доступним через програмний інтерфейс застосування (API – Application Programming Interface) Rhino. Rhinoceros (Rhino), згідно <https://uk.wikipedia.org>, - NURBS-орієнтована програма для тривимірного моделювання, розроблена Робертом МакНілом (Robert McNeel & Associates). Це програмне забезпечення здебільшого використовується для промислового дизайну, архітектури, ювелірного дизайну, дизайну транспортних засобів, САПР, швидкого прототипування, зворотної розробки, а також у галузях мультимедіа і графічного дизайну.

На рис. 1 перше фото ліворуч та інші фото нижче (з відображенням комп'ютерного меню) відтворено у вигляді скріншота з екрану, де автори статті використовували програму Rhinoceros 8 для моделювання.

Алгоритм за допомогою хмарного API може заповнити проектний об'єм оболонками з поверхнею ADMS, геометрія якої повторює перевернуті сферичні поверхні для створення міцної та відкритої структури, або серцевини тіла чи стінок тривимірних фізичних об'єктів (рис. 2). Сфери складають наче один безперервний оболонковий лабіринт і є ідеальною формою для втримання і розподілення напружень всередині порожнього об'єму.

Засновник компанії, Крістіан Вальдвогель, колишній архітектор і художник, експериментуючи з паперовою моделлю семикутників, прийшов до висновку, що мінімальні поверхні можна розглядати як перевернуті сфери, що заповнюють простір [4]. Створений Spherene Inc. (замість окремої програми) хмарний API інтегрується як з програмним забезпеченням САПР Rhino, так може застосовуватися і в інших середовищах САПР. Компанія є стартапом з 2018 р. і пропонує послуги з інтеграції сферичних структур у САД-моделі клієнтів, а також планує надати комерційне ліцензування метаматеріалу spherenes.

Переваги матеріалу spherenes заявлено такі [4].

- Зменшення ваги. Заміняє інший матеріал на заданій об'ємній ваги заповнення, зберігаючи міцність.
- Настроюваність. Сфероподібну пористу «геометрію» можна поєднати з суцільними областями, щоб закрити певні об'єми, ввести отвори під гвинти чи створити внутрішні порожнини. Можна використовувати градієнти для зменшення маси матеріалу (рис. 3), зміщення центру ваги або контролю еластичності.



Рисунок 2 - Приклади друківаних полімерних і металевих виробів типу коралу чи кістки, кронштейнів та декоративної фігурки (з сайту <https://spherene.ch>)

- Відповідність поверхні. Сферени за своєю природою повторюють форму обмежувальної геометрії.
- Самоокупний. У більшості процесів 3D-друку об'єкти, виготовлені зі сферичного метаматеріалу, можна друкувати без опорних структур.
- Економія матеріалів. Конструкції, наповнені такими структурами, використовують менше матеріалу для друку та можуть друкуватися швидше.

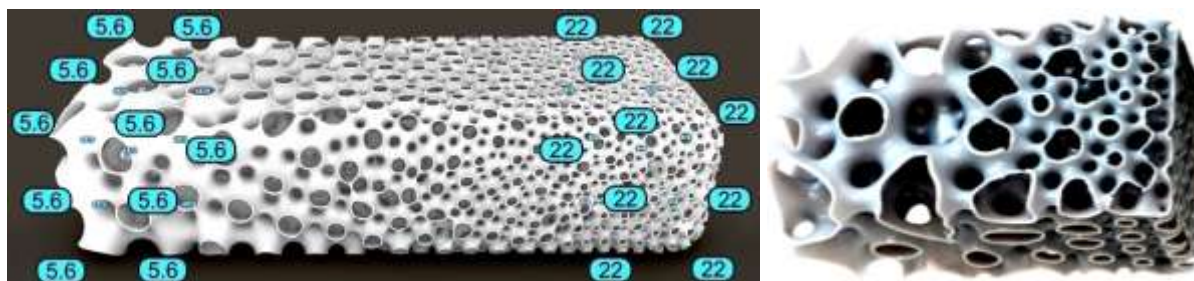


Рисунок 3 - Структура з градієнтом щільності і її друківаний приклад (з сайту <https://spherene.ch>)

Використання Spherene API потребує, щоб користувач спочатку визначив модель у САПР, що слугує обчислювальною оболонкою, у якій генеруватимуться оболонки сферичної геометрії. Залежно від вибору дизайнера, модель може бути заповнена сферою постійної щільності та фіксованої товщини, або вона може містити градієнти щільності та товщини, порожнини чи суцільні області. Спосіб, у який сферичні поверхні зустрічаються (стикуються) з конвертом (відомий як «умова конверта»), також можна контролювати.

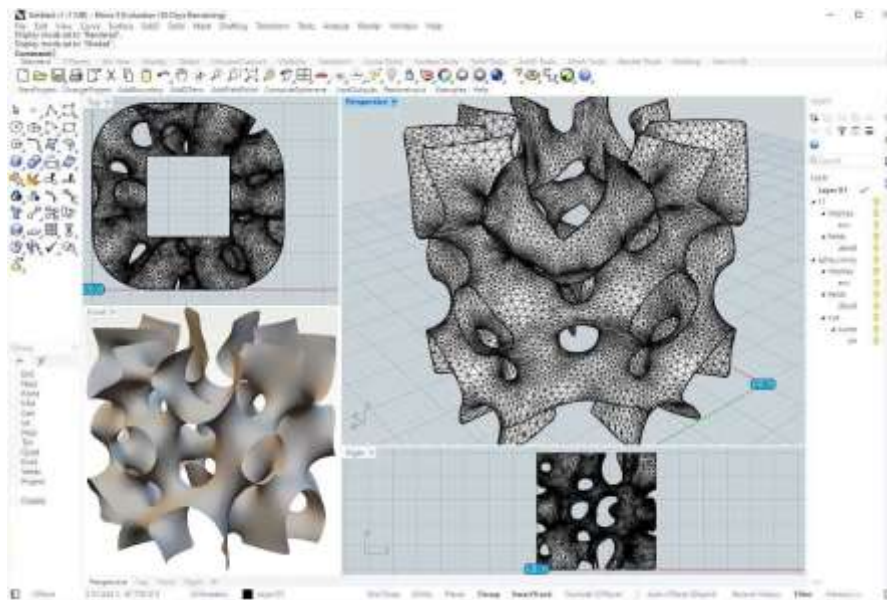
Незалежно від вхідних даних або геометричної складності оболонки, алгоритм Spherene Inc. генеруватиме ізотропну мінімальну поверхню, що складається з двох переплетених просторів [4]. Якщо цього не буде спеціально вказано, алгоритм ніколи не створить повністю закриту форму для 3D-друку. API Spherene автоматично адаптує заповнення до вимог, встановлених користувачем, створюючи структури, схожі на корал або кістку в перерізі (рис. 2). Це означає, що користувачам не потрібно мати справу з особливостями загальної форми або маніпулювати такими параметрами, як розмір пор або товщина стінки, щоб отримати бажаний результат; замість цього вони починають рух до бажаного результату, вираженого в термінах щільності заповнення та стану оболонки. Вищий відсоток щільності заповнення створює більше оболонкового матеріалу, який може бути використаний, наприклад, для збільшення жорсткості в певних областях, тоді як нижчу щільність може бути застосовано для

забезпечення гнучкості або пружності. Алгоритм метаматеріалу spherene виконає моделювання матеріалу автоматично.

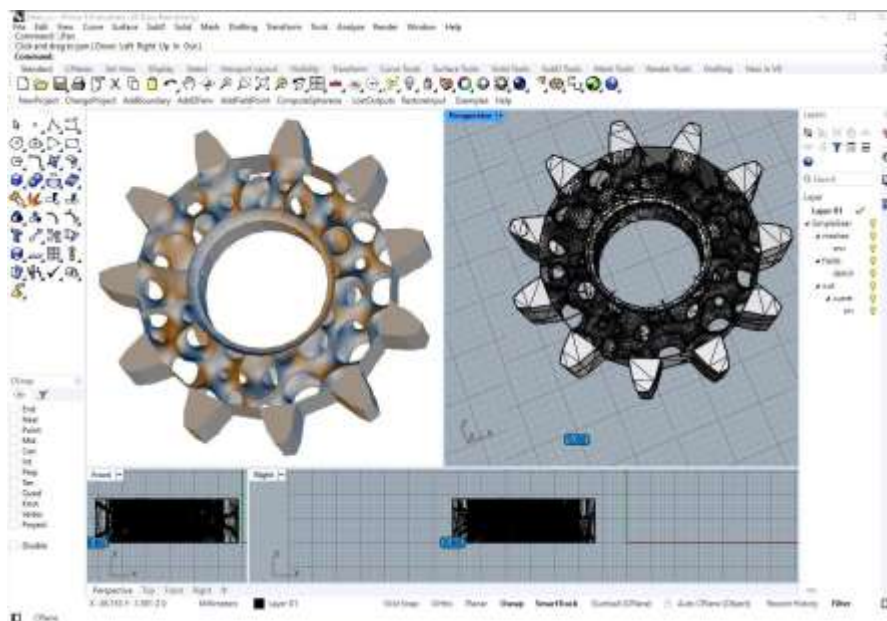
У багатьох випадках градієнти потрібні для створення жорсткіших окремих областей деталі. При цьому постійні практичні застосування дозволяють точніше прогнозувати, як можуть працювати конкретні 3D-друковані об'єкти, не обов'язково покладаючись на моделювання та тестування. Так, можна надрукувати сталеву деталь зі зниженою щільністю до такої міри, що матеріал буде нагадувати алюміній, як за вагою, так і за міцністю. Економія часу та матеріалів на розробку істотно впливає на зміну економічності деталі [4].

Як методика заповнення (порівняно з іншими геометричними системами, такими як TPMS і балкові решітки), ADMS від Spherene Inc. має ті переваги, що забезпечує ізотропну міцність по всьому об'єму деталі, а також сферо-похідні оболонки є самонесучими для виготовлення за допомогою більшості технологій 3D-друку. За словами компанії, відповідність поверхні та контрольований стан оболонки також забезпечують бездоганну інтеграцію збірки з цими структурами [4]. Інструмент дизайну Spherene Inc. наразі знаходиться в загальнодоступній бета-версії для тестування безкоштовно, а також компанія надає індивідуальні рішення для замовників у таких галузях, як аерокосмічна промисловість, високоефективні технології, інструменти, спортивне взуття та медицина [4].

На рис. 4, а-г показано наші моделювання у програмі Rhinoceros 8 за алгоритмом ADMS.



а



б

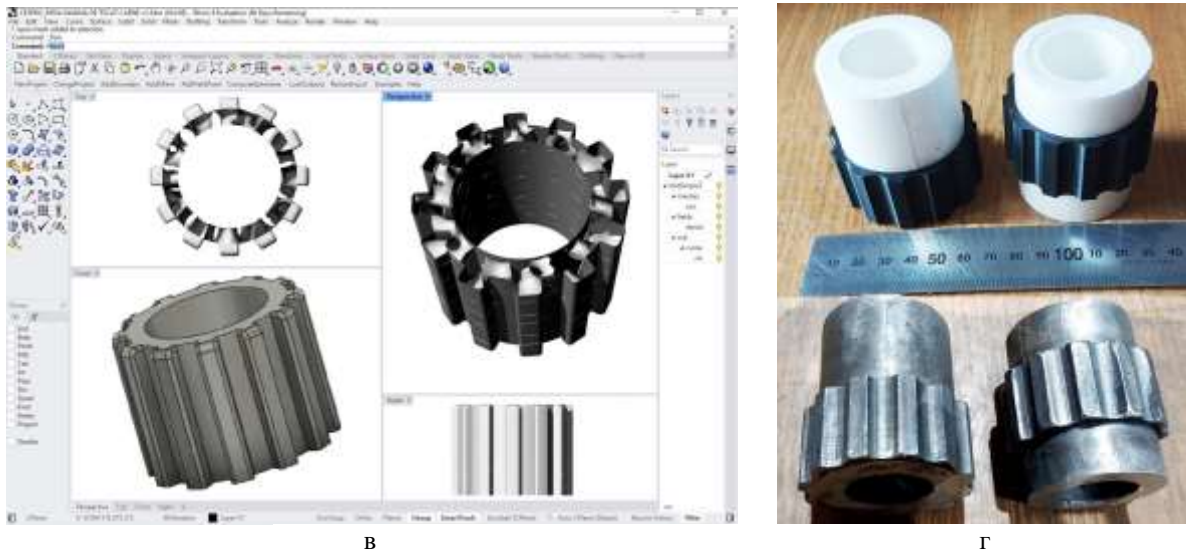


Рисунок 4 - Моделювання у програмі Rhinoceros 8 за алгоритмом ADMS: а – заповнення оболонками простору «куб» з каналом під трубу профільну квадратну; б – модель шестерні; в – модель «втулка приводна»; г – ливарні моделі і вилівки «втулка приводна» (3D-друк суцільної моделі зі вставкою з ППС)

Для порівняння з модельованими за алгоритмом ADMS на рис. 4, в показано два варіанти подібної форми ливарних моделей на рис. 4, г (верхній ряд) і вилитих (з чавуну СЧ200 ДСТУ EN 1561:2010) по ним деталей «втулка приводна» (нижній ряд), раніше виготовлених згідно із роботою [7]. Друковані методом FDM суцільні формуючі частини моделі чорного кольору (рис. 4, г) для полегшення маси всієї моделі були насаджені на патрубки з ППС (білого кольору). Інакше вилити способом ЛГМ за друкованими моделями без створення в них пористої стінки з ППС в моделях не вдавалось, попередні спроби давали лише браковані металовироби.

На рис. 5 показано наші перші пробні друкування з пластику PLA на принтері «Vambu Lab A1 mini» елементів, змодельованих за алгоритмом ADMS. Ці елементи дещо схожі на спрощений варіант моделей, зображених на рис. 4, а. Оскільки на цьому принтері досягається товщина друкованого шару 0,1-0,4 мм (100-400 мкм), то ми прагнемо подальшим відпрацюванням досягти друку більш складних і ажурних конструкцій включно з ливарними моделями спрямованої пористості для ЛГМ.

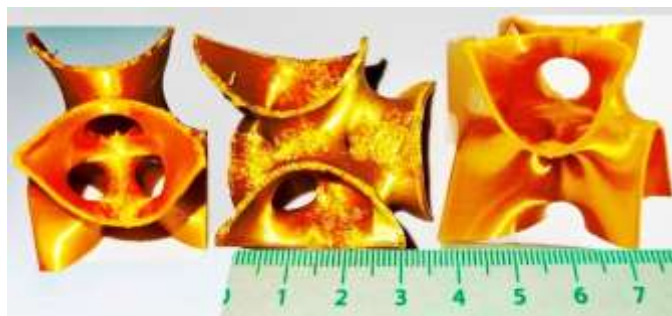


Рисунок 5 – Друковані елементи за алгоритмом ADMS на 3D-принтері методом FDM

Виконані нами перші приклади цифрового моделювання для друку і спроби друкування пористих (порожнистих) полімерних ливарних моделей показали придатність використання алгоритму від Sphere Inc. з гармонійним включення пор до їх конструкції для зменшення маси моделей. Наступними кроками будуть вибір оптимального способу їх друкування і досягнення майстерності в цьому, а також дослідження декількох можливих переваг чи додаткових функцій з огляду мінімізації маси (кількості матеріалу) в залежності від достатніх механічних властивостей друкованої ливарної моделі та регулювання аеродинамічних характеристик утворених вентканалів в пористому середовищі моделі, зниження коефіцієнта опору фільтрації в них газів в залежності від рівня впливу вакуумування з боку піщаної ливарної форми і ступеня його силової дії на стінки піщаної форми (для забезпечення їх непорушності) та на метал, що газифікує модель, тощо.

Таким чином, після першого етапу впровадження 3D-друку в ЛГМ-процес лиття металу за комбінованими моделями з підкладками з ППС, які покриті друкованими поверхневими оболонками [2, 7] чи

змонтовані з окремими друківаними на 3D-принтері деталями (рис. 4, в), створюються передумови переходу до наступного етапу: 3D-моделювання і друкування оптимально спроектованих цільних пористих ливарних моделей. Такий крок значно розширює можливості 3D-друку, практично повністю автоматизуючи виробництво полімерних газопроникних ливарних моделей, яке можливо виконувати цілодобово, наслідуючи такий процес на вже існуючих фермах 3D-друку [9].

Підбиваючи підсумки, нагадаємо з роботи [2] про концепцію здійснення ЛГМ-процесу за пористими друківаними моделями, відображену в способі лиття [8] і для реалізації якої виконано вище описані приклади моделювання. При газифікації металом у ливарній формі полімерної моделі з пористою серцевиною стінок цю пористість використовують як соти-вентканалі, крізь які виводять газу по ходу поступової газифікації моделі металом, що заповнює вакуумовану піщану форму і заміщує модель. Верхню частину моделей друкують так, щоб до моделі доєднати полімерні трубки-надставки для випорів чи надливів, які сполучають з вентканалами моделі, накривають газопроникним матеріалом, що не пропускає пісок, і крізь ці надставки виводять газу від моделі у пори піску форми з відсмоктуванням їх завдяки вакууму, який підтримують у цій формі.

Якщо традиційна ливарна модель з ППС газонепроникна, має закриті пори і метал випаровує хаотично орієнтовані стінки-оболонки цих пор, то 3D-друком отримують відкриті (трансляційні) пори заданої орієнтації (раніше внесені в конструкцію моделі на моніторі комп'ютера) для суцільної вентиляції і відкачування вакуумом газів (від випаровування - газифікації металом цієї моделі) разом з частковим засмоктуванням металу, що полегшує заповнення ним формотворної порожнини, загалом підвищуючи якість лиття. Описаний механізм застосування пористих друківаних моделей [8] дозволяє лити метал навіть за моделями дещо більшої газотвірності, ніж з традиційного ППС. Цьому сприяє розкриття потенціалу друку, що надає ливарній моделі як традиційну функцію відтворення геометрії виливка, так і функцію спрямованого і примусового видалення продуктів її газифікації крізь піщане середовище вакуумованої ливарної форми.

Висновки

Адитивні технології виробництва відкривають можливості для змін у конструкціях ливарної продукції та її ливарних моделей шляхом внесення змін у цифрову модель продукції без необхідності зміни ливарного обладнання. Це дозволяє швидко та ефективно адаптувати (варіювати) конструкції для виробництва за новими вимогами чи замовленнями без значних витрат часу і коштів на виготовлення нового оснащення та інших засобів виробництва, сприяє швидкому та ефективному росту виробництва та модифікації металопродукції. При виготовленні і застосуванні для ЛГМ-процесу легковагих друківаних моделей, що за об'ємною вагою та газотвірністю наближаються до типових моделей з ППС, методи конструювання пористих вентиляційних моделей, оптимізації процесу газифікації друківаних матеріалів запропоновано реалізувати за допомогою нових алгоритмів проектування легковагих конструкцій, які інтегровані у діюче програмне забезпечення для тривимірного моделювання, зокрема у програму Rhinoceros. В статті досліджено і випробувано недавно створений компанією Spherene Inc. алгоритм проектування 3D-друківаних конструкцій стосовно друкування ливарних моделей низької об'ємної ваги, придатних для ЛГМ-процесу. Цей алгоритм є прикладом новаторського впровадження в діючу програму тривимірного моделювання досягнень прикладної математики в галузі теорії тривимірних періодичних мінімальних поверхонь. Виконані нами перші приклади цифрового моделювання макропористих ливарних моделей для їх друку і пробні друкування з полімеру підтвердили доступність використання алгоритму від Spherene Inc. і гармонійного включення пор чи порожнин сфероподібної конфігурації в їх конструкцію як з можливістю збереження достатньої міцності моделей при зменшенні їх маси, так і друкування відкритих (трансляційних чи спрямованих) пор заданої орієнтації для суцільної вентиляції і відкачування газів вакуумом ливарної форми разом з частковим засмоктуванням металу в робочу порожнину форми.

Науково-технологічне дослідження виконано згідно договору 226 (166/24) від 22.02.2024 про наукове співробітництво між Фізико-технологічним інститутом металів та сплавів НАН України та Вінницьким національним технічним університетом.

Список літератури

- [1] N. D. Rasmussen, "A Digital Revolution is Transforming Foundries Worldwide", *Foundry Management & Technology*. Jan./Feb., pp. 27-28. 2024.
- [2] В. С. Дорошенко, О. Б. Янченко, "Застосування комп'ютерних систем для проектування та 3D-друку ливарної моделі з вентиляційними каналами в її стінках", *Інформаційні технології та комп'ютерна інженерія*, № 3, с. 53-58. 2023.
- [3] Industry 4.0: How to navigate digitization of the manufacturing sector. McKinsey Digital. [Online]. Available: https://www.mckinsey.de/files/mck_industry_40_report.pdf. Accessed on: 2015.

- [4] S. Hendrixson, "Metamaterial With Geometry Derived From Spheres", *Additive Manufacturing*. May, p. 40. 2024.
- [5] Meeks. William H. The Theory of Triply Periodic Minimal Surfaces. *Indiana University Mathematics Journal*. 39, no. 3, pp. 877-936. 1990.
- [6] Triply-periodic minimal surfaces. [Online]. Available: <https://schoengeometry.com/e-tpms.html>.
- [7] П. Б. Калюжний, В. С. Дорошенко, О. В. Нейма, "Лиття за комбінованими полімерними моделями, що газифікуються", *Процеси лиття*, № 2, с. 49-55. 2023.
- [8] І. А. Шалевська, О. В. Нейма, С. О. Кротюк, В. С. Дорошенко, "Спосіб лиття металу за 3D-друкованими моделями, що газифікуються у вакуумованих формах з сипкого піску", *заявка України u202305216. МПК8 B22 C7/02, B22C 9/04*. 3.11.2023.
- [9] В. С. Дорошенко, П. Б. Калюжний, С. В. Коломійцев, "Приклади 3D-технологій виробництва металовиробів і полімерних моделей", *Процеси лиття*, № 4, с. 48- 54. 2021.

Стаття надійшла до редакції: 27.04.2024

References

- [1] N. D. Rasmussen, "A Digital Revolution is Transforming Foundries Worldwide", *Foundry Management & Technology*. Jan./Feb., pp. 27-28. 2024.
- [2] V. S. Doroshenko, O. B. Yanchenko, "Application of computer systems for designing and 3D printing of a foundry pattern with ventilation channels in its walls", *Information technologies and computer engineering*, No. 3, pp. 53-58. 2023.
- [3] Industry 4.0: How to navigate digitization of the manufacturing sector. McKinsey Digital. [Online]. Available: https://www.mckinsey.de/files/mck_industry_40_report.pdf. Accessed on: 2015.
- [4] S. Hendrixson, "Metamaterial With Geometry Derived From Spheres", *Additive Manufacturing*. May, p. 40. 2024.
- [5] Meeks. William H. The Theory of Triply Periodic Minimal Surfaces. *Indiana University Mathematics Journal*. 39, no. 3, pp. 877-936. 1990.
- [6] Triply-periodic minimal surfaces. [Online]. Available: <https://schoengeometry.com/e-tpms.html>.
- [7] P. B. Kalyuzhny, V. S. Doroshenko, O. V. Neyma, "Casting according to combined polymer patterns that are gasified", *Casting Processes*, No. 2, pp. 49-55. 2023.
- [8] Pat. Appl. u202305216 UA, IPC B22C7/02, B22C9/04, Method of metal casting according to 3D-printed patterns, which are gasified in vacuum molds from loose sand, P. B. Kalyuzhny, I. A. Shalevska, O. V. Neyma, S. O. Krotiyuk, V. S. Doroshenko, Publ. 3.11.2023.
- [9] V. S. Doroshenko, P. B. Kalyuzhny, S. V. Kolomiitsev, "Examples of 3D technologies for the production of hardware and polymer patterns", *Casting Processes*, No. 4, с. 48- 54. 2021.

Відомості про авторів

Бродовий Олег Володимирович – студент ліцею.

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

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

O. V. Brodovy¹, V. S. Doroshenko², O. B. Yanchenko³

3D DESIGN OF POROUS FOUNDRY PATTERNS IN THE RHINOCEROS 8 PROGRAM

¹Mikhail International Lyceum, Kyiv

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

³Vinnitsia National Technical University, Vinnitsia

УДК 004.415.5:621.3.019.3:005.591.6

А. С. Шантир

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ МОДЕЛЕЙ ОЦІНКИ ЯКОСТІ НА ЕТАПАХ РОЗРОБКИ ТА ВИКОРИСТАННЯ ПРОГРАМНИХ СИСТЕМ

Державний університет інформаційно-комунікаційних технологій, Київ

Анотація. В статті аналізуються особливості застосування моделей оцінки якості на різних етапах розробки та використання програмних систем з метою забезпечення їхньої високої якості. Головною метою дослідження є визначення нових комбінованих підходів, щодо оцінки ефективності та впливу використання моделей якості на різних етапах життєвого циклу програмних продуктів. У ході роботи використовується системний підхід до аналізу, що враховує взаємодію моделей якості з різними етапами проектування, розробки, тестування та експлуатації програмного забезпечення. Зокрема, розглядається роль моделей якості у підвищенні ефективності процесів розробки та їх вплив на остаточну якість продуктів. Методологія включає в себе аналіз існуючих моделей якості, їх адаптацію до конкретних умов проекту, а також вивчення практичних прикладів впровадження моделей якості в реальних проектах. Реалізується аналіз існуючих моделей якості, їх адаптацій до конкретних умов програмних системних проектів та аналіз впровадження в реальних проектах. Цей підхід дозволив нам отримати конкретні результати та розкрити ключові аспекти впровадження моделей якості. Розглядається взаємодія моделей якості із загальними стратегіями забезпечення якості та їхній вплив на підвищення продуктивності та надійності програмних систем. В загальнонауковому аспекті дослідження зводиться до оцінки ефективності цього підходу та визначенні його ключових особливостей. Подальший розгляд показав, що використання нових комбінованих моделей якості на етапах проектування, розробки та тестування сприяє покращенню різних аспектів якості програмного забезпечення. Вони не лише визначають критерії якості, але й сприяють забезпеченню відповідності цим критеріям протягом усього життєвого циклу проекту. Отримані результати підтверджують важливість використання комбінованих моделей якості на всіх етапах розробки програмних систем. Це сприяє не лише покращенню якості кінцевого продукту, але і ефективності всього процесу розробки. Наші результати можуть слугувати основою для практичного впровадження моделей якості в проекти програмного забезпечення та покращення загального рівня якості у цій галузі.

Ключові слова: Інтеграційна модель зрілості можливостей, процеси забезпечення якості програмного забезпечення, квадранти гнучкого тестування, Шість Сигм, загальне управління якістю, процес програмного забезпечення, фреймворк архітектури групи.

Abstract. The article examines the peculiarities of applying quality models at different stages of development and utilization of software systems to ensure their high quality. The main aim of the research is to identify new combined approaches for evaluating the effectiveness and impact of quality models usage at various stages of software product life cycles. The work employs a systematic approach to analysis, considering the interaction of quality models with different stages of software design, development, testing, and operation. Specifically, the role of quality models in enhancing the efficiency of development processes and their impact on the final product quality is discussed. The methodology involves analyzing existing quality models, adapting them to specific project conditions, and studying practical examples of quality model implementation in real projects. An analysis of existing quality models, their adaptation to specific conditions of software system projects, and an analysis of implementation in real projects are carried out. This approach has enabled us to obtain specific results and reveal key aspects of quality model implementation. The interaction of quality models with overall quality assurance strategies and their impact on improving the productivity and reliability of software systems is considered. In a general scientific aspect, the research boils down to evaluating the effectiveness of this approach and determining its key features. Further examination showed that the use of new combined quality models in the stages of design, development, and testing contributes to the improvement of various aspects of software quality. They not only define quality criteria but also ensure compliance with these criteria throughout the project life cycle. The obtained results confirm the importance of using combined quality models at all stages of software development. This contributes not only to the improvement of the final product quality but also to the efficiency of the entire development process. Our results can serve as a basis for the practical implementation of quality models in software projects and improving the overall quality level in this field.

Key words: Capability maturity model integration, software quality assurance processes, agile testing quadrants, Six Sigma, total quality management, software process, group architecture framework.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-127-138>.

Вступ

В сучасному світі, де програмні системи стають невід'ємною частиною практично будь-якої сфери діяльності, забезпечення їх якості має вирішальне значення. Зростання вимог до надійності, ефективності та безпеки програмних продуктів вимагає від розробників постійного вдосконалення методів тестування та контролю якості. Перед впровадженням будь-якої програмної системи необхідно ретельно проаналізувати її вимоги та визначити критерії якості, які відображають очікувані властивості та параметри. Моделі якості допомагають не лише визначити ці критерії, але й встановити методи їх вимірювання та оцінки. Зважаючи на вищевказане досить актуальною проблемою є розуміння особливостей та переваг використання моделей якості на різних етапах розробки та використання програмних систем, яка поправу стала ключовою в області забезпечення успішної реалізації проектів та задоволення потреб користувачів. Аналіз цих аспектів допомагає ефективно впроваджувати стратегії контролю якості та забезпечувати високу якість програмних продуктів.

Актуальність

Актуальність проблеми забезпечення якості програмних систем на кожному етапі їх життєвого циклу відображається в потребі постійного пошуку нових ефективних методів оцінки та контролю якості програмних продуктів. Навіть при успішній розробці даних продуктів, важливо забезпечити їх високу якість протягом усього періоду їх використання. Таким чином, розуміння особливостей та вибір оптимальних моделей якості стає ключовим для ефективної розробки та використання програмних систем. За останні роки програмне забезпечення проникає в усі сфери життя, проблема забезпечення його якості стає надзвичайно актуальною. Висока конкуренція, швидкі темпи розвитку технологій та зростання очікувань користувачів створюють виклики для розробників у плані забезпечення надійності, продуктивності та безпеки програмних продуктів. При цьому, складність програмних систем та розмір їх кодової бази ускладнюють процес тестування та виявлення помилок, що може призвести до зниження якості та недоліків у функціональності. Таким чином, необхідність вдосконалення методів оцінки, контролю та забезпечення якості програмного забезпечення є актуальною проблемою, яка потребує пошуку ефективних рішень.

Мета

Метою дослідження є визначення та розробка нових комбінованих підходів, щодо оцінки ефективності та впливу використання моделей якості на різних етапах життєвого циклу програмних продуктів.

Задачі

1. Проаналізувати відомі проблеми які виникають в моделях якості, котрі застосовуються для оцінки та підтримки якості програмних систем на різних етапах їх розробки та використання.
2. Виконати постановку завдання розробки комбінованої системної моделі оцінки якості в межах адаптивного застосування моделей якості із цілю підвищення ефективності процесів розробки та їх впливу на механізм оцінювання якості програмних продуктів.
3. Розробити комбінований метод оцінки ефективності та впливу використання моделей якості на різних етапах життєвого циклу програмних продуктів.

Розв'язання задач

1. Аналіз проблем. У реаліях швидкозмінюваного інформаційного середовища, розробка програмних систем (ПС) стає відокремлюючою лінією між успіхом та викликами у сфері інформаційних технологій. Постійні та динамічні зміни у вимогах користувачів, ростучі обсяги даних та загострена конкуренція вимагають від розробників не тільки креативності та експертності, але і вдосконалення стратегій управління якістю програмного забезпечення. В останні роки відзначається активний розвиток підходів до розробки, орієнтованих на досягнення високої якості продукту [1]. Застосування моделей якості на різних етапах життєвого циклу програмної системи визнається, як важлива стратегія для покращення процесів розробки та забезпечення високого рівня функціональності та надійності[2]. У цьому контексті, наукове дослідження та аналіз останніх вирішених проблем в галузі застосування моделей якості стають невід'ємною частиною стратегічного планування для компаній і розробників програмного забезпечення. Проте, залишаються відкритими питання невизначеності в розробці нових методичних технологій із оцінки якості ПС [3] та пошуку оптимальних рішень у змінюючихся умовах ринку, що потребує глибокого наукового аналізу ролі та ефективності застосування моделей якості на кожному етапі розробки програмних систем, розглядаючи як вирішені проблеми, так і ті аспекти, які залишаються під великим питанням. Розглядання цих питань має на меті поглиблене розуміння та визначення оптимальних підходів для досягнення високих стандартів якості у розробці програмного забезпечення. Дослідження в області застосування моделей якості в розробці та використанні програмних систем відбувається постійно, і багато проблем вже мають вирішення, але також існують ті, які залишаються відкритими.

Вирішені проблеми:

- Розробка стандартів якості: Великий крок був зроблений у напрямку стандартизації методів та метрик оцінки якості програмних систем [1–15]. Наприклад, ISO 25010 визначає модель якості програмного забезпечення визначає набір характеристик та сценарії їх використання;
- Автоматизація тестування [1, 4]: Автоматизовані засоби тестування дозволяють ефективніше виявляти помилки та проблеми якості на ранніх етапах розробки;
- Моделювання процесів розробки [3–5]: Застосування моделей для опису та аналізу процесів розробки сприяє покращенню якості виробництва програмного забезпечення.

Невирішені, або актуальні проблеми:

- Оцінка користувацького досвіду: Визначення об'єктивних метрик для оцінки користувацького досвіду залишається складною задачею, оскільки він є суб'єктивним поняттям [4];
- Моделі для безпеки та захисту: Забезпечення ефективних моделей для визначення та оцінювання безпеки програмних систем залишається відкритою проблемою [7];

- Врахування вимог до взаємодії та масштабованості: Зростання складності систем та вимог до їх взаємодії може створювати виклики при розробці моделей якості, які повинні враховувати ці аспекти [8];
- Врахування змінливості вимог: В межах технологічного прогресу нині постійно змінюються вимоги до програмних систем, які можуть призводити до потреби в адаптації моделей якості для забезпечення їх актуальності та ефективності [9];
- Врахування впливу різних технологій: Швидкі зміни технологій можуть створювати труднощі у врахуванні їх впливу на якість програмного забезпечення [10];
- Моніторинг у реальному часі: Розробка засобів моніторингу, які надають інформацію в реальному часі та дозволяють швидко реагувати на проблеми, залишається важливою задачею [11].

Зазначені вище фахові тематичні спрямованості відображають сучасні виклики та тенденції в області оцінки якості програмного забезпечення, і вони можуть бути об'єктом активного дослідження та розвитку.

В табл.1. наведено результати порівняльного аналізу щодо застосування популярних моделей якості на різних етапах розробки та використання програмних систем.

З табл.1. видно, що кожна модель якості має свої унікальні особливості, які можуть бути корисними на різних етапах розробки та використання програмних систем. Зокрема деякі моделі, такі як ISO/IEC 25010 та IEEE 730, акцентують на оцінці якості продукту та процесів розробки, зазначаючи ключові критерії, які можна використовувати для цього. Інші, наприклад, CMMI та SPICE, спрямовані на підвищення зрілості процесів розробки програмного забезпечення. Деякі моделі, такі як Agile Testing Quadrants та Lean Software Development, спеціалізуються на використанні в Agile-процесах та мінімізації витрат. Зважаючи на вище наведене вибір моделі якості повинен залежати від конкретних потреб та характеристик проекту. Інтеграція моделей якості з процесами розробки може допомогти забезпечити більш ефективну та якісну розробку програмного забезпечення.

Відповідно аналізу наукових праць [1–15] застосування моделей якості на різних етапах розробки та використання програмних систем може стикатися з рядом проблем. Зокрема в праці [1] піднімається проблема, щодо недооцінки вимог до якості, дана проблема зводиться до того, що не завжди вдається коректно визначити та врахувати всі вимоги до якості програмної системи на ранніх етапах розробки. Аналізуючи більш детально дану проблему можна зробити висновок, що проблема недооцінки вимог до якості програмної системи полягає в тому, що на ранніх етапах розробки не завжди вдається коректно визначити та врахувати всі аспекти якості, які можуть вплинути на подальший процес розробки та експлуатації програмного продукту. Це може призвести до недоліків у функціональності, надійності, ефективності та інших аспектах якості програмного забезпечення. З нашої позиції доцільно відмітити, що для вирішення цієї проблеми важливо застосовувати адекватні методи та моделі управління якістю, які дозволять виявляти, визначати та враховувати вимоги до якості на початкових етапах розробки. Також в даному аспекті досить важливо використовувати практики та методології, що сприяють ранньому виявленню та вирішенню проблем якості, такі як Agile-підходи, Continuous Integration та Continuous Delivery, тестування на ранніх етапах розробки тощо. Загалом, управління якістю на ранніх етапах розробки є критично важливим для успішної поставки програмного забезпечення, і це вимагає уваги до всіх аспектів якості від самого початку процесу розробки.

В праці [2] піднімається проблема, щодо недостатнього охоплення тестування в межах застосування моделей якості на різних етапах розробки та використання програмних систем: не завжди можна забезпечити повне тестування всіх аспектів програми, що може призводити до уникнення або неправильного виявлення деяких дефектів, що загрожує якості та надійності програмного забезпечення. Згідно з [2–4] для вирішення цієї проблеми важливо використовувати комплексний підхід до тестування, який охоплює різні аспекти програмного забезпечення, такі як функціональність, надійність, ефективність, безпека та інші.

Згідно з [5] у вирішенні вище зазначеної проблеми важливо використовувати автоматизоване тестування та інструменти для підвищення ефективності тестування та забезпечення більш широкого охоплення коду.

Аналізуючи погляди авторів праці [6] доцільно погодитися що в піднятій проблемі виникає нагальна необхідність, щодо врахування особливостей конкретного проекту та контексту використання програмного забезпечення при плануванні та виконанні тестування, щоб забезпечити його високу якість та надійність.

Автори праці [9] акцентують увагу на потребі, щодо надання належної уваги тестуванню на ранніх етапах розробки, що в свою чергу дозволить виявляти та виправляти дефекти на ранніх стадіях, коли вони ще не вирішилися в серйозні проблеми.

Таблиця 1 – Результати порівняльного аналізу щодо застосування популярних моделей якості на різних етапах розробки та використання програмних систем

Найменування моделі якості	Етап Застосування	Основна мета	Ключові критерії	Застосування в Agile	Інтеграція з Процесами
ISO/IEC 25010	Різні етапи від концепції до підтримки	Оцінка якості продукту та процесів	Функціональність, Надійність, Ефективність	Так	Можлива
CMMI	Розробка та підтримка	Зрілість процесів та управління	Зрілість процесів, Продуктивність	Не прямо спрямовано	Є процеси зрілості
IEEE 730	Етапи розробки та тестування	Вимоги до процесів розробки	Вимоги до процесів розробки	Так	Можлива
Agile Testing Quadrants	Особливо актуальна в Agile	Класифікація тестування в Agile	Цілі тестування на кожному квадранті	Так	Можливість інтеграції в Agile процес
Six Sigma	Етап підтримки	Покращення якості та ефективності	Виявлення та виправлення помилок	Неявно	Вимагає особливостей процесів
TQM (Total Quality Management)	Різні етапи	Загальне управління якістю	Клієнтське задоволення, Залученість персоналу, Постійне покращення	Так	Так
SPICE (Software Process Improvement and Capability Determination)	Розробка та експлуатація	Покращення процесів розробки програмного забезпечення	Здатність до процесів, Ефективність	Можливе	Так
TOGAF (The Open Group Architecture Framework)	Різні етапи	Управління та підтримка корпоративної архітектури	Архітектурна якість, Взаємодія з бізнес-потребами	Частково	Так
SPICE (ISO/IEC 15504)	Розробка та експлуатація	Визначення та оцінка процесів розробки ПЗ	Процесна зрілість та продуктивність	Неявно	Так
COBIT (Control Objectives for Information and Related Technologies)	Управління та оптимізація ІТ	Керування ІТ з метою досягнення бізнес-цілей	Забезпечення стійкості, Забезпечення безпеки	Частково	Так
Lean Software Development	Розробка та підтримка	Мінімізація витрат та оптимізація	Велика цінність, Мінімальне марноспоживання	Так	Можлива
ITIL (Information Technology Infrastructure Library)	Управління послугами ІТ	Забезпечення якісних ІТ-послуг	Забезпечення належного рівня сервісу, Ефективність процесів	Частково	Так
Capability Maturity Model (CMM)	Розробка та підтримка	Зрілість процесів розробки ПЗ	Зрілість процесів, Продуктивність	Не прямо спрямовано	Є процеси зрілості

В праці [10] порушується проблема, щодо неспроможності передбачити в моделях якості умови експлуатації в яких перебуватимуть ПС: моделі якості можуть не враховувати всі можливі умови реального використання системи, що призводить до недоліків у функціональності або ефективності.

Про дану проблему також згадується в праці [11] в якій вказується, що вона може призвести до недоліків у функціональності, або ефективності ПС в умовах її експлуатації. В межах вирішення цієї проблеми згідно поглядів, які наведені в [10–11] важливо застосовувати методології та практики, які сприя-

ють адаптації програмного забезпечення до різних умов експлуатації: наприклад, Agile-підходи передбачають ітеративний розвиток програмного забезпечення та зміну відповідно до змін у вимогах користувачів або умовах експлуатації. Також важливо використовувати тестування з реальними умовами, або тестування на сценаріях, яке відображає реальні ситуації використання системи. Також доцільно зважати на те, що вирішення зазначеної проблеми потребує налагодження додаткової, комунікації з користувачами та стейкхолдерами може допомогти зрозуміти реальні очікування та умови експлуатації системи, що дозволить врахувати їх у моделях якості та в процесі розробки. Такий підхід сприяє покращенню функціональності та ефективності програмного забезпечення в умовах його реального використання.

В праці [12] відмічаються проблеми з масштабованістю: Деякі моделі якості можуть бути непридатними для масштабування, особливо при рості розміру та складності програмної системи. Для вирішення цієї проблеми необхідно розробляти та використовувати моделі якості, які можуть ефективно працювати на різних рівнях масштабу, від невеликих проєктів до великих розподілених систем. Це може включати в себе розробку або адаптацію моделей, які забезпечують гнучкість та можливість розширення, щоб вони могли адаптуватися до зростаючих потреб системи.

Автори праць [12–13] наголошують, що досить важливо враховувати масштабованість в процесі розробки та впровадження моделей якості. Це означає, що моделі повинні бути легко впроваджуватися та масштабуватися разом з ростом системи без великих зусиль зі змінами або модифікаціями. Загалом, для успішного вирішення проблеми масштабованості моделей якості важливо приділяти увагу їх архітектурі та гнучкості, щоб вони могли ефективно функціонувати в умовах зростання розміру та складності програмної системи.

В праці [14] підкреслюється проблематика, щодо «нестабільності вимог якості»: Вимоги до якості можуть змінюватися протягом життєвого циклу проєкту, і моделі можуть стати застарілими або непридатними для нових умов. Для вирішення цієї проблеми важливо використовувати гнучкі методології розробки програмного забезпечення, які дозволяють легко вносити зміни у вимоги та моделі якості протягом життєвого циклу проєкту. Наприклад, Agile-підходи передбачають ітеративний розвиток та постійне вдосконалення, що дозволяє адаптувати вимоги та моделі якості до змін у вимогах бізнесу або умовах ринку.

Згідно з [15] в межах піднятої вище проблеми виникає необхідність в забезпеченні підтримання постійного моніторингу та оновлення моделей якості, щоб вони відповідали актуальним вимогам та умовам. Це може включати в себе регулярну перевірку та оцінку моделей якості, а також внесення необхідних змін та коригувань. Загалом, для успішного вирішення проблеми «нестабільності вимог якості» важливо мати гнучкість у розробці та управлінні вимогами, а також постійно оновлювати та підтримувати актуальні моделі якості.

В праці [5] підкреслюється проблематика відсутності однозначних метрик якості: Визначення якості може бути суб'єктивним, і відсутність чітких метрик може ускладнити оцінку якості програмної системи: порівняння якості між різними системами, або версіями однієї системи. Автори вищезазначеної праці наголошують на тому, що для вирішення цієї проблеми важливо розробляти та застосовувати стандартизовані метрики якості, які були б об'єктивними та відображали б реальні характеристики програмного забезпечення. Такі метрики можуть включати в себе показники продуктивності, ефективності, надійності, безпеки, інтерфейсу користувача тощо. З даного приводу важливо враховувати контекст використання програмного забезпечення при визначенні метрик якості.

Згідно з [7] одні й ті ж метрики можуть мати різне значення для різних типів програмних продуктів або для різних галузей застосування. Наприклад, для веб-додатків можуть бути важливими метрики швидкодії, часу завантаження сторінок, частоти відмов, а для програмного забезпечення в області критичних застосувань – метрики надійності та безпеки. Загалом, розробка і використання об'єктивних та стандартизованих метрик якості є важливою складовою управління якістю програмного забезпечення і дозволяє об'єктивно оцінювати та порівнювати рівень якості різних систем.

В праці [14] підкреслюється проблематика недостатності моніторингу у реальному часі: Відсутність засобів моніторингу та аналізу в реальному часі може призвести до затримок в виявленні та виправленні проблем, що може погіршити якість та надійність програмного продукту. Для вирішення цієї проблеми важливо використовувати засоби моніторингу та аналізу, які дозволяють виявляти проблеми в реальному часі або навіть передбачати їх виникнення на основі аналізу даних. Наприклад, системи моніторингу продуктивності, навантаження та відмов можуть допомогти виявляти проблеми в роботі системи та реагувати на них негайно. Також важливо використовувати автоматизовані засоби тестування та контролю якості, які дозволяють проводити тестування та аналіз результатів в реальному часі. Це дозволяє оперативно виявляти проблеми та вносити необхідні корективи ще на ранніх етапах розробки або в етапі експлуатації. Загалом, моніторинг у реальному часі є ключовою складовою управління якістю програмного забезпечення, оскільки дозволяє швидко реагувати на виявлені проблеми та забезпечує підтримку високої якості та надійності програмного продукту.

В праці [15] особливої уваги заслуговують проблеми з безпекою: моделі якості можуть не враховувати аспекти безпеки, що може призводити до вразливостей та забезпечувати недостатню захист від атак. Для вирішення цієї проблеми важливо включати аспекти безпеки в моделі якості та процеси управління якістю. Це може включати аудит безпеки, тестування на вразливості, перевірку безпеки на ранніх етапах розробки, а також впровадження засобів захисту в програмне забезпечення. Також важливо враховувати конкретні потенційні загрози та вразливості для програмного забезпечення у відповідній галузі або контексті використання. Це дозволить розробникам та управлінцям якості ефективно оцінювати ризики та вживати відповідні заходи забезпечення безпеки. Загалом, безпека програмного забезпечення повинна бути важливою складовою будь-якої моделі якості, і вона повинна бути врахована на всіх етапах розробки та використання програмного продукту.

Автори праці [13] звертають увагу на проблему недостатності врахування користувацького досвіду: В деяких випадках моделі можуть недооцінювати важливість користувацького досвіду, що може впливати на прийняття програмної системи користувачами. Для вирішення цієї проблеми важливо включати аспекти користувацького досвіду в моделі якості та процеси управління якістю. Це може включати оцінку зручності використання, швидкості реакції інтерфейсу, відповідність функціональності потребам користувачів та інші аспекти, що впливають на задоволеність та прийняття програмного продукту. Також важливо залучати користувачів до процесу розробки та тестування програмного забезпечення, щоб отримати зворотний зв'язок щодо їхніх потреб та вимог до користувацького досвіду. Це дозволить розробникам налагодити програмний продукт так, щоб він краще відповідав очікуванням та потребам користувачів. Загалом, врахування користувацького досвіду у моделях якості та процесах управління якістю є ключовим для забезпечення успішного прийняття та використання програмного забезпечення користувачами.

Автори праці [12] окрім вище зазначених проблем також акцентують наукову увагу на проблемі неспроможності враховувати контекст: моделі якості можуть не завжди враховувати контекст використання програмної системи, що призводить до втрати реалізму в оцінці її якості. Це означає, що деякі моделі якості можуть не достатньо, або взагалі не враховувати особливості середовища, в якому програмна система буде використовуватися, що може призводити до втрати реалізму в оцінці її якості. Для вирішення цієї проблеми важливо розробляти моделі якості, які були б призначені для конкретних контекстів використання програмного забезпечення. Це може включати в себе адаптацію існуючих моделей до специфічних умов або розробку нових моделей, які враховують особливості конкретного домену або індустрії. Крім того, важливо збирати та аналізувати дані про реальне використання програмного забезпечення, щоб зрозуміти його характеристики та вимоги в конкретному контексті. Це дозволить розробникам та управлінцям якістю зробити більш об'єктивну оцінку якості програмного продукту і прийняти відповідні заходи для його поліпшення. Загалом, врахування контексту використання є важливим аспектом при розробці та оцінці якості програмного забезпечення, і ця проблема потребує уваги, як у наукових дослідженнях, так і в практичній роботі з програмними системами.

Згідно з результатами аналізу праць [1–15] оцінка якості програмних систем може включати в себе різні аспекти, і існує кілька міжнародних стандартів, які можуть бути використані для цього. Зазвичай, ці стандарти визначають загальні принципи оцінки якості та надають рамки для впровадження методів оцінки. Даний метод оцінки якості може бути включений у ряд стандартів, таких як:

- ISO/IEC 9126: Software Engineering –Product Quality: Цей стандарт визначає модель якості програмного забезпечення та надає метрики для вимірювання якості в аспектах, таких як функціональність, ефективність, надійність і т. д.;

- ISO/IEC 25010: Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models: Цей стандарт є оновленою версією ISO/IEC 9126 та надає більш сучасну модель якості програмного забезпечення, включаючи аспекти, такі як сумісність та безпека;

- IEEE Std 730: Software Quality Assurance Processes: Стандарт визначає процеси забезпечення якості програмного забезпечення і може включати стратегії тестування, такі як юніт-тестування.;

- IEEE Std 829: IEEE Standard for Software Test Documentation: Цей стандарт визначає вимоги до документації тестування, що може бути використано для оцінки якості тестування, включаючи юніт-тестування.;

- ISO/IEC 33001: Process Assessment – Concepts and Vocabulary: Стандарт надає концепції та терміни, пов'язані з оцінкою процесів розробки програмного забезпечення, які включають у себе тестування та методи оцінки якості.;

- ISO/IEC 29119: Software and systems engineering – Software testing: Це набір стандартів, який визначає вимоги до процесів та управління тестуванням програмного забезпечення.

В загальному спектрі наведені вище стандарти визначають фундаментальні принципи оцінки якості та надають рамки для впровадження методів оцінки. Інтеграція цих методів оцінки у різні стандарти дозволяє більш повно і системно оцінювати якість програмного забезпечення на всіх етапах його життєвого

циклу. Комбінована модель дозволяє врахувати специфіку кожного конкретного проекту шляхом адаптації ваг кожної метрики в залежності від його потреб та характеристик. Математично це виражається через можливість зміни ваг для кожної метрики у формулі оцінки. Відповідно [12] кожна метрика якості вказує на певний аспект програмного продукту, що допомагає виявити недоліки та проблеми. Математично це виражається через аналіз показників метрик та їх порівняння з прийнятними стандартами або поріговими значеннями.

2. Постановка завдання. Завдання полягає в розробці комбінованої системної моделі оцінки якості програмного продукту, яка базується на інтеграції різних моделей якості, таких як CMMI, IEEE 730, Agile Testing Quadrants, Six Sigma, TQM, SPICE та TOGAF, з метою забезпечення комплексного та повного оцінювання якості продукту. Модель передбачає використання ряду метрик, таких, як частота виникнення помилок, час відгуку, використання пам'яті, пропускна здатність, зручність використання та безпека, які оцінюються на різних етапах розробки та експлуатації програмного продукту. Узагальнена ідея постановки даного завдання передбачає створення моделі, яка буде враховувати особливості кожної з використаних моделей та метрик, забезпечуючи об'єктивне оцінювання якості програмного продукту з урахуванням вимог користувача та відповідності стандартам якості. Вище зазначена постановка завдання визначає потребу в розробці комбінованої системної моделі оцінки якості програмного продукту, яка базується на інтеграції різноманітних моделей та метрик якості з різних наукових областей.

Формування вирішення даного завдання є досить важливим з ряду наукових та практичних причин, а саме:

- Мультидисциплінарний підхід: узагальнена потреба в узагальненій підході, який буде базуватися на інтеграції різних моделей та метрик, враховує різноманітність аспектів якості програмного продукту, таких як функціональність, продуктивність, зручність використання та безпека. Це дозволяє розглядати якість з різних точок зору та забезпечує більш повне оцінювання;

- Використання передових практик: Інтеграція таких відомих моделей як CMMI, Six Sigma, TQM та TOGAF дозволяє використовувати передові методик та практики управління якістю та розробки програмного забезпечення. На практиці це забезпечує високий рівень якості в розробці програмних продуктів та їх відповідності числених стандартів якості;

- Комплексний підхід до вимірювання якості: потреба в застосуванні метрик, таких, як частота виникнення помилок, час відгуку, використання пам'яті, пропускна здатність тощо, враховують різні аспекти якості, такі як надійність, продуктивність та ефективність використання ресурсів;

- Відповідність науковим стандартам: Розробка комбінованої системної моделі ґрунтується на наукових дослідженнях та теоріях у галузі управління якістю та інформаційних технологій, що забезпечує відповідність вимогам наукової області та підвищує довіру до результатів оцінювання.

Обґрунтування доцільності розроблення комбінованої моделі зводиться до її переваг, а саме:

- Комплексний підхід до якості: Поєднання різних методик та стандартів дозволяє охопити різні аспекти якості програмного продукту, включаючи процеси розробки, тестування, управління якістю та архітектурні вимоги;

- Використання найкращих практик: Включення таких широко визнаних методик, як CMMI, Six Sigma, Agile Testing Quadrants тощо, дозволяє використовувати найкращі практики відповідно до конкретних потреб та характеристик проекту;

- Гнучкість та адаптивність: Модель може адаптуватися до різних типів проектів та специфічних потреб команди розробників. Ваги кожного з методик можуть змінюватися в залежності від контексту;

- Постійне поліпшення: Використання методик Total Quality Management (TQM), Six Sigma та SPICE дозволяє постійно вдосконалювати процеси розробки та управління якістю, що сприяє підвищенню якості програмного продукту;

- Об'єктивність оцінки: Включення різних метрик та стандартів дозволяє забезпечити більш об'єктивну оцінку якості програмного продукту та процесів його розробки.

Отже постановка завдання визначає потребу, щодо створення високоефективної та науково обґрунтованої моделі оцінки якості програмного продукту, яка враховує різноманітність вимог та стандартів якості.

3. Розробка методу. В межах розробки комбінаційної моделі була задіяна комбінація наступних моделей: CMMI (Capability Maturity Model Integration), IEEE 730 (Software Quality Assurance Processes), Agile Testing Quadrants, Agile Testing Quadrants, Six Sigma, TQM (Total Quality Management), SPICE (Software Process Improvement and Capability Determination) та TOGAF (The Open Group Architecture Framework).

В запропонованій комбінованій моделі передбачається застосування наступних метрик:

- Частота виникнення помилок (Error Rate): Цю метрику можна застосувати на будь-якому етапі розробки та використання програмного продукту, але особливо важливо виміряти її під час тестування та експлуатації для виявлення недоліків та вдосконалення якості [5];

- Час відгуку (Response Time): Цю метрику можна виміряти на етапах тестування та використання для оцінки продуктивності та швидкодії програмного продукту [7];
- Використання пам'яті (Memory Usage): Вимірювання використання пам'яті зазвичай проводиться під час тестування та використання програмного продукту для визначення ефективності використання ресурсів [4];
- Пропускна здатність (Throughput): Ця метрика зазвичай оцінюється під час тестування програмного продукту для визначення його продуктивності та швидкодії під навантаженням [9];
- Зручність використання (Usability): Оцінка зручності використання зазвичай проводиться на етапі дизайну та тестування для забезпечення зручного та інтуїтивно зрозумілого інтерфейсу користувача [10];
- Безпека (Security): Оцінка безпеки може бути важливою на будь-якому етапі розробки, але особливо на етапах аналізу вимог, розробки та тестування для забезпечення захисту від зловмисних атак та вразливостей [13].

Представимо повну комбіновану модель оцінки якості програмного продукту з використанням вказаних методик та стандартів. Для кращого розуміння представимо модель у вигляді модулів для кожного етапу розробки та експлуатації програмного продукту:

- ❖ Етапи розробки:
 - Вимоги та архітектура:
 - CMMI: Використання процесів забезпечення якості (QA) для визначення вимог та архітектури.
 - TOGAF: Використання архітектурного підходу для розробки архітектури ПЗ.
 - Проектування та розробка:
 - Six Sigma: Використання методів для мінімізації дефектів та вдосконалення процесів розробки.
 - SPICE: Використання процесів забезпечення якості для розробки ПЗ.
- Тестування та QA:
 - Agile Testing Quadrants: Використання різних видів тестування для забезпечення високої якості ПЗ.
 - IEEE 730: Визначення процесів тестування та QA.
 - ❖ Етапи експлуатації:
 - Впровадження та підтримка:
 - TQM: Впровадження стратегій управління якістю для підтримки та поліпшення програмного продукту під час експлуатації.
 - SPICE: Використання методів оцінки якості під час експлуатації для постійного поліпшення програмного продукту.
 - Цикли оцінювання якості ПЗ:
 - Під час розробки:
 - Використання Agile Testing Quadrants для тестування на кожному етапі розробки.
 - Проведення аудитів з використанням CMMI для визначення рівня зрілості процесів.
 - Під час експлуатації:
 - Використання TQM для постійного вдосконалення програмного продукту під час його експлуатації.
 - Впровадження моніторингу та аналізу даних з використанням Six Sigma для виявлення та виправлення проблем.

Математично застосування вказаних метрик в комбінованій моделі може бути обґрунтоване через їхню спроможність забезпечити об'єктивність, комплексність оцінки, врахування специфіки проекту та виявлення недоліків та проблем програмного продукту. Математично підходи до оцінки якості наведено в формулах (1– 11.):

$$Q_{CMMI} = \sum_{j=1}^{M_{CMMI}} (w_{CMMI_j} \times Q_{CMMI_j}), \quad (1)$$

де: Q_{CMMI} – це оцінка якості ПЗ за моделлю CMMI; w_{CMMI_j} – вага підкритерію j для моделі CMMI; Q_{CMMI_j} – оцінка підкритерію j для моделі CMMI; M_{CMMI} – підкритерії моделі CMMI.

$$Q_{IEEE730} = \sum_{j=1}^{M_{IEEE730}} (w_{IEEE730_j} \times Q_{IEEE730_j}), \quad (2)$$

де: $Q_{IEEE730}$ – це оцінка якості ПЗ за стандартом оцінки якості IEEE730; $w_{IEEE730_j}$ – вага підкритерію j для моделі за стандартом оцінки якості IEEE730; $Q_{IEEE730_j}$ – оцінка підкритерію j для моделі за стандартом оцінки якості IEEE730; $M_{IEEE730}$ – підкритерії моделі за стандартом оцінки якості IEEE730.

$$Q_{AgileTesting} = \sum_{j=1}^{M_{AgileTesting}} (w_{AgileTesting_j} \times Q_{AgileTesting_j}), \quad (3)$$

де: $Q_{AgileTesting}$ – це оцінка якості ПС за Agile Testing Quadrants; $w_{AgileTesting_j}$ – вага підкритерію j для моделі згідно з Agile Testing Quadrants; $Q_{AgileTesting_j}$ – оцінка підкритерію j для моделі оцінки якості ПС згідно з Agile Testing Quadrants; $M_{AgileTesting}$ – підкритерії моделі згідно з Agile Testing Quadrants.

$$Q_{SixSigma} = \sum_{j=1}^{M_{SixSigma}} (w_{SixSigma_j} \times Q_{SixSigma_j}), \quad (4)$$

де: $Q_{SixSigma}$ – це оцінка якості ПС за методологією Six Sigma; $w_{SixSigma_j}$ – вага підкритерію j для моделі оцінки якості ПС згідно з засадами Six Sigma; $Q_{SixSigma_j}$ – оцінка підкритерію j для моделі оцінки якості ПС згідно з методологією Six Sigma; $M_{SixSigma}$ – підкритерії моделі згідно з Six Sigma.

$$Q_{TQM} = \sum_{j=1}^{M_{TQM}} (w_{TQM_j} \times Q_{TQM_j}), \quad (5)$$

де: Q_{TQM} – це оцінка якості ПС за Total Quality Management; w_{TQM_j} – вага підкритерію j для моделі оцінки якості ПС згідно з засадами Total Quality Management; Q_{TQM_j} – оцінка підкритерію j для моделі оцінки якості ПС згідно з Total Quality Management; M_{TQM} – підкритерії моделі згідно з Total Quality Management.

$$Q_{SPICE} = \sum_{j=1}^{M_{SPICE}} (w_{SPICE_j} \times Q_{SPICE_j}), \quad (6)$$

де: Q_{SPICE} – це оцінка якості ПС згідно з засад SPICE (Software Process Improvement and Capability Determination); w_{SPICE_j} – вага підкритерію j для моделі оцінки якості ПС згідно з засадами SPICE; Q_{SPICE_j} – оцінка підкритерію j для моделі оцінки якості ПС згідно з SPICE; M_{SPICE} – підкритерії моделі згідно з SPICE.

$$Q_{TOGAF} = \sum_{j=1}^{M_{TOGAF}} (w_{TOGAF_j} \times Q_{TOGAF_j}), \quad (7)$$

де: Q_{TOGAF} – це оцінка якості ПС згідно з засад TOGAF (The Open Group Architecture Framework); w_{TOGAF_j} – вага підкритерію j для моделі оцінки якості ПС згідно з засадами TOGAF; Q_{TOGAF_j} – оцінка підкритерію j для моделі оцінки якості ПС згідно з TOGAF; M_{TOGAF} – підкритерії моделі згідно з TOGAF.

Загальна оцінка якості розробленої комбінованої моделі оцінки якості ПС буде сумою оцінок кожної моделі, помноженої на її вагу та розраховуватиметься згідно (8):

$$Q = w_{CMMI} \times Q_{CMMI} + w_{IEEE730} \times Q_{IEEE730} + w_{AgileTesting} \times Q_{AgileTesting} + w_{SixSigma} \times Q_{SixSigma} + w_{TQM} \times Q_{TQM} + w_{SPICE} \times Q_{SPICE} + w_{TOGAF} \times Q_{TOGAF}, \quad (8)$$

Комбінована оцінка якості $EQ_{комб.і}$ розраховується шляхом врахування оцінки ефективності та впливу для кожного етапу розробки та використання ПС у відповідності до (9):

$$EQ_{комб.і} = w_e \times E_i + w_i \times I_i, \quad (9)$$

де: $EQ_{комб.і}$ – це комбінована оцінка якості із врахуванням оцінки ефективності та впливу для кожного етапу розробки та використання ПС; w_e та w_i – ваги ефективності та впливу відповідно, які визначаються експертно або на основі аналізу даних які надходять із спеціальних програмних застосунків із оцінювання якості ПС.; M_{TOGAF} – підкритерії моделі згідно з TOGAF.

В даному разі до спеціальних програмних застосунків із оцінювання якості ПС відносимо:

– Project Management Software (PM): Програми для управління проектами, такі як Microsoft Project, Jira, Asana, Trello тощо, можуть збирати дані про виконання завдань та календарний графік. Ці дані можуть бути використані для аналізу впливу різних методик на продуктивність та результативність проекту;

– Software Testing Tools: Інструменти для тестування програмного забезпечення, такі як Selenium, JUnit, TestRail тощо, зазвичай надають детальні дані про результати тестування, включаючи кількість та тип дефектів. Ці дані можуть бути використані для оцінки впливу методик тестування на якість продукту;

– Version Control Systems (VCS): Системи контролю версій, такі як Git, SVN, Mercurial тощо, зберігають історію змін коду. Ці дані можуть бути використані для аналізу ефективності розробки та виявлення зв'язку між використанням різних методик та якістю коду;

– Quality Management Software (QMS): Програми для управління якістю, такі як Qualityze, MasterControl, Sparta Systems тощо, можуть надавати інструменти для збору та аналізу даних про якість та впровадження різних методик та стандартів управління якістю;

– Business Intelligence Tools (BI): Інструменти бізнес-аналітики, такі як Tableau, Power BI, Google Data Studio тощо, можуть бути використані для аналізу даних з різних джерел та створення звітів та візуалізації результатів аналізу.

Для врахування інтеграції з процесом розробки, візуалізації результатів та стратегій управління якістю у нашій комбінованій моделі оцінки ефективності та впливу використання моделей якості застосуються наступні підходи:

1. Модифікуємо нашу комбіновану оцінку $EQ_{комб.і.}$ додаючи член, що відображає наявність API яка застосовуватиметься для автоматизованої оцінки якості на різних етапах розробки ПС (10):

$$EQ_{комб.і.} = \frac{1}{N} \sum_{i=1}^N (w_{адаптовані} \times M_i) \times p_j \times API_i, \quad (10)$$

де: API_i – параметр, який відображає наявність API для інтеграції моделі якості API_i i з процесом розробки; M_i – оцінка якості, отримана за допомогою моделі i ; p_j – рівень застосовності моделі до проекту j ; $w_{адаптовані}$ – адаптовані ваги кожної моделі (моделі, які були включені в комбіновану модель), які можуть змінюватися в залежності від контексту проекту; N – кількість проектів.

Відповідно в межах інтеграції з процесом розробки формула (10) дозволяє урахувати гнучкість, різноманітність методів оцінки та застосовність до різних проектів у комбінованій моделі оцінки якості програмного продукту.

2. Модифікуємо нашу комбіновану оцінку $EQ_{комб.і.}$ додаючи параметр, який відображає рівень візуалізації результатів оцінки якості для моделі (10):

$$EQ_{комб.і.} = \frac{1}{N} \sum_{i=1}^N (w_{адаптовані} \times M_i) \times p_j \times T_{Віз.іj}, \quad (11)$$

де: $T_{Віз.іj}$ – параметр, який відображає рівень візуалізації результатів оцінки якості для моделі.

3. Включимо в комбіновану оцінку $EQ_{комб.і.}$ врахування застосування стратегії управління якістю на основі засад включення коефіцієнту стратегії управління якістю ($T_{Стр.іj}$) для проекту та коефіцієнта візуалізації результатів (віз) для i -ї метрики на проекті можуть бути сформовані з урахуванням різних факторів (12):

$$EQ_{комб.і.} = \frac{1}{N} \sum_{i=1}^N (w_{адаптовані} \times M_i \times Q_{ij}) \times p_j \times API_i \times T_{Віз.іj} \times T_{Стр.іj}, \quad (12)$$

де: $T_{Стр.іj}$ – коефіцієнт стратегії управління якістю.

Коефіцієнт стратегії управління якістю може бути сформований на основі особливостей та вимог конкретного проекту [11]. Наприклад, якщо проект вимагає великої уваги до якості та неперервного моніторингу, коефіцієнт може бути вищим. Це може бути числове значення, що відображає рівень важливості управління якістю для проекту. Згідно [14] при оцінці ризиків коефіцієнт візуалізації результатів для конкретної метрики може бути сформований на основі оцінки ризиків. Згідно [4,6] якщо певна метрика відіграє критичну роль у проекті та має великий вплив на його успішність, коефіцієнт візуалізації може бути вищим. Згідно [11] залучення експертів у галузі керування якістю та візуалізації результатів може допомогти сформувати адекватні коефіцієнти. Експерти можуть враховувати різні аспекти проекту та метрик якості для визначення оптимальних значень цих коефіцієнтів. Отже, коефіцієнт стратегії управління якістю та коефіцієнт візуалізації результатів формуються на основі аналізу із застосуванням метрик якості. Застосування вказаних метрик якості в комбінованій моделі може бути обґрунтоване математично з точки зору досягнення об'єктивної та комплексної оцінки якості програмного продукту. Комбінування різних метрик якості дозволяє забезпечити об'єктивність оцінки, оскільки кожна метрика вимірює конкретний аспект якості. Математично це виражається через розрахунок середнього значення або вагового середнього значення метрик для отримання загального показника якості. Використання різних метрик дозволяє оцінити якість програмного продукту з різних точок зору, що забезпечує комплексність оцінки. Математично це виражається через включення різних метрик у формулу для комбінованої оцінки якості. Загалом, подібна комбінована модель допомагає забезпечити високу якість програмного продукту, оптимізувати процеси розробки та управління якістю, а також забезпечити відповідність стандартам та вимогам клієнтів.

Висновки

1. Кожна модель якості має свої унікальні особливості, які можуть бути корисними на різних етапах розробки та використання програмних систем. Відповідно вибір моделі якості повинен залежати від конкретних потреб та характеристик проекту. Інтеграція моделей якості з процесами розробки може допомогти забезпечити більш ефективну та якісну розробку програмного забезпечення. Хоч дослідження в області застосування моделей якості в розробці та використанні програмних систем відбувається постійно, і багато проблем вже мають вирішення, проте також існують ті, які залишаються відкритими.

2. Математично застосування метрик якості в комбінованій моделі може бути обґрунтоване через їхню спроможність забезпечити об'єктивність, комплексність оцінки, врахування специфіки проекту та виявлення недоліків та проблем програмного продукту.

3. Запропонована комбінована модель дозволяє використовувати найкращі практики та методики з кожної з вказаних областей для забезпечення високої якості програмного продукту на кожному етапі його життєвого циклу.

Список літератури

- [1] H. Foidl and M. Felderer, "Integrating software quality models into risk-based testing," *Software Quality Journal*, vol. 26, pp. 809–847, 2018.
- [2] K. Sahu and R. K. Srivastava, "Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.
- [3] K. Sahu, F. A. Alzahrani, R. K. Srivastava, and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.
- [4] S. Sackey, D. E. Lee, and B. S. Kim, "Duration Estimate at Completion: Improving Earned Value Management Forecasting Accuracy," *KSCE Journal of Civil Engineering*, vol. 24, no. 3, pp. 693–702, 2020. DOI: 10.1007/s12205-020-0407-5
- [5] P. Sharma and A. L. Sangal, "Building and Testing a Fuzzy Linguistic Assessment Framework for Defect Prediction in ASD Environment Using Process-Based Software Metrics," *Arabian Journal of Science and Engineering*, vol. 45, no. 12, pp. 10327–10351, 2020.
- [6] Y. Hassouneh et al., "Boosted Whale Optimization Algorithm With Natural Selection Operators for Software Fault Prediction," *IEEE Access*, vol. 9, pp. 14239–14258, 2021. DOI: 10.1109/ACCESS.2021.3052149.
- [7] R. Al-Qutaish, "Quality Models in Software Engineering Literature: An Analytical and Comparative Study," *Journal of American Science*, vol. 6, pp. 10, 2010.
- [8] J. Estdale and E. Georgiadou, "Applying the ISO/IEC 25010 Quality Models to Software Product," in *Systems, Software and Services Process Improvement. EuroSPI 2018*, X. Larrucea, I. Santamaria, R. O'Connor, and R. Messnarz, Eds., vol. 896, 2018, pp. 12.
- [9] O. Fonseca-Herrera, A. E. Rojas, and H. Florez, "A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard," *IAENG International Journal of Computer Science*, vol. 48, pp. 213, 2021.
- [10] M. N. Aziz, I. M. Saptia, and S. Rochimah, "Security Characteristic Evaluation Based on ISO/IEC 25023 Quality Model, Case Study: Laboratory Management Information System," in *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, IEEE, pp. 332–336.
- [11] J.-X. Chen, "Overall performance evaluation: new bounded DEA models against unreachability of efficiency," *The Journal of the Operational Research Society*, vol. 65, no. 7, pp. 1120–1132, 2014.
- [12] M. Filz, C. Herrmann, and S. Thiede, "Simulation-based Assessment of Quality Inspection Strategies on Manufacturing Systems," *Procedia CIRP*, vol. 93, pp. 777–782, 2020.
- [13] A. Golabchi, S. Han, and S. AbouRizk, "A simulation and visualization-based framework of labor efficiency and safety analysis for prevention through design and planning," *Automation in Construction*, vol. 96, pp. 310–323, 2018.
- [14] P. Han, L. Wang, and P. Song, "Doubly robust and locally efficient estimation with missing outcomes," *Statistica Sinica*, vol. 26, no. 2, pp. 691–719, 2016.
- [15] L. Hund, B. Schroeder, K. Rumsey, and G. Huerta, "Distinguishing between model- and data-driven inferences for high reliability statistical predictions," *Reliability Engineering and System Safety*, vol. 180, pp. 201–210, 2018.

Стаття надійшла: 21.03.2024

References

- [1] Foidl, H., & Felderer, M. (2018). Integrating software quality models into risk-based testing. *Software Quality Journal*, 26(2018), 809–847.
- [2] Sahu, K., & Srivastava, R. K. (2021). Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective. *Advances in Mathematics: Scientific Journal*, 10(1), 543–555.
- [3] Sahu, K., Alzahrani, F. A., Srivastava, R. K., & Kumar, R. (2021). Evaluating the impact of prediction techniques: Software reliability perspective. *Computers, Materials & Continua*, 67(2), 1471–1488.
- [4] Sackey, S., Lee, D. E., & Kim, B. S. (2020). Duration Estimate at Completion: Improving Earned Value Management Forecasting Accuracy. *KSCE Journal of Civil Engineering*, 24(3), 693–702. <https://doi.org/10.1007/s12205-020-0407-5>
- [5] Sharma, P., & Sangal, A. L. (2020). Building and Testing a Fuzzy Linguistic Assessment Framework for Defect Prediction in ASD Environment Using Process-Based Software Metrics. *Arabian Journal of Science and Engineering*, 45(12), 10327–10351.
- [6] Hassouneh, Y., Turabieh, H., Thaher, T., Tumar, I., Chantar, H., & Too, J. (2021). Boosted Whale Optimization Algorithm With Natural Selection Operators for Software Fault Prediction. *IEEE Access*, 9, 14239–14258. <https://doi.org/10.1109/ACCESS.2021.3052149>
- [7] Al-Qutaish, R. (2010). Quality Models in Software Engineering Literature: An Analytical and Comparative Study. *Journal of American Science*, 6, 10.
- [8] Estdale, J., & Georgiadou, E. (2018). Applying the ISO/IEC 25010 Quality Models to Software Product. In X. Larrucea, I. Santamaria, R. O'Connor, & R. Messnarz (Eds.), *Systems, Software and Services Process Improvement. EuroSPI 2018. Communications in Computer and Information Science* (Vol. 896, pp. 1-12).
- [9] Fonseca-Herrera, O., Rojas, A. E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, 48, 213.
- [10] Aziz, M. N., Sapta, I. M., & Rochimah, S. (2018). Security Characteristic Evaluation Based on ISO/IEC 25023 Quality Model, Case Study: Laboratory Management Information System. In 2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS) (pp. 332–336). IEEE.
- [11] Chen, J.-X. (2014). Overall performance evaluation: new bounded DEA models against unreachability of efficiency. *The Journal of the Operational Research Society*, 65(7), 1120–1132.
- [12] Filz, M., Herrmann, C., & Thiede, S. (2020). Simulation-based Assessment of Quality Inspection Strategies on Manufacturing Systems. *Procedia CIRP*, 93, 777–782.
- [13] Golabchi, A., Han, S., & AbouRizk, S. (2018). A simulation and visualization-based framework of labor efficiency and safety analysis for prevention through design and planning. *Automation in Construction*, 96, 310–323.
- [14] Han, P., Wang, L., & Song, P. (2016). Doubly robust and locally efficient estimation with missing outcomes. *Statistica Sinica*, 26(2), 691–719.
- [15] Hund, L., Schroeder, B., Rumsey, K., & Huerta, G. (2018). Distinguishing between model- and data-driven inferences for high reliability statistical predictions. *Reliability Engineering and System Safety*, 180, 201–210.

Відомості про авторів

Шантыр Антон Сергійович – кандидат технічних наук, доцент кафедри Штучного інтелекту ДУІКТ

Shantyr Anton – candidate of technical sciences, associate professor of the Department of artificial intelligence SUICT

A. S. Shantyr

SPECIFICS OF QUALITY ASSESSMENT MODELS APPLICATION AT DEVELOPMENT AND USE STAGES OF SOFTWARE SYSTEMS

State University of Information and Communication Technologies, Kyiv

УДК 519.6

В.П. Карашецький, В.І. Яркун

РОЗРАХУНОК ТРИВИМІРНИХ СТАЦІОНАРНИХ ПОТЕНЦІАЛЬНИХ ТЕПЛОВИХ ПОЛІВ МЕТОДОМ СКІНЧЕННИХ ЕЛЕМЕНТІВ

Національний лісотехнічний університет України, Львів

Анотація. У статті описано чіткий алгоритм формування системи нелінійних алгебраїчних рівнянь виходячи з мінімуму функціонала для розрахунку розподілу температури в тривимірній області з безгістерезисними нелінійними анізотропними середовищами. Сформульовано крайову задачу розрахунку тривимірного стаціонарного потенціального температурного поля. Побудовано скінченно-елементну модель розрахунку розподілу температури всередині тривимірної області, заповненої безгістерезисними нелінійними анізотропними середовищами. Виведені основні формули методу скінчених елементів для крайової задачі розрахунку тривимірних стаціонарних потенціальних теплових полів в областях з безгістерезисними нелінійними анізотропними середовищами використовуючи лагранжеві тетраедри 1 – 4 порядків в якості скінчених елементів, та кубатурні формули чисельного інтегрування за об'ємом лагранжевого тетраедра. Запропоновано алгоритм визначення вкладу скінченного елемента у вектор нев'язок та матрицю Якобі нелінійної системи рівнянь, яку розв'язують методом Ньютона використовуючи елементи тензора диференціальної теплопровідності середовища. Застосовано кубатурну формулу чисельного інтегрування за об'ємом лагранжевого тетраедра на базі інтерполяційного повного поліному для лагранжевого тетраедра першого порядку. Даний алгоритм придатний при використанні лагранжевих скінчених елементів другого, третього та четвертого порядків із застосуванням відповідних кубатурних формул чисельного інтегрування за об'ємом лагранжевого тетраедра. Наведено формули для обчислення тензорів диференціальної теплопровідності для нелінійного ізотропного та лінійного середовищ. Описані граничні умови Діріхле (першого роду), Неймана (другого роду), третього і четвертого роду та їх врахування.

Ключові слова: потенціальне теплове поле, лагранжевий тетраедр, метод скінчених елементів, кубатурна формула, граничні умови, метод Ньютона.

Abstract. The article describes a clear algorithm for forming a system of nonlinear algebraic equations from the condition of the minimum of the functional to calculate the temperature distribution inside the three-dimensional domain filled with hysteresis-free nonlinear anisotropic environments. The boundary value problem of calculating the three-dimensional stationary potential temperature field is formulated. The finite element model for calculating the temperature distribution inside a three-dimensional domain filled with hysteresis-free nonlinear anisotropic environments is built. Basic formulas of the finite element method for the boundary value problem of calculating three-dimensional stationary potential thermal fields in domains filled with hysteresis-free nonlinear anisotropic environments with using Lagrangian tetrahedrons 1–4 orders as finite elements and cubature formulas of numerical integration over the volume of the Lagrangian tetrahedron are derived. The algorithm determining the contribution of each finite element to the vector of residuals and matrix Jacobi nonlinear system of equations solved by Newton's method using the elements of the tensor of the differential thermal conductivity of the environment was considered. The cubature formula of numerical integration over the volume of the Lagrangian tetrahedron based on the interpolation complete polynomial for the Lagrangian finite element of the first order was applied. This algorithm is suitable when using Lagrangian finite elements of the second, third, and fourth orders with the use of the corresponding cubature formulas for numerical integration over the volume of the Lagrangian tetrahedron. Formulas for calculating tensors of differential thermal conductivity for non-linear isotropic and linear environments are given. The boundary conditions of Dirichlet (first kind), Neumann (second kind), third and fourth kind and their consideration are described.

Keywords: potential thermal field, Lagrangian tetrahedron, finite element method, cubature formula, boundary conditions, Newton's method.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-139-145>.

Вступ

Не зважаючи на велику кількість публікацій з методу скінчених елементів (МСЕ), у них відсутній чіткий алгоритм формування системи нелінійних алгебраїчних рівнянь для розрахунку розподілу температури в тривимірній області з безгістерезисними нелінійними анізотропними середовищами.

З метою підвищення точності розрахунків актуальним завданням залишається теж використання лагранжевих тетраедрів 1 – 4 порядків в якості скінчених елементів (СЕ) [8].

Актуальність

В ході дослідження були розглянуті розв'язання деяких задач розрахунку теплових процесів МСЕ в різних пристроях [1 – 6]. Деякі з цих задач володіють геометричною симетрією, що дозволяє використовувати для їх опису дві, а не три просторові координати. Однак в багатьох задачах такої симетрії не має, тому потрібна їх тривимірна постановка [7].

Отримано формули МСЕ для крайової задачі розрахунку тривимірних стаціонарних потенціальних теплових полів в областях з безгістерезисними нелінійними анізотропними середовищами використовуючи лагранжеві тетраедри 1 – 4 порядків в якості СЕ, кубатурні формули чисельного інтегрування. Розглянуто алгоритм визначення вкладу СЕ у вектор нев'язок та матрицю Якобі нелінійної системи рівнянь, яка розв'язується методом Ньютона.

Мета

Мета роботи полягає в розробленні методики розрахунку тривимірних статичних температурних полів МСЕ, яка б дала можливість врахувати розподіл температури всередині тривимірної області, заповненої безгістерезисними нелінійними анізотропними середовищами.

Виклад основного матеріалу

Для крайової задачі розрахунку статичного потенціального теплового поля, яка описується рівняннями

$$\operatorname{div} \bar{B}(\bar{H}) = 0, \quad (1)$$

$$\bar{H} = -\operatorname{grad} U, \quad (2)$$

у тривимірній області D функціонал F представляється у вигляді

$$F = \int_V W dV, \quad (3)$$

де

$$W = \int_0^{\bar{B}} \bar{B} d\bar{H}; \quad (4)$$

U – температура в області D ; \bar{H} , \bar{B} – вектори напруженості теплового поля та густини теплового потоку в області D ; V – об'єм області D .

Оптимальний розподіл температури U у межах тривимірної області D , яка мінімізує функціонал F , дозволяє вирішити поставлену крайову задачу. Умова мінімуму функціонала (3) приймає вигляд

$$\frac{dF}{dU} = 0. \quad (5)$$

Для побудови скінченно-елементної моделі заповнимо область розрахунку D сукупністю лагранжевих тетраедрів n -го порядку [9].

Нехай внаслідок триангуляції тривимірної області D отримуємо M лагранжевих скінченних елементів. Кожному з них присвоїмо порядковий номер m ($m = \overline{1, M}$) і локальну нумерацію вузлів, згідно якої i -ому вузлу m -го СЕ відповідає номер mi . Для всієї області розрахунку встановимо сіткову (наскрізну) нумерацію R внутрішніх вузлів і G граничних вузлів. Поточні значення порядкових номерів внутрішніх вузлів позначимо r .

Для скінченно-елементної області функціонал F з урахуванням (3), (4) набуде вигляду

$$F = \sum_{m=1}^M F_m = \sum_{m=1}^M W_m, \quad (6)$$

де

$$W_m = \int_{V_m} W dv; \quad (7)$$

V_m – об'єм m -го СЕ, який визначається за координатами його вершин у прямокутній системі координат за формулою

$$V_m = \frac{1}{6} \det \begin{vmatrix} 1 & x_{m1} & y_{m1} & z_{m1} \\ 1 & x_{m2} & y_{m2} & z_{m2} \\ 1 & x_{m3} & y_{m3} & z_{m3} \\ 1 & x_{m4} & y_{m4} & z_{m4} \end{vmatrix}. \quad (8)$$

Утворимо R -мірний вектор-рядок і вектор-стовпець температури U у внутрішніх вузлах

$$\vec{U} = (U_1, \dots, U_R); \quad \vec{U}_* = (U_1, \dots, U_R)_*. \quad (9)$$

Умова мінімуму функціонала F з врахуванням (5) рівносильна нелінійній системі алгебраїчних рівнянь

$$\vec{\varphi}_*[\vec{U}_*] = \frac{dF}{d\vec{U}_*} = 0. \quad (10)$$

Застосуємо для (7) кубатурні формули чисельного інтегрування за об'ємом лагранжевого тетраедра [12]. Наприклад, для лагранжевих тетраедрів першого порядку ($n=1$), кількість вузлів у яких $p=4$, одержимо

$$F_m = \frac{1}{4} v_m \sum_{i=1}^4 W_{mi}, \quad (11)$$

де

$$W_{mi} = \int_0^{\bar{H}_{mi}} \bar{B} d\bar{H}; \quad (12)$$

Представимо залежність температури U в межах m -го СЕ повним поліномом першого степеня

$$U = \bar{U}_m k_m^{-1} \bar{k}_* = \bar{k} k_{m*}^{-1} \bar{U}_{m*}, \quad (13)$$

де

$$\bar{U}_m = (U_{m1}, \dots, U_{m4}) \quad (14)$$

– вектор-рядок значень температури U у вузлах m -го СЕ;

$$\bar{k} = (1, x, y, z) \quad (15)$$

– координатний вектор-рядок поточної точки з координатами x, y, z ;

$$k_{m*} = \begin{vmatrix} 1 & x_{m1} & y_{m1} & z_{m1} \\ 1 & x_{m2} & y_{m2} & z_{m2} \\ 1 & x_{m3} & y_{m3} & z_{m3} \\ 1 & x_{m4} & y_{m4} & z_{m4} \end{vmatrix} \quad (16)$$

– координатна матриця, рядки якої є координатними векторами вигляду (15) у вузлах m -го СЕ;

– $\bar{U}_{m*}, \bar{k}_*, k_m$ – відповідно вектори-стовпці і матриця, транспоновані по відношенню до $\bar{U}_m, \bar{k}, k_{m*}$.

В локальній прямокутній системі координат вектор \bar{H} напруженості теплового поля визначається через температуру U співвідношенням

$$\bar{H} = -\text{grad}U = -\frac{\partial U}{\partial x} \bar{i} - \frac{\partial U}{\partial y} \bar{j} - \frac{\partial U}{\partial z} \bar{k}. \quad (17)$$

Проекції H_x, H_y, H_z вектора \bar{H} в mi -ому вузлі з врахуванням (13) і (17) отримують вигляд

$$H_{xmi} = -\frac{\partial U}{\partial x} \Big|_{x_{mi}, y_{mi}, z_{mi}} = -\bar{U}_m \bar{K}_{mi}^{(x)} = -\bar{K}_{mi}^{(x)} \bar{U}_{m*}; \quad (18)$$

$$H_{ymi} = -\frac{\partial U}{\partial y} \Big|_{x_{mi}, y_{mi}, z_{mi}} = -\bar{U}_m \bar{K}_{mi}^{(y)} = -\bar{K}_{mi}^{(y)} \bar{U}_{m*}; \quad (19)$$

$$H_{zmi} = -\frac{\partial U}{\partial z} \Big|_{x_{mi}, y_{mi}, z_{mi}} = -\bar{U}_m \bar{K}_{mi}^{(z)} = -\bar{K}_{mi}^{(z)} \bar{U}_{m*}, \quad (20)$$

де

$$\bar{K}_{mi}^{(x)} = \bar{k}_{mi}^{(x)} k_{m*}^{-1}; \quad \bar{K}_{mi}^{(y)} = \bar{k}_{mi}^{(y)} k_{m*}^{-1}; \quad \bar{K}_{mi}^{(z)} = \bar{k}_{mi}^{(z)} k_{m*}^{-1}; \quad (21)$$

$$\bar{K}_{mi*}^{(x)} = k_m^{-1} \bar{k}_{mi}^{(x)}; \quad \bar{K}_{mi*}^{(y)} = k_m^{-1} \bar{k}_{mi}^{(y)}; \quad \bar{K}_{mi*}^{(z)} = k_m^{-1} \bar{k}_{mi}^{(z)}; \quad (22)$$

$$\bar{k}_{mi}^{(x)} = \frac{\partial \bar{k}}{\partial x} \Big|_{x_{mi}, y_{mi}, z_{mi}} = (0, 1, 0, 0);$$

$$\begin{aligned}\vec{k}_{mi}^{(y)} &= \frac{\partial \vec{k}}{\partial y} \Big|_{x_{mi}, y_{mi}, z_{mi} = (0,0,1,0)}; \\ \vec{k}_{mi}^{(z)} &= \frac{\partial \vec{k}}{\partial z} \Big|_{x_{mi}, y_{mi}, z_{mi} = (0,0,0,1)};\end{aligned}\quad (23)$$

$\vec{k}_{mi}^{(x)}$, $\vec{k}_{mi}^{(y)}$, $\vec{k}_{mi}^{(z)}$ – стовпці, одержані транспонуванням рядків (23).

Диференціюючи вираз (11) по вектору \vec{U}_m і враховуючи (18) – (20), одержуємо

$$\begin{aligned}\vec{\varphi}_{m^*} &= \frac{dF_m}{d\vec{U}_m} = \frac{1}{4} v_m \sum_{i=1}^4 \frac{d}{d\vec{U}_m} \int_0^{\vec{H}_{mi}} (d\vec{H}) \vec{B} = \frac{1}{4} v_m \sum_{i=1}^4 \frac{d\vec{H}_{mi}}{d\vec{U}_m} \vec{B}_{mi} = \\ &= \frac{1}{4} v_m \sum_{i=1}^4 \left(\frac{dH_{xmi}}{d\vec{U}_m} B_{xmi} + \frac{dH_{ymi}}{d\vec{U}_m} B_{ymi} + \frac{dH_{zmi}}{d\vec{U}_m} B_{zmi} \right) = \\ &= -\frac{1}{4} v_m \sum_{i=1}^4 \left(\vec{K}_{mi}^{(x)} B_{xmi} + \vec{K}_{mi}^{(y)} B_{ymi} + \vec{K}_{mi}^{(z)} B_{zmi} \right),\end{aligned}\quad (24)$$

де \vec{B}_{mi} , B_{xmi} , B_{ymi} , B_{zmi} – відповідно вектор густини теплового потоку і його складові в mi -ому вузлі, які визначаються за значеннями проєкцій (18) – (20) вектора напруженості теплового поля і характеристикою теплопровідності безгістерезисного нелінійного середовища, що виражається векторним рівнянням або трьома скалярними рівняннями

$$\vec{B} = \vec{B}[\vec{H}] \quad (25)$$

$$B_x = B_x[H_x, H_y, H_z]; \quad B_y = B_y[H_x, H_y, H_z]; \quad B_z = B_z[H_x, H_y, H_z]. \quad (26)$$

Нелінійна система рівнянь (10) розв'язується, як правило, ітераційним методом Ньютона.

Для визначення вкладу m -го СЕ в систему рівнянь (10) необхідно:

- знайти вектор $\vec{\varphi}_{m^*}$ на кожній ітерації за формулою (24);
- за таблицею відповідності локальної і сіткової нумерації встановити номери r вузлів, які збігаються з вузлами $m1, \dots, m4$;

– кожний елемент вектора $\vec{\varphi}_{m^*}$, який відповідає r -ому внутрішньому вузлу, внести відповідно в r -е рівняння системи (10).

Повну систему рівнянь (10) одержимо, виконавши дану процедуру для всіх M елементів. Викладену процедуру використовуємо на етапі формування вектора нев'язок. Більш складною операцією є формування для векторної функції $\vec{\varphi}_* = (\varphi_1, \dots, \varphi_R)_*$ матриці Якобі ϕ розмірності $R \times R$. Виведемо вирази, які будуть використовуватись для цієї операції.

Диференціюючи вираз (24) за вектором \vec{U}_{m^*} , отримуємо матрицю ϕ_m розмірності 4×4 :

$$\phi_m = \frac{d\vec{\varphi}_{m^*}}{d\vec{U}_{m^*}} = -\frac{1}{4} v_m \sum_{i=1}^4 \left(\vec{K}_{mi}^{(x)} \frac{dB_{xmi}}{d\vec{U}_{m^*}} + \vec{K}_{mi}^{(y)} \frac{dB_{ymi}}{d\vec{U}_{m^*}} + \vec{K}_{mi}^{(z)} \frac{dB_{zmi}}{d\vec{U}_{m^*}} \right). \quad (27)$$

З врахуванням (18) – (20), (26) і (27) маємо

$$\begin{aligned}\phi_m &= -\frac{1}{4} v_m \sum_{i=1}^4 \left(\vec{K}_{mi}^{(x)} \left(\mu_{xxmi} \frac{dH_{xmi}}{d\vec{U}_{m^*}} + \mu_{xyyi} \frac{dH_{ymi}}{d\vec{U}_{m^*}} + \mu_{xzmi} \frac{dH_{zmi}}{d\vec{U}_{m^*}} \right) + \vec{K}_{mi}^{(y)} \left(\mu_{yxmi} \frac{dH_{xmi}}{d\vec{U}_{m^*}} + \right. \right. \\ &\left. \left. \mu_{yyyi} \frac{dH_{ymi}}{d\vec{U}_{m^*}} + \mu_{yzmi} \frac{dH_{zmi}}{d\vec{U}_{m^*}} \right) + \vec{K}_{mi}^{(z)} \left(\mu_{zxmi} \frac{dH_{xmi}}{d\vec{U}_{m^*}} + \mu_{zyyi} \frac{dH_{ymi}}{d\vec{U}_{m^*}} + \mu_{zzmi} \frac{dH_{zmi}}{d\vec{U}_{m^*}} \right) \right) = \\ &\frac{1}{4} v_m \sum_{i=1}^4 \left(\vec{K}_{mi}^{(x)} \left(\mu_{xxmi} \vec{K}_{mi}^{(x)} + \mu_{xyyi} \vec{K}_{mi}^{(y)} + \mu_{xzmi} \vec{K}_{mi}^{(z)} \right) + \vec{K}_{mi}^{(y)} \left(\mu_{yxmi} \vec{K}_{mi}^{(x)} + \mu_{yyyi} \vec{K}_{mi}^{(y)} + \mu_{yzmi} \vec{K}_{mi}^{(z)} \right) + \right. \\ &\left. \vec{K}_{mi}^{(z)} \left(\mu_{zxmi} \vec{K}_{mi}^{(x)} + \mu_{zyyi} \vec{K}_{mi}^{(y)} + \mu_{zzmi} \vec{K}_{mi}^{(z)} \right) \right),\end{aligned}\quad (28)$$

де μ_{jkm} ($j, k = x, y, z$) – елементи тензора диференціальної теплопровідності середовища

$$\mu = \frac{d\bar{B}}{d\bar{H}} = \begin{Bmatrix} \frac{\partial B_x}{\partial H_x} & \frac{\partial B_x}{\partial H_y} & \frac{\partial B_x}{\partial H_z} \\ \frac{\partial B_y}{\partial H_x} & \frac{\partial B_y}{\partial H_y} & \frac{\partial B_y}{\partial H_z} \\ \frac{\partial B_z}{\partial H_x} & \frac{\partial B_z}{\partial H_y} & \frac{\partial B_z}{\partial H_z} \end{Bmatrix} = \begin{Bmatrix} \mu_{xx} & \mu_{xy} & \mu_{xz} \\ \mu_{yx} & \mu_{yy} & \mu_{yz} \\ \mu_{zx} & \mu_{zy} & \mu_{zz} \end{Bmatrix}, \quad (29)$$

обчислювані в i -ому вузлу m -го СЕ.

Для безгістерезисного середовища на основі теореми взаємності [10] $\mu_{xy} = \mu_{yx}$, $\mu_{xz} = \mu_{zx}$,

$\mu_{yz} = \mu_{zy}$, тому $\mu_{xymi} = \mu_{yxmi}$, $\mu_{xzmi} = \mu_{zxmi}$, $\mu_{yzmi} = \mu_{zymi}$.

Для ізотропного нелінійного середовища тензор диференціальної теплопровідності визначається за формулою [11]

$$\mu = \begin{Bmatrix} \mu_\rho \cos^2 \eta_x + \mu_\tau \sin^2 \eta_x & (\mu_\rho - \mu_\tau) \cos \eta_x \cos \eta_y & (\mu_\rho - \mu_\tau) \cos \eta_x \cos \eta_z \\ (\mu_\rho - \mu_\tau) \cos \eta_y \cos \eta_x & \mu_\rho \cos^2 \eta_y + \mu_\tau \sin^2 \eta_y & (\mu_\rho - \mu_\tau) \cos \eta_y \cos \eta_z \\ (\mu_\rho - \mu_\tau) \cos \eta_z \cos \eta_x & (\mu_\rho - \mu_\tau) \cos \eta_z \cos \eta_y & \mu_\rho \cos^2 \eta_z + \mu_\tau \sin^2 \eta_z \end{Bmatrix}, \quad (30)$$

де $\mu_\rho = \frac{dB}{dH}$, $\mu_\tau = \frac{B}{H}$ – відповідно радіальна диференціальна і тангенціальна теплопровідність середовища; η_l ($l = x, y, z$) – кути між вектором \bar{H} або $\bar{B}[\bar{H}]$ і відповідно ортами $\bar{i}, \bar{j}, \bar{k}$ локальної декартової системи координат.

У випадку лінійного ізотропного середовища $\mu_\rho = \mu_\tau = \frac{B}{H} = \mu_s$, тому тензор диференціальної теплопровідності набуває вигляду

$$\mu = \begin{Bmatrix} \mu_s & 0 & 0 \\ 0 & \mu_s & 0 \\ 0 & 0 & \mu_s \end{Bmatrix}. \quad (31)$$

Для визначення вкладу m -го СЕ в матрицю Якобі ϕ , необхідно обчислити матрицю ϕ_m на кожній ітерації за формулою (28) і підсумувати всі її елементи з відповідними елементами матриці ϕ , враховуючи, що елемент ϕ_{mij} належить ns -й клітині матриці ϕ , де n, s – сіткові номери вузлів з локальними номерами mi і mj .

Повну матрицю Якобі ϕ одержимо, виконавши дану процедуру для кожного з M скінченних елементів області розрахунку D .

При використанні лагранжевих тетрадрів 2-го, 3-го і 4-го порядків необхідно застосувати відповідні кубатурні формули чисельного інтегрування [12] і вивести основні залежності за вище наведеною методикою.

На поверхні S області D можуть бути задані граничні умови [13] різного роду:

- на поверхні S або її частині задано значення температури U (граничні умови Діріхле або першого роду);
- на поверхні S або її частині задані граничні умови Неймана або другого роду

$$H_n = -\frac{\partial U}{\partial n} = 0, \quad (32)$$

де H_n – нормальна складова вектора \bar{H} на одиничний вектор \bar{n} зовнішньої нормалі до поверхні S ;

• на поверхні S або її частині задана лінійна комбінація температури і теплового потоку (граничні умови третього роду)

$$\mu \frac{\partial U}{\partial n} + \alpha(U - U_c) = 0, \quad (33)$$

де α – коефіцієнт тепловіддачі; U_c – температура навколишнього середовища;

• на поверхні S або її частині у випадку її ідеального контакту з іншою областю з температурою U_1 на границі та теплопровідністю μ_1 задано рівність температур та теплових потоків (граничні умови четвертого роду)

$$U = U_1; \mu \frac{\partial U}{\partial n} = \mu_1 \frac{\partial U_1}{\partial n}. \quad (34)$$

Висновки

1. Сформульовано краєву задачу розрахунку тривимірного стаціонарного потенціального температурного поля.
2. Побудовано скінченно-елементну модель розрахунку розподілу температури всередині тривимірної області, заповненої безгістерезисними нелінійними анізотропними середовищами.
3. Застосовано кубатурну формулу чисельного інтегрування за об'ємом лагранжевого тетраедра на базі інтерполяційного повного поліному для лагражевого тетраедра першого порядку.
4. Отримано систему нелінійних алгебраїчних рівнянь з умови мінімуму функціонала, яку часто розв'язують ітераційним методом Ньютона.
5. Запропоновано алгоритм визначення вкладу внутрішнього СЕ у вектор нев'язок і матрицю Якобі нелінійної системи рівнянь використовуючи елементи тензора диференціальної теплопровідності середовища.

Список літератури

- [1] Faiz J., Mazaheri E. An overview of thermal modelling techniques for permanent magnet machines. IET Science, Measurement & Technology, 2022.
- [2] Prajwal K T, Bhat P. Thermal analysis of a Thermoelectric Generator (TEG) using FEM technique. IOP Conference Series Materials Science and Engineering, 2021.
- [3] Petreševics F., Nagy B. FEM-Based Evaluation of the Point Thermal Transmittance of Various Types of Ventilated Façade Cladding Fastening Systems. Buildings, 2022.
- [4] Jindra D., Hradil P., Kala J., Salajka V. {Non linear FEM analysis of composite concrete slab exposed to extreme thermal load. AIP Conference Proceedings, 2020.
- [5] Ponsati T. L., Bahman A. S., Iannuzzo F. Thermal Modeling of Large Electrolytic Capacitors Using FEM and Considering the Internal Geometry. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2020.
- [6] Boukounacha A. Y., Zegnini B., Belkacem Y., Tahar S. The Effect of Temperature on the Thermal Conductivity of Transformer Oils Using the Finite Element Method. 1st International Conference on Materials Sciences and Applications "ICMSA2023", Khenchela, Algeria, 2023.
- [7] Silvester P. P., Ferrari R. L. Finite elements for electrical engineers. Cambridge University Press, 1996.
- [8] Gallagher R. H. Finite element analysis. Fundamentals. Pearson College Div; First Edition, 1975.
- [9] Segerlind L. J. Applied Finite Element Analysis. J. Wiley & Sons, 1984.
- [10] Silvester P., Cabayan H. S., Browne B. T. Efficient techniques for finite element analysis of electric machines. – IEEE Trans. PAS, 1973, 92, № 4, p. 1274 – 1281.
- [11] Дышовый Р.В. Расчет статического магнитного поля в неявнополюсных электрических машинах дифференциальным сеточным методом. Автореф. дисс. канд. техн. наук. – Львов, 1983. – 18 с.
- [12] Карашецкий В.П. Кубатурні формули чисельного інтегрування за об'ємом тетраедра на основі інтерполяційних повних поліномів//Наук. вісник НЛТУ України: Зб. наук.-техн. праць. – Львів: НЛТУУ. – 2007, вип. 17.6. – С. 258-264.
- [13] Юшко С. В. Стаціонарна теплопровідність: навч. посіб./ С.В. Юшко, О. Є. Борщ, М.А. Юшко – Х.: НТУ "ХПІ", 2011. – 80 с.

Стаття надійшла: 21.03.2024

References

- [1] Faiz J., Mazaheri E. An overview of thermal modelling techniques for permanent magnet machines. IET Science, Measurement & Technology, 2022.
- [2] Prajwal K T, Bhat P. Thermal analysis of a Thermoelectric Generator (TEG) using FEM technique. IOP Conference Series Materials Science and Engineering, 2021.
- [3] Petresevics F., Nagy B. FEM-Based Evaluation of the Point Thermal Transmittance of Various Types of Ventilated Façade Cladding Fastening Systems. Buildings, 2022.
- [4] Jindra D., Hradil P., Kala J., Salajka V. {Non linear FEM analysis of composite concrete slab exposed to extreme thermal load. AIP Conference Proceedings, 2020.
- [5] Ponsati T. L., Bahman A. S., Iannuzzo F. Thermal Modeling of Large Electrolytic Capacitors Using FEM and Considering the Internal Geometry. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2020.
- [6] Boukounacha A. Y., Zegnini B., Belkacem Y., Tahar S. The Effect of Temperature on the Thermal Conductivity of Transformer Oils Using the Finite Element Method. 1st International Conference on Materials Sciences and Applications "ICMSA2023", Khenchela, Algeria, 2023.
- [7] Silvester P. P., Ferrari R. L. Finite elements for electrical engineers. Cambridge University Press, 1996.
- [8] Gallagher R. H. Finite element analysis. Fundamentals. Pearson College Div; First Edition, 1975.
- [9] Segerlind L. J. Applied Finite Element Analysis. J. Wiley & Sons, 1984.
- [10] Silvester P., Cabayan H. S., Browne B. T. Efficient techniques for finite element analysis of electric machines. – IEEE Trans. PAS, 1973, 92, № 4, p. 1274 – 1281.
- [11] Dyshovyy R.V. Raschet statycheskoho mahnytnoho polya v neyavnopolyusnykh élektrycheskykh mashynakh dyfferentsyal'nym setochnym metodom. Avtoref. dyss. kand. tekhn. nauk. – L'vov, 1983. – 18 s.
- [12] Karashets'kyi V.P. Kubaturni formuly chysel'noho intehruvannya za ob'yemom tetraedra na osnovi interpolyatsiynykh povnykh polinomiv//Nauk. visnyk NLTU Ukrayiny: Zb. nauk.-tekhn. prats'. – L'viv: NLTUU. – 2007, vyp. 17.6. – S. 258-264.
- [13] Yushko S. V. Statsionarna teploprovidnist': navch. posib./ S.V. Yushko, O. YE. Borshch, M.A. Yushko – KH.: NTU "KHPI", 2011. – 80 s

Відомості про авторів

Карашецький Володимир Петрович, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення Національного лісотехнічного університету України

Volodymyr Petrovych Karashetskyi, candidate of technical sciences, associate professor, associate professor of the Department of Software Engineering of the Ukrainian National Forestry University

Яркун Володимир Ігорович, старший викладач кафедри інженерії програмного забезпечення Національного лісотехнічного університету України

Yarkun Volodymyr Ihorovych, senior lecturer of the Department of Software Engineering of the Ukrainian National Forestry University

CALCULATION OF THREE-DIMENSIONAL STATIONARY POTENTIAL THERMAL FIELDS BY THE FINITE ELEMENT METHOD

Ukrainian National Forestry University

БІОЛОГІЧНІ ТА МЕДИЧНІ ПРИЛАДИ І СИСТЕМИ

УДК 681.7:616-71

Н. І. Заболотна, В. В. Шолота

СИСТЕМА ДВОХВИЛЬОВОЇ ЛАЗЕРНОЇ ДІАГНОСТИКИ МОЛОЧНИХ ЗАЛОЗ ЗА ПОЛЯРИЗАЦІЙНИМ КАРТОГРАФУВАННЯМ ЗОБРАЖЕНЬ ПЛІВОК ПЛАЗМИ КРОВІ

Вінницький національний технічний університет, Вінниця

Анотація. В статті наведено метод та систему лазерної діагностики молочних залоз за результатами картографування та аналізу на довжинах хвиль 0,638 мкм та 0,405 мкм мап азимутів та еліптичностей поляризації плівок плазми крові людини. Розроблено та реалізовано нечіткі підтримки прийняття рішення в системі. Отримано підвищення достовірності діагностики на 3–4% в порівнянні із аналогами.

Ключові слова: система, двохвильова лазерна діагностика, молочні залози, азимут та еліптичність поляризації, плівки плазми крові, моделі нечіткої логіки.

Abstract. The article presents the method and system of laser diagnostics of mammary glands based on the results of mapping and analysis at wavelengths of 0.638 μm and 0.405 μm of azimuth and ellipticity maps of polarization of human blood plasma films. Fuzzy decision support models in the system were developed and implemented. A 3–4% increase in the reliability of the diagnosis was obtained in comparison with analogues.

Key words: system, two-wave laser diagnostics, mammary glands, azimuth and ellipticity of polarization, blood plasma films, models of fuzzy logic.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-146-156>.

Вступ

Системи та методи поляризаційного картографування оптично неоднорідних біологічних тканин (БТ) та рідин сьогодні знайшли ефективне застосування при проведенні медичної діагностики патологічних станів різних органів людини [1–4], доповнюючи відомі медичні технології діагностування. Суттєвою перевагою поляризаційних лазерних методів є висока чутливість поляризаційних параметрів поля, перетвореного досліджуванним біологічним шаром, до змін його оптико-геометричних параметрів, обумовлених зміною фізіологічного стану. Ця особливість методів лазерної поляриметрії БТ в поєднанні з можливістю реалізації в широкому діапазоні довжин хвиль, інформаційною повнотою вимірювань та комплексним оцінюванням одержаних даних на основі сучасних інформаційних технологій дозволяє реалізувати успішну діагностику доброякісних та злоякісних пухлин БТ органів людини [2, 3, 5, 6].

Проблема захворюваності на рак молочних залоз тривалий час займає провідні місця у структурі захворюваності, смертності та відмічається щорічним приростом серед онкологічних нозологій в Україні. Це обумовлює необхідність створення сучасних систем лазерної поляриметричної діагностики молочних залоз з високою достовірністю оцінювання патологічних змін, особливо на ранніх стадіях розвитку пухлинних процесів.

Актуальність

Відомими та досить травматичними є методи діагностування на основі виявлення патологічних змін на лазерних поляризаційних зображеннях гістологічних зрізів біологічної тканини молочної залози. Проте виявлення злоякісного новоутворення молочних залоз до виникнення структурних змін потребує застосування нових методів, які дозволяють зафіксувати пухлинні зміни на етапах їх доклінічного розвитку. Саме на етапі доклінічного діагностування раку молочних залоз відбувається зміна третичної, четвертичної структури білків плазми крові при незмінній їх біохімічній структурі, що виявляється за змінами двопронезаломлення білків плазми крові при лазерній поляриметрії, але не властиво іншим методам діагностики. Тому перспективність застосування систем діагностики патологічних станів молочних залоз (МЗ) на основі аналізу поляризаційних зображень плівок плазми крові не викликає сумніву [7–9].

В той же час, існуючим системам лазерного поляризаційного картографування плівок білків плазми крові властиві певні недоліки, які обмежують їх потенціальні можливості щодо достовірності діагностики молочних залоз. Зокрема, ці обмеження накладаються реалізацією вимірювань мап азимутів та еліптичностей поляризації зображень плівок плазми крові лише на одній довжині хвилі [7, 10, 11]. Недостатня кількість аналізованих вимірних параметрів може збільшувати ризики хибної ідентифікації на зразках із непередбаченими навчальною вибіркою діагнозами.

Разом з тим, сучасний рівень розвитку інформаційних технологій створює всі можливості для застосування інтелектуального аналізу та впровадження підсистем підтримки прийняття рішень в такі системи.

Мета

Метою статті є підвищення достовірності оцінювання патологічних станів молочних залоз в системі лазерної діагностики шляхом розвитку метода поляризаційного картографування зображень плівок плазми крові, який доповнено можливостями проведення картографування на другій довжині хвилі опромінюючого лазерного випромінювання у поєднанні з багатопараметричним аналізом даних.

Задачі

1. Розвинути метод лазерної поляризаційної діагностики молочних залоз шляхом проведення картографування та аналізу розподілів азимутів та еліптичностей поляризації зображення плівок плазми крові на другій довжині хвилі.
2. Удосконалити архітектуру системи лазерної діагностики молочних залоз з відображенням особливостей методу двохвильового поляризаційного картографування та аналізу плівок плазми крові із запровадженням підсистеми підтримки прийняття рішення (ППР).
3. Оцінити достовірність діагностики патологічних станів молочних залоз за запропонованим методом за результатами експериментального дослідження плівок плазми крові в удосконаленій системі.

Матеріали для дослідження

Для проведення досліджень краплю плазми крові з піпетки наносять на підкладку з оптично однорідного скла. Наносити потрібно так, щоб плазма по поверхні скла рівномірно розтікалася. Потім протягом 24 годин відбувається просушування препарату, в результаті чого утворюється плівка.

Метод та архітектура системи двохвильової лазерної діагностики молочних залоз

Вирішуючи проблему створення поляризаційних технологій достовірної діагностики доклінічних форм раку молочних залоз, розвитку набув підхід, заснований на аналізі трансформації поляризаційних характеристик плазми крові при онкологічних змінах в БТ. Основними складовими плазми крові в стані фізіологічної норми БТ є альбуміни та глобуліни [5, 7]. За відомою ізотропно-анізотропною моделлю плазми крові [5, 7] кристали альбуміну та глобуліну мають такі ж поляризаційні властивості, як і оптичні одноосні кристали, що характеризуються подвійним променезаломленням в умовах одноразового розсіювання оптично тонких біологічних шарів.

Альбумін-глобулінова кристалічна складова розглядається як об'єктивна фізична причина формування координатних розподілів азимутів та еліптичностей поляризації точок лазерного зображення плазми крові. Для виявлення зміни орієнтації елементів розподілу голкоподібних кристалів альбуміну застосовують мапи азимутів $\alpha(X, Y)$ поляризації лазерного зображення плівок плазми крові. Для виявлення змін концентрацій альбумінів та глобулінів в структурі плазми крові більш чутливою є мапа еліптичностей $\beta(X, Y)$ поляризації її лазерного зображення.

Стан поляризації перетвореного альбумінами та глобулінами зразку плівки плазми крові лазерного пучка визначається азимутами $\alpha(x, y)$ та еліптичностями $\beta(x, y)$ поляризації за вимірними елементами вектора Стокса $S_2(x, y), S_3(x, y), S_4(x, y)$ в кожній точці (x, y) лазерного зображення плівки плазми крові

$$\alpha(x, y) = 0,5 \arctg \frac{S_3(x, y)}{S_2(x, y)}, \quad (1)$$

$$\beta(x, y) = 0,5 \arcsin(S_4(x, y) / S_1(x, y)). \quad (2)$$

В традиційному однохвильовому лазерному стокс-поляриметрі на довжині хвилі лазера 638 нм було встановлено чутливість статистичних оцінок координатних, автокореляційних та спектральних розподілів мап азимутів $\alpha(M \times N)$ та еліптичностей $\beta(M \times N)$ поляризаційних зображень плазми крові до змін фізіологічного стану молочних залоз [5, 7, 10–12]. Також встановлено діапазони відмінностей між вказаними оцінками при діагностиці станів молочних залоз «норма», «доброякісні зміни», «злоякісні зміни» та визначено верхні оцінки достовірності діагностики з максимальними значеннями на рівні 86%.

В процесі досліджень було розроблено метод двохвильової лазерної діагностики молочних залоз за поляризаційним картографуванням та аналізом плівок плазми крові, який є розвитком вказаного

однохвильового метода лазерної поляризаційної діагностики. В розробленому методі здійснюють вимірювання та аналіз елементів мап азимутів та еліптичностей поляризації зображень плівок плазми крові на довжинах хвиль 0,638 мкм та 0,405 мкм лазерного поляризованого випромінювання.

Апаратно-орієнтований метод двохвильової лазерної діагностики молочних залоз реалізують в системі, зображеній на рисунку 1. Система складається із вимірювального каналу з блоком керування та комп'ютера.

Основними елементами вимірювального каналу є такі [13]:

- блок генерації двохвильового лазерного випромінювання 1 з двома лазерами, що працюють на довжинах хвиль відповідно 0,638 мкм на 0,405 мкм і світлооб'єднувач;
- коліматор 2;
- блок поляризаційного опромінення 3, який утворено двома фазовими чвертьхвильовими пластинками 4_1 та 4_2 та лінійним поляризатором 5_1 ;
- об'єктний блок 6, на якому розташовується досліджуваний зразок;
- проєкційний блок 7;
- блок 8 поляризаційної фільтрації, утворений лінійним поляризаційним аналізатором 5_2 та фазовою чвертьхвильовою пластинкою 4_3 ;
- цифрова камера 9.

Система містить персональний комп'ютер 10 та блок мікроконтрольного керування 11, який керує поворотами та позиціонуванням двигунів 13_1 – 13_4 через драйвери двигунів 12_1 – 12_4 при організації зворотного зв'язку за допомогою позиційних датчиків 14_1 – 14_4 .

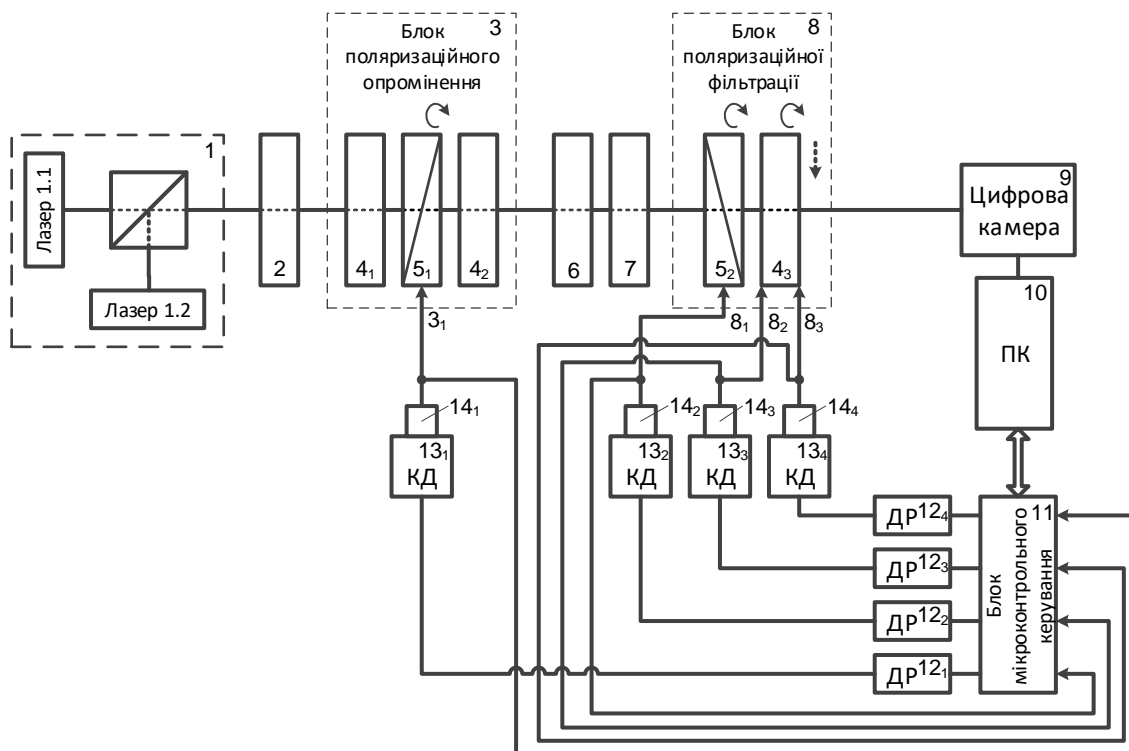


Рисунок 1 – Схема системи двохвильової лазерної діагностики молочних залоз за поляризаційним картографуванням плівок плазми крові

Розглянемо суть апаратно-орієнтованого методу двохвильової лазерної діагностики МЗ.

1. Формують поляризований лазерний пучок у вигляді випромінювання низькокогерентного напівпровідникового лазерного діоду з довжиною хвилі $\lambda = 0,638 \mu\text{m}$.

2. Шляхом пропускання сформованого лазерного пучка через поляризатор одержують поляризований лазерний пучок зі сталим значенням азимуту поляризації ($\alpha_0 = \text{const}$) плоскополяризованого лазерного пучка на обраній довжині хвилі.

3. Опромінують зразок плівки плазми крові лінійно поляризованим лазерним пучком зі сталим азимуту поляризації α_0 .

4. Орієнтують площину пропускання поляризатора-аналізатора послідовно під кутами $0^\circ; 45^\circ; 90^\circ; 135^\circ$.

5. Проектують за допомогою мікрооб'єктива послідовно відповідні чотири координатні розподіли одержаних відфільтрованих інтенсивностей $I_{x,y}(\alpha_0 - \alpha)$ ($x = \overline{1:M}; y = \overline{1:N}$) лазерних мікроскопічних зображень в площину фотоприймальної камери з роздільною здатністю $M \times N$ пікселів, яка їх реєструє.

6. Формують умови правоциркулярної фільтрації (\otimes) за допомогою блоку поляризаційної фільтрації: оптичну вісь фазової пластинки орієнтують під кутом 0° , а площину пропускання аналізатора орієнтують під кутом 45° .

7. Опромінюють зразок плівки плазми крові лінійно поляризованим лазерним пучком зі сталим азимутом поляризації α_0 за умов проведення правоциркулярної фільтрації.

8. Реєструють за допомогою камери координатний розподіл інтенсивності $I_{x,y}(\alpha_0 - \otimes)$ в площині поляризаційно відфільтрованого мікроскопічного лазерного зображення плівки плазми крові.

9. Формують умови лівоциркулярної фільтрації (\oplus) за допомогою блоку поляризаційної фільтрації: оптичну вісь фазової пластинки орієнтують під кутом 0° , а площину пропускання аналізатора орієнтують під кутом (-45°) .

10. Реєструють за допомогою камери координатний розподіл інтенсивності $I_{x,y}(\alpha_0 - \oplus)$ в площині поляризаційно відфільтрованого мікроскопічного лазерного зображення плівки плазми крові.

11. Для кожного пікселя (x, y) камери роздільною здатністю $(M \times N)$ обчислюють відповідні значення азимутів $\alpha_{x,y}^\lambda$ та еліптичностей $\beta_{x,y}^\lambda$ поляризації зображення плівки плазми крові за інтенсивностями поляризаційно відфільтрованих розподілів $I_{x,y}$ на довжині хвилі λ за формулами

$$\alpha_{x,y}^\lambda = 0,5 \arctg \left[\frac{I_{x,y}(\alpha_0 - 45^\circ) - I_{x,y}(\alpha_0 - (135^\circ))}{I_{x,y}(\alpha_0 - 0^\circ) - I_{x,y}(\alpha_0 - 90^\circ)} \right]; \quad (3)$$

$$\beta_{x,y}^\lambda = 0,5 \arcsin \left[\frac{I_{x,y}(\alpha_0 - \otimes) - I_{x,y}(\alpha_0 - \oplus)}{I_{x,y}(\alpha_0 - 0^\circ) + I_{x,y}(\alpha_0 - 90^\circ)} \right]. \quad (4)$$

12. Обчислюють оцінки статистичних моментів, з першого по четвертий порядок $M_1(\alpha^\lambda, \beta^\lambda) - M_4(\alpha^\lambda, \beta^\lambda)$, розподілів елементів [12, 13] відповідно мапи азимутів та мапи еліптичностей, виміряних на довжині хвилі λ .

13. Обчислюють автокореляційні функції (АКФ) мап азимутів та мап еліптичностей на довжині хвилі λ , а також значення кореляційної площі $S(\alpha^\lambda, \beta^\lambda)$ та оцінок статистичних моментів визначених розподілів АКФ $Q_2(\alpha^\lambda, \beta^\lambda), Q_4(\alpha^\lambda, \beta^\lambda)$, названих оцінками кореляційних моментів 2-го та 4-го порядків [12, 13].

14. Формують поляризований лазерний пучок у вигляді випромінювання низькокогерентного напівпровідникового лазерного діоду з довжиною хвилі $\lambda = 0,405 \mu m$.

15. Виконують дії, описані в пунктах з 2-го по 13-ий.

16. Приймають рекомендоване діагностичне рішення про норму та патологію молочних залоз за аналізом мап азимутів та еліптичностей плівки плазми крові, використовуючи розроблені моделі вирішальних правил нечіткої логіки, які враховують інформативні ознаки мап у вигляді відповідних оцінок статистичних та кореляційних моментів, одержаних на двох довжинах хвиль в п. 12 та п. 13.

Для реалізації аналізу виміряних мап азимутів $\alpha(M \times N)$ та еліптичностей $\beta(M \times N)$ плівок плазми крові в системі діагностики, наведеній на рисунку 1, застосовують алгоритмічно-програмне забезпечення комп'ютера, структура якого наведена на рисунку 2. До його складу входять модулі

захоплення та збереження зображень, модуль формування мікрокоманд для блоку керування, головний модуль, блок обчислення азимутів і еліптичностей, блок аналізу для визначення інформативних ознак, підсистема підтримки прийняття рішення. Особливістю підсистеми ППР є застосування «нечітких» моделей вирішальних правил [14], отриманих для діагностики станів «норма» та «фрак МЗ» в системі.

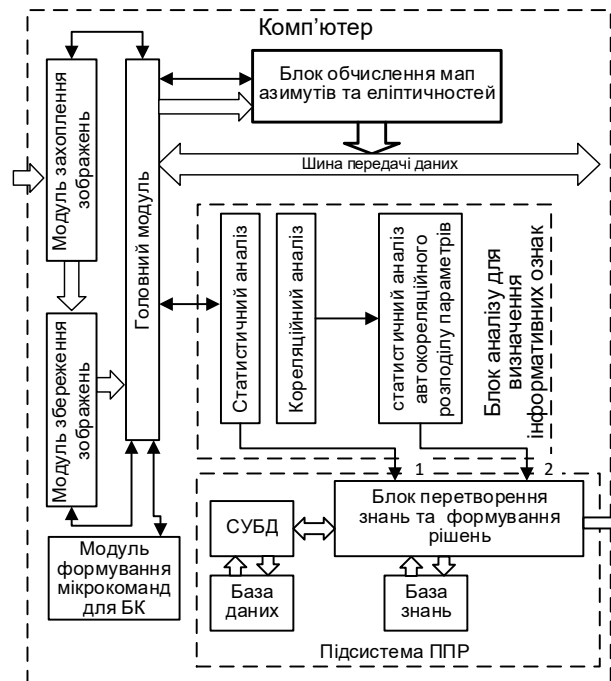


Рисунок 2 – Структура алгоритмічно-програмного забезпечення системи двохвильової лазерної діагностики молочних залоз

Нечіткі моделі підтримки прийняття рішення в системі двохвильової лазерної діагностики молочних залоз

Для отримання моделей підтримки прийняття рішень було проведено експериментальне дослідження двох груп вибірок плівок плазми крові, взятої у здорових жінок (група 1 – 35 зразків) та у жінок із раком молочних залоз (група 2 – 35 зразків). В системі, наведеній на рисунку 1, на довжинах хвиль 0,638 мкм та 0,405 мкм було визначено та проаналізовано мапи азимутів та еліптичностей поляризації зображень досліджуваних плівок плазми крові із встановленими попередньо діагнозами.

Статистичні оцінки координатних розподілів та АКФ азимутів та еліптичностей поляризації зображень плівок плазми крові, взятої у жінок групи 1 та групи 2, визначені на двох довжинах хвиль, наведено в таблиці 1. Серед всіх наведених ознак найбільш інформативними є такі, діапазони змінювання яких для стану норми та стану раку молочних залоз не перетинаються.

Найбільш чутливими до зміни фізіологічного стану МЗ на двох довжинах хвиль виявились оцінки таких характеристик розподілу елементів мап азимутів поляризації плівок плазми крові:

- статистичних моментів 1-го та 3-го порядків на довжині хвилі 0,638 мкм $M_1(\alpha^{21}); M_3(\alpha^{21});$
- статистичних моментів 2-го–4-го порядків на довжині хвилі 0,405 мкм $M_2(\alpha^{22}); M_3(\alpha^{22}); M_4(\alpha^{22})$

Найбільш чутливими до зміни фізіологічного стану МЗ на двох довжинах хвиль виявились оцінки таких характеристик розподілу елементів мап еліптичностей плівок плазми крові:

- статистичного моменту 2-го порядку на довжині хвилі 0,638 мкм $M_2(\beta^{21});$
- кореляційного моменту 4-го порядку на довжині хвилі 0,638 мкм $Q_4(\beta^{21});$
- статистичного моменту 1-го порядку на довжині хвилі 0,405 мкм $M_1(\beta^{22});$
- статистичного моменту 3-го порядку на довжині хвилі 0,405 мкм $M_3(\beta^{22});$
- статистичного моменту 4-го порядку на довжині хвилі 0,405 мкм $M_4(\beta^{22});$
- кореляційного моменту 4-го порядку на довжині хвилі 0,638 мкм $Q_4(\beta^{22}).$

Таблиця 1 – Середнє та стандартне відхилення статистичних оцінок координатних розподілів та АКФ азимутів та еліптичностей зображень плівок плазми крові пацієнток групи 1 та 2 для довжин хвиль $\lambda_1 = 0,638$ мкм; $\lambda_2 = 0,405$ мкм

Характеристики параметрів	Довжина хвилі $\lambda_1 = 0,638$ мкм		Довжина хвилі $\lambda_2 = 0,405$ мкм	
	Стан «норма МЗ»	Стан «рак МЗ»	Стан «норма МЗ»	Стан «рак МЗ»
Вимірювальний параметр – мапа азимутів $\alpha(M \times N)$				
$M_1(\alpha^\lambda)$	0,740±0,050	0,160±0,040	0,130±0,020	0,120±0,015
$M_2(\alpha^\lambda)$	0,013±0,004	0,013±0,080	0,060±0,010	0,130±0,020
$M_3(\alpha^\lambda)$	0,070±0,006	0,130±0,060	0,050±0,004	0,080±0,010
$M_4(\alpha^\lambda)$	0,500±0,100	0,600±0,200	2,080±0,080	1,700±0,040
$S(\alpha^\lambda)$	2,070±0,600	1,800±0,400	1,333±0,400	2,100±0,700
$Q_2(\alpha^\lambda)$	2,300±0,900	3,200±1,300	0,020±0,013	0,020±0,010
$Q_4(\alpha^\lambda)$	0,020±0,004	0,020±0,003	0,750±0,110	0,810±0,190
Вимірювальний параметр – мапа еліптичностей $\beta(M \times N)$				
$M_1(\beta^\lambda)$	0,810±0,100	0,780±0,090	0,750±0,080	0,810±0,090
$M_2(\beta^\lambda)$	0,064±0,008	0,054±0,006	0,110±0,030	0,410±0,050
$M_3(\beta^\lambda)$	0,014±0,003	0,024±0,011	0,030±0,010	0,180±0,040
$M_4(\beta^\lambda)$	3,800±0,180	3,900±0,340	2,640±0,090	0,680±0,070
$S(\beta^\lambda)$	18,80±6,700	20,20±5,400	9,300±1,900	7,900±1,400
$Q_2(\beta^\lambda)$	2,900±0,130	4,100±3,600	5,200±1,400	5,800±1,900
$Q_4(\beta^\lambda)$	0,03±0,011	0,018±0,015	0,020±0,005	0,010±0,006

На основі інформативних ознак мап азимутів та еліптичностей зображень плівок плазми крові, одержаних на двох довжинах хвиль в умовах інформаційної невизначеності, застосовують відомі методи ППР при оцінюванні патологічних станів молочних залоз. За умов відсутності великорозмірних вибірок даних та специфіки подання інформативних ознак за середнім та стандартним відхиленням статистичних оцінок розподілів елементів $\alpha(M \times N)$; $\beta(M \times N)$ доцільним є застосування нечітких методів ППР.

Застосовуючи положення теорії нечіткої логіки та обираючи інформативні ознаки мап азимутів та еліптичностей зображень плівок плазми крові як лінгвістичні змінні, отримано моделі вирішальних правил ППР. Для їх реалізації служить підсистема ППР, подана на рисунку 2, яка містить базу знань, базу даних, СУБД та блок перетворення знань та формування рішень. В останньому блоці здійснюється налаштування функцій належності нечітких термів (наприклад, низький (Н), нижче середнього (НС), середній (С), вище середнього (ВС), високий (В)) та реалізація нечітких моделей вирішальних правил.

Так, в таблиці 2 наведено значення лінгвістичних змінних за нечіткими термами для мап азимутів.

Таблиця 2 – Інформативні параметри мап азимутів плівок плазми крові, отримані на довжинах хвиль $\lambda_1 = 0,638$ мкм; $\lambda_2 = 0,405$ мкм, подані в нечітких термах для діагностики молочних залоз

Діагноз	$M_1(\alpha^{\lambda_1})$	$M_3(\alpha^{\lambda_1})$	$M_2(\alpha^{\lambda_1})$	$M_3(\alpha^{\lambda_2})$	$M_4(\alpha^{\lambda_2})$
Норма МЗ	ВС В	Н НС	Н НС	Н НС	ВС В
Рак МЗ	Н	ВС В	В	С ВС, В	Н НС

Також за інформативними ознаками мапи азимутів визначено модель обчислення функції належності зразку півки плазми крові до групи «рак МЗ» μ_{α}^{pat} у вигляді

$$\begin{aligned} \mu_{\alpha}^{pat}(M_1(\alpha^{\lambda_1}), M_3(\alpha^{\lambda_1}), M_2(\alpha^{\lambda_2}), M_3(\alpha^{\lambda_2}), M_4(\alpha^{\lambda_2})) = & \\ & \{ [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^C(M_3(\alpha^{\lambda_2})) \wedge \mu^H(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^C(M_3(\alpha^{\lambda_2})) \wedge \mu^{HC}(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_2})) \wedge \mu^H(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_2})) \wedge \mu^{HC}(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^B(M_3(\alpha^{\lambda_2})) \wedge \mu^H(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^B(M_3(\alpha^{\lambda_2})) \wedge \mu^{HC}(M_4(\alpha^{\lambda_2}))] \vee \quad (6) \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^B(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^C(M_3(\alpha^{\lambda_2})) \wedge \mu^H(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^B(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^C(M_3(\alpha^{\lambda_2})) \wedge \mu^{HC}(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^B(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_2})) \wedge \mu^H(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^B(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^{BC}(M_3(\alpha^{\lambda_2})) \wedge \mu^{HC}(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^B(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^B(M_3(\alpha^{\lambda_2})) \wedge \mu^H(M_4(\alpha^{\lambda_2}))] \vee \\ & [\mu^H(M_1(\alpha^{\lambda_1})) \wedge \mu^B(M_3(\alpha^{\lambda_1})) \wedge \mu^B(M_2(\alpha^{\lambda_2})) \wedge \mu^B(M_3(\alpha^{\lambda_2})) \wedge \mu^{HC}(M_4(\alpha^{\lambda_2}))] \}. \end{aligned}$$

Графічний вигляд функцій належності $\mu^H(r), \mu^{HC}(r), \mu^C(r), \mu^{BC}(r), \mu^B(r)$ нечітких термів наведено на рисунку 3 та описано математично в роботі [15].

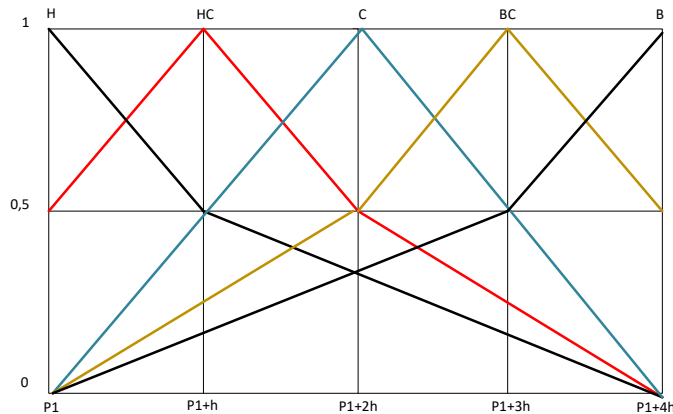


Рисунок 3 – Графічне подання функцій належності нечітких термів [15]

Рекомендований діагноз за аналізом інформативних ознак мап азимутів зображень плівок плазми крові визначається за максимальним значенням обрахованих функцій $\mu^{norm}(\alpha)$ та $\mu^{pat}(\alpha)$.

Також в таблиці 3 наведено значення інформативних ознак як лінгвістичних змінних, поданих за нечіткими термами, для мап еліптичностей поляризації зображень плівок плазми крові.

Таблиця 3 – Інформативні ознаки мап еліптичностей плівок плазми крові, отримані на довжинах хвиль $\lambda_1 = 0,638$ мкм; $\lambda_2 = 0,405$ мкм, подані в нечітких термах для діагностики молочних залоз

Діагноз	$M_2(\beta^{\lambda_1})$	$Q_4(\beta^{\lambda_1})$	$M_1(\beta^{\lambda_2})$	$M_3(\beta)^{\lambda_2}$	$M_4(\beta^{\lambda_2})$	$Q_4(\beta^{\lambda_2})$
Норма МЗ	НС, С, BC, B	B, BC, C	H, HC	H	B	C, BC, B
Рак МЗ	H, HC, C	H, HC, C, BC	BC B	C, BC B	H	H, HC C

За принципами нечіткої логіки та на основі даних таблиці 3 одержано нечіткі моделі вирішальних правил ППР на основі аналізу мап еліптичностей плівок плазми крові. Не наводимо їх в статті із-за громіздкого вигляду співвідношень.

Чотири нечіткі моделі вирішальних правил, одержані при аналізі мап азимутів та еліптичностей поляризації на двох довжинах хвиль 0,638 мкм та 0,405 мкм, програмно реалізовано на мові Java в підсистемі ППР системи діагностики молочних залоз.

Оцінювання достовірності двохвильової лазерної діагностики молочних залоз в системі

Дослідження достовірності методу двохвильової діагностики МЗ проводились при використанні експериментальної системи, схема якої подана на рисунку 1. Дві групи зразків плазми крові, взятої відповідно у здорових жінок (група 1) та у жінок із раком молочних залоз (група 2), перемішувались та опрацьовувались в системі. Обсяг опрацьованої вибірки склав 70 зразків, по 35 зразків в кожній групі.

Для кожного зразку плазми крові визначалась мапа азимутів та мапа еліптичностей на довжинах хвиль 0,638 мкм та 0,405 мкм та здійснювався їх відповідний аналіз із автоматичним формуванням рекомендованого діагнозу підсистемою ППР. При цьому було отримано як істинно позитивні (TP) та істинно негативні (TN) рішення, так і хибно позитивні (FP) та хибно негативні (FN) рішення. За вказаними категоріями рішень, отриманими під час діагностування в системі за картографуванням азимутів та картографуванням еліптичностей, визначено оцінки достовірностей відповідного діагностичного методу, які наведено в таблиці 4.

Таблиця 4 – Оцінка достовірності діагностики МЗ за картографуванням та аналізом азимутів та еліптичностей плівок плазми крові

N з/п	Метод діагностики	Категорія та кількість рішень				Оцінка достовірності, %
		TP	FP	TN	FN	
1	Метод двохвильової діагностики МЗ за картографуванням азимутів поляризації плівок плазми крові із нечіткою ППР	33	5	30	2	90
2	Метод діагностики МЗ за картографуванням та аналізом мап азимутів поляризації плівок плазми крові на довжині хвилі 0,638 мкм – аналог 1 [10]	32	7	28	3	86
3	Метод двохвильової діагностики МЗ за картографуванням еліптичностей поляризації плівок плазми крові із нечіткою ППР	31	3	32	4	90
4	Метод діагностики МЗ за картографуванням та аналізом мап еліптичності поляризації плівок плазми крові на довжині хвилі 0,638 мкм – аналог 2 [11]	29	3	32	6	87

В таблиці 4 також наведено оцінку достовірності відповідних аналогів досліджуваних методів, в яких здійснюють картографування параметрів поляризації об'єктного поля лише на одній довжині хвилі 0,638 нм та не застосовують методи ППР. Очевидно, що достовірність двохвильових методів лазерної діагностики МЗ зростає у порівнянні із однохвильовими аналогами на 4% при картографуванні азимутів та на 3% при картографуванні еліптичностей поляризації плівок плазми крові.

Висновки

1. Розроблено метод лазерної поляризаційної діагностики молочних залоз шляхом проведення картографування та аналізу розподілів азимутів та еліптичностей поляризації зображення плівок плазми крові на двох довжинах хвиль 0,638 мкм та 0,405 мкм, що дозволило збільшити кількість інформативних ознак для розроблених нових нечітких моделей підтримки прийняття рішення.

2. Удосконалено архітектуру системи лазерної діагностики МЗ за рахунок введення в блок генерації лазерного випромінювання другого лазера, що працює на довжині хвилі 0,405 мкм, та світлооб'єднувача, а також введення підсистеми ППР для реалізації нечітких моделей вирішальних правил.

3. Проведено оцінку достовірності двохвильового методу діагностики патологічних станів молочних залоз в удосконаленій системі. У порівнянні із аналогами при картографуванні азимутів та еліптичностей поляризації плівок плазми крові на двох довжинах хвиль у поєднанні із нечіткими методами ППР досягнуто зростання достовірності діагностики відповідно на 4% та на 3%.

Матеріали статті підготовлено за підтримки Національного фонду досліджень України за проєктом 2022.01/0135

Список літератури

- [1] N. Ghosh, I. A. Vitkin, "Tissue polarimetry: concepts, challenges, applications, and outlook," *Journal of Biomedical Optics*, vol. 16, no.11, 110801. 2011.
- [2] M. Anastasiadou et al., "Polarimetric imaging for the diagnosis of cervical cancer," *Phys. Status Solidi C*, vol. 5, pp. 1423–1426. 2008.
- [3] A. Pierangelo et al., "Ex-vivo characterization of human colon cancer by Mueller polarimetric imaging," *Optics express*, vol. 19, no 2, pp. 1582–1593. 2011.
- [4] S. Alalia S., A. Vitkin, "Polarized light imaging in biomedicine: emerging Mueller matrix methodologies for bulk tissue assessment," *Journal of Biomedical Optics*, vol. 20, no 6, 061104. 2015.
- [5] О. Г. Ушенко та ін., *Лазерна поляриметрія біологічних тканин. Діагностика пухлин жіночих репродуктивних органів*. Чернівці, Україна: Чернівецький нац. ун-т, 2010.
- [6] Ye Wang et al., "Mueller matrix microscope: a quantitative tool to facilitate detections and fibrosis scorings of liver cirrhosis and cancer tissues," *Journal of Biomedical Optics*, vol. 21, no 7, 071112. 2016.
- [7] O. P. Mintser, N. I. Zabolotna, B. P. Oliinychenko, and P. Komada, "Differential phase analysis of laser images of a polycrystalline component of blood plasma in diagnostics of pathological changes in mammary gland," *Proc. SPIE*, vol. 8698, 86980D. 2012.
- [8] N. I. Zabolotna et al., "System of polarization phasometry of polycrystalline blood plasma networks in mammary gland pathology diagnostics," *Proc. of SPIE*, vol. 9613, 961311. 2015.
- [9] N. I. Zabolotna, K. O. Radchenko, M. H. Tarnovskiy, "System of Mueller-Jones matrix polarizing mapping of blood plasma films in breast pathology," *Proc. SPIE*. 2017, vol. 10407, 1040714. 2017.
- [10] Н. І. Заболотна, Б. П. Олійниченко, В. В. Шолота, "ROC – аналіз поляризаційного картографування азимутів зображень плівок плазми крові у діагностуванні патологій молочних залоз," *Оптико-електронні інформаційно-енергетичні технології*, №2, с. 52-59. 2017.
- [11] N. I. Zabolotna et al., "ROC analysis of informativeness of mapping of the ellipticity distributions of blood plasma films laser images polarization in the evaluation of pathological changes in the breast," *Proc. SPIE*, vol., no 11456, 114560I. 2020.
- [12] Н. І. Заболотна, "Інтелектуалізована система поляризаційного картографування плівок плазми крові у діагностиці онкологічного стану молочних залоз," *Оптико-електронні інформаційно-енергетичні технології*, №1, с. 39–46. 2016.
- [13] Н. І. Заболотна, "Архітектура і алгоритми функціонування та аналізу даних двовимірних систем лазерної поляриметрії біологічних тканин," *Оптико-електронні інформаційно-енергетичні технології*, № 1, с. 54–65. 2013.
- [14] L. A. Zadeh, "Fuzzy logic: principles, applications, and perspectives," *Proc. SPIE*, vol. 1468. 1991.
- [15] Н. І. Заболотна, О. В. Бісікало, В. В. Шолота, "Підтримка прийняття рішень в системі поляризаційної зображальної діагностики гістологічних зрізів за аналізом їх параметрів анізотропії," *Оптико-електронні інформаційно-енергетичні технології*, том 40, № 2, с. 29–40. 2020.

Стаття надійшла: 19.04.2024

References

- [1]N. Ghosh, I. A. Vitkin, "Tissue polarimetry: concepts, challenges, applications, and outlook," *Journal of Biomedical Optics*, vol. 16, no.11, 110801. 2011
- [2]M. Anastasiadou et al., "Polarimetric imaging for the diagnosis of cervical cancer," *Phys. Status Solidi C*, vol. 5, pp. 1423–1426. 2008.
- [3] A. Pierangelo et al., "Ex-vivo characterization of human colon cancer by Mueller polarimetric imaging," *Optics express*, vol. 19, no 2, pp. 1582–1593. 2011.
- [4] S. Alalia S., A. Vitkin, "Polarized light imaging in biomedicine: emerging Mueller matrix methodologies for bulk tissue assessment," *Journal of Biomedical Optics*, vol. 20, no 6, 061104. 2015.
- [5]О. Н. Ушенко та ін., *Лазерна поляриметрія біологічних тканин. Діагностика пухлин жіночих репродуктивних органів*. Чернівці, Україна: Чернівецький нац. ун-т, 2010.–[in Ukrainian].
- [6]Ye Wang et al., "Mueller matrix microscope: a quantitative tool to facilitate detections and fibrosis scorings of liver cirrhosis and cancer tissues," *Journal of Biomedical Optics*, vol. 21, no 7, 071112. 2016.
- [7] O. P. Mintser, N. I. Zabolotna, B. P. Oliinychenko, and P. Komada, "Differential phase analysis of laser images of a polycrystalline component of blood plasma in diagnostics of pathological changes in mammary gland," *Proc. SPIE*, vol. 8698, 86980D. 2012.

- [8] N. I. Zabolotna et al., "System of polarization phasometry of polycrystalline blood plasma networks in mammary gland pathology diagnostics," *Proc. of SPIE*, vol. 9613, 961311. 2015.
- [9] N. I. Zabolotna, K. O. Radchenko, M. H. Tarnovskiy, "System of Mueller-Jones matrix polarizing mapping of blood plasma films in breast pathology," *Proc. SPIE*. 2017, vol. 10407, 1040714. 2017.
- [10] N. I. Zabolotna, B. P. Oliinychenko, V. V. Sholota, "ROC – analiz poliaryzatsiinoho kartohrafuvannia azymutiv zobrazhen plivok plazmy krovi u diahnostuvanni patolohii molochnykh zaloz," *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, №2, s. 52-59. 2017.– [in Ukrainian].
- [11] N. I. Zabolotna et al., "ROC analysis of informativeness of mapping of the ellipticity distributions of blood plasma films laser images polarization in the evaluation of pathological changes in the breast," *Proc. SPIE*, vol., no 11456, 114560I. 2020.
- [12] N. I. Zabolotna, "Intelektualizovana systema poliaryzatsiinoho kartohrafuvannia plivok plazmy krovi u diahnostytsi onkolohichnoho stanu molochnykh zaloz," *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, № 1, s. 39–46. 2016.– [in Ukrainian].
- [13] N. I. Zabolotna, "Arkhitektura i alhorytmy funktsionuvannia ta analizu danykh dvovymirnykh system lazernoi poliarymetrii biolohichnykh tkanyn," *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, № 1, s. 54–65. 2013.– [in Ukrainian].
- [14] L. A. Zadeh, "Fuzzy logic: principles, applications, and perspectives," *Proc. SPIE*, vol. 1468. 1991.
- [15] N. I. Zabolotna, O. V. Bisikalo, V. V. Sholota, "Pidtrymka pryiniattia rishen v systemi poliaryzatsiinoi zobrazhalnoi diahnostyky histolohichnykh zriziv za analizom yikh parametriv anizotropii," *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*, tom 40, № 2, s. 29–40. 2020. – [in Ukrainian].

Відомості про авторів

Заболотна Наталія Іванівна – д.т.н., доцент, професор кафедри біомедичної інженерії та оптико-електронних систем, Вінницький національний технічний університет, Вінниця, Україна

Zabolotna Natalia Ivanivna – D.Sc., Associate Professor, Professor of the Department of Biomedical Engineering and Opto-Electronic Systems, Vinnytsia National Technical University, Vinnytsia, Ukraine

Шолота Владислава Владиславівна – асистент кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця, Україна

Sholota Vladyslava Vladyslavivna – assistant professor of computer sciences, Vinnytsia National Technical University, Vinnytsia, Ukraine

N. I. Zabolotna, V. V. Sholota

SYSTEM OF DOUBLE-WAVE LASER DIAGNOSTICS OF THE MAMMARY GLANDS BY POLARIZATION MAPPING OF IMAGES OF BLOOD PLASMA FILMS

Vinnytsia National Technical University

УДК 681.5:613

Li Jinqiong, Sergii Pavlov, Olexii Stakhov

EXPERT SYSTEMS FOR ANALYSIS OF BIOMEDICAL INFORMATION IN THE DIAGNOSIS OF ACUTE LEUKEMIA

Vinnytsia National Technical University, 95, Khmelnytske shosse, 21021, Vinnytsia, Ukraine,

Анотація. Це дослідження сприяє подальшому вдосконаленню знань, точності діагностичних методів. Це також відіграє важливу роль у діагностиці лікування гострого лейкозу сьогодні. Застосування різноманітних технологій, обмін досвідом та ідеями мають значні досягнення, які матимуть революційний ефект у медичному обслуговуванні пацієнтів, а також підвищать точність діагностики. Найбільш вагомим внеском є розробка та впровадження технологій, особливо штучного інтелекту (ШІ) або машинного навчання. Дослідження ілюструє, як моделі на основі штучного інтелекту можуть допомогти в оцінці та інтерпретації біомедичних даних, забезпечуючи більш точний діагноз і полегшуючи прийняття рішень. Натреновані на великих базах даних, такі моделі показують перспективу у виявленні тонких моделей, що вказують на різні підтипи лейкемії, що може призвести до більш точних і адаптованих методів лікування. Вивчення нових біомаркерів, використання передових методів візуалізації та використання нових технологій, таких як блокчейн, для безпеки даних представляють багатообіцяючі шляхи для прогресу. Однак вирішення таких проблем, як дотримання нормативних вимог, етичні міркування та складність визначення відповідних препаратів-кандидатів, залишається ключовим для відповідального розвитку.

Ключові слова: гострий лейкоз, діагностика та терапія, біомедичне зображення, зображення бластних і небластних клітин крові, біомедична інформація.

Abstract. This research helps to further improve the knowledge, accuracy of diagnostic techniques. It also plays an important role in the diagnosis of acute leukemia treatment today. The application of various technologies, the sharing of experiences and ideas, and even ethics all represent significant advances that will have a revolutionary effect on medical care for patients as well as improve accuracy in diagnosis. A most significant contribution is the development and introduction of technology, especially artificial intelligence (AI) or machine learning. The study illustrates how artificial intelligence-based models may be able to help in the evaluation and interpretation of biomedical data, providing more accurate diagnosis and facilitating decision-making. Trained on large databases, such models show promise in the detection of subtle patterns suggestive of different leukemia subtypes that can lead to more accurate and tailored treatment modalities. Looking ahead, the future of acute leukemia diagnosis is ripe with potential and challenges alike. Exploring novel biomarkers, incorporating advanced imaging techniques, and leveraging emerging technologies like blockchain for data security represent promising avenues for advancement. However, addressing challenges such as regulatory compliance, ethical considerations, and the complexity of identifying suitable drug candidates remains pivotal for responsible evolution.

Keywords: acute leukemia, diagnosis and therapy, biomedical image, images of blast and non-blast blood cells

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-157-164>.

Introduction

Editing of biomedical images usually involves preprocessing to make them clear and sharp, or free from noise or artifacts. This important step improves the images' clarity and reliability so that the following analyses are done with sharp, precise visual data (Wagner et al., 2012). Methods such as noise reduction, contrast adjustment, and image normalization are used for preprocessing the images. In this way preprocessing helps ensure that the next steps of feature extraction and classification use high-quality data, reducing possible errors. After the images undergo preprocessing, the next step is to extract features of importance that reflect key biological information. Lab techniques to extract features focus on finding quantifiable properties unique to the image, such as cell morphology, or texture and intensity variations (Arber et al., 2017). These extracted features provide quantifiable measures of the cellular characteristics, which can then be used to distinguish normal vs leukemic cells. Where feature extraction is crucial, capture the subtle differences in cells that help clinicians pin down an accurate diagnosis via texture analysis, shape descriptors, and other image intensity-related features.

After feature extraction, classification allows cells to be separated from the images and identified. These algorithms use advanced machine learning methods to identify the clusters formed by these extracted cells (Wagner et al., 2012). For example, sophisticated classification methods such as neural networks or support vector machines separate the different cell types especially problems in leukemic blast prediction (Harrison & Johansson, 2015). Segmentation techniques also make it easier to determine the boundaries of cells, so that abnormal cells can be more clearly identified and counted—which is crucial in acute leukemia diagnosis.

Combining the data from image analysis with clinical information and patient history is ultimately what constitutes true diagnostic support. Although image analysis provides important visual data, integrating it with clinical information laboratory tests, and genetic markers as well as the symptoms of individual patients offers more context for diagnostics (Wagner et al., 2012). Such integration provides completeness, adding to the validity of diagnosis. When the visual findings are placed within the context of the patient's entire health history, clinicians then have a picture that serves as an essential basis for accurate diagnosis and treatment planning. All of these aspects in interpreting biomedical images are crucial to the proper diagnosis of acute leukemia (Arber et al., 2017). All these from preprocessing to feature extraction, classification, and integration of the extracted features with clinical data are crucial in coming up with a better understanding of leukemia pathology [1,2].

The purpose of this work is to develop a conceptual model of an expert system for diagnosing acute leukemia using computer microscopy methods, as well as to analyze the influence of factors that influence the result of recognition of poorly formalized objects (images of blast and non-blast cells).

Decision Support in Acute Leukemia Diagnosis

Technology and the use of data-driven tools are integrated throughout acute leukemia diagnosis, supporting decision-making by medical professionals as they develop diagnostic hypotheses in light of objective facts. It uses technologies such as artificial intelligence, computational models, and clinical databases to improve the accuracy of diagnosing acute leukemia quickly (Arber et al., 2017). Starting from patient data, which incorporates genetic info and proteomic studies as well as clinical information on each case. This comprehensive approach allows for an overall health picture of the patient and leads to a more accurate above all subtle diagnosis. Differentiating between the various subtypes of acute leukemia is a key function served by decision support systems (Wagner et al., 2012; Cicconi & Lo-Coco, 2016). By spirit-like advanced algorithms, these systems can break down complex molecular and genetic markers to help doctors recognize the distinct traits that define each subtype to be able to guide appropriate treatment strategies [3,4].

The real-time processing capabilities of decision support tools provide valuable insight into acute leukemia diagnosis. This is especially valuable in emergencies, as it allows healthcare professionals to rapidly analyze key data at a glance, reach fast decisions, and begin treatment with the timeliest information possible (Wagner et al., 2012). Unlike traditional mathematics, machine learning models integrated into decision support systems always learn from new data and experiences (Harrison & Johansson, 2015). This ability to adapt guarantees that the diagnostic equipment continually changes, becoming ever more accurate and commensurate with developments in medical science and technology.

Tailored to fit individual patients, decision support tools aid personalized medicine. Such tools can thus evaluate a patient based on their unique genetic makeup, clinical history, and other relevant factors to fine-tune treatment recommendations. In this way, therapeutic interventions are enhanced for better results (Harrison & Johansson, 2015). It attempts to resolve the difficulty of interpreting enormous datasets in acute leukemia diagnosis with decision support. These tools, which use advanced computational models to identify patterns and associations too subtle for simple human interpretation alone, greatly improve diagnostic precision. Besides helping to make the initial diagnosis, decision support systems also help healthcare professionals predict disease courses. Analysis of historical data and the reaction to treatment help estimate what pattern acute leukemia will likely take so that care plans can be more proactive and personalized [5,6].

Validation and Performance Evaluation of the System

Therefore, the development and implementation of any system must go through two important phases such as validation and performance evaluation. These will ensure that a system is reliable, accurate, or able to effectively achieve its intended goals (Arber et al., 2017). Given acute leukemia diagnosis as an example of the use of a bio-information system, these processes can all help to build trust with users and healthcare professionals, as well as regulatory bodies (Harrison & Johansson, 2015). The first step in validation is to verify that the system meets pre-established requirements and specifications. This means that the system works appropriately for these specific needs and objectives.

The validation process even involves the system's data integrity and security measures. The system must meet safeguards for the patient data, maintain confidentiality, and prevent unintentional access. Performance evaluation measures system performance in handling different workloads and datasets. This entails measuring the system's response time, its computational efficiency, and its scalability so that it can deal with growing and growing amounts of biomedical data. A standard method for performance evaluation is benchmarking. That is, comparing the system's performance to established standards or existing systems of a similar nature (Harrison & Johansson, 2015). This allows areas for improvement to be identified and establishes a foundation of acceptable performance metrics.

In the process of validation and performance evaluation, artificial or historical datasets that represent realistic problems are frequently heard. This provides a basis for controlled testing, verifying that the system is robust across different use cases and helping to understand its generalizability (Harrison & Johansson, 2015). To

reduce the risk of overfitting and increase its applicability to a wider patient population, cross-validation techniques are used herein to evaluate system performance on assorted datasets. When evaluating the diagnosis of acute leukemia, validation and performance assessment should relate to whether the system can identify various subtypes of leukemia; accurately predict treatment responses; and provide clinically useful information (Arber et al., 2017). These outcomes are vital for better decision-making by healthcare professionals.

Clinical validation is working with medical professionals to see how the diagnostic outputs of a system match up against actual patient outcomes. In this way, the system's predictions are checked for congruence with real-world clinical situations, providing evidence of its use in a medical context (Arber et al., 2017). Verification is also an iterative process, with feedback from clinicians and end-users guiding refinement. Addressing new challenges, incorporating new medical knowledge into the system, and improving performance requires a steady stream of updates to, and upgrades of, the system [7].

For this reason, easily interpretable models are preferred in validation and performance evaluation to ensure that clinicians understand the reasons for the system's predictions. These transparent models engender trust among healthcare providers and encourage responsible use of the system in clinical application. In AI-based models, in particular, addressing biases in the system is a big part of validation. Bias may be introduced by an unbalanced distribution of training data, and we must strive to avoid such biases and ensure fair and impartial results for different patient groups (Harrison & Johansson, 2015). The system's ability to detect leukemia and to distinguish between subtypes is measured by quantitative metrics such as sensitivity, specificity, and positive predictive value. These metrics offer a standardized way to measure the diagnostic accuracy of the system.

Evaluation of the system's ability to discriminate between classes is often performed by using Receiver Operating Characteristic (ROC) curves and area under the curve (AUC) analysis. These pictures show the trade-off between sensitivity and specificity. After implementation, it is important to monitor the performance of the system on an ongoing basis, to detect any drift in accuracy or efficiency (Harrison & Johansson, 2015). Regular audits and upgrades further enhance the system's long-term stability, while keeping it in step with constantly changing health care standards. Verification and performance assessment should take the usability of the system from an end-user point. Inspects critical to usability assessment include user feedback, ease of integration into existing workflows, and overall impact on clinical decision-making.

Compliance with regulatory standards such as medical device regulations and data privacy regulations is an integral part of the verification process. Compliance ensures that patient rights are protected and the system is used ethically in hospitals (Harrison & Johansson, 2015). External validation-- independent assessment by external bodies or regulatory agencies adds extra weight to the system. Third-party verification enhances the trustworthiness and assurance that people have in the system. Documentation of validation and performance evaluation procedures is necessary for transparency and accountability.

Precision of the system's diagnosis

The performance of the IBS might also be impacted by the setting in which it is utilized. The precision of the system's diagnosis can be influenced by several circumstances, such as the accessibility to superior biological data and the proficiency of the physicians utilizing it.

Mathematical Model

$$dN/dt = p - dN - \beta * N * L + K * N * L$$

$$dL/dt = \beta * N * L - K * N * L - dL$$

$$dM/dt = K * N * L - dM - sM$$

The equations above can be combined in a matrix form as shown below:

$$A = \begin{bmatrix} dN/dt & dL/dt & dM/dt \\ p - dN & \beta * NL & K * NL \\ 0 & \beta * NL - K * NL & -dM - sM \end{bmatrix}$$

where:

- 1). N(t) is the number of normal cells at time t
- 2). L(t) is the number of leukemic cells at time t
- 3). M(t) is the number of mature blood cells at time t
- 4). p is the rate of production of new normal cells
- 5). d is the rate of death of normal cells
- 6). a is the rate of proliferation of leukemic cells due to interaction with normal cells
- 7). b is the rate of differentiation of leukemic cells into mature blood cells
- 8). s is the rate of death of mature blood cells
- 9). beta is the rate of proliferation of leukemic cells
- 10). K is the rate of differentiation of leukemic cells

The figure below shows the mathematical model that was made and used during the simulation to obtain the graph.

The analysis of biomedical images in acute leukemia diagnosis entails meticulous steps, from preprocessing to feature extraction and integration with clinical data. Image preprocessing ensures refined data quality, while feature extraction and classification algorithms identify distinctive cellular attributes. Integration with clinical data enriches the diagnostic process, contextualizing visual findings within the patient's broader health profile. Moreover, advancements in hardware, such as high-resolution imaging systems and GPU accelerators, enhance imaging clarity, expediting data processing and interpretation (fig 1).

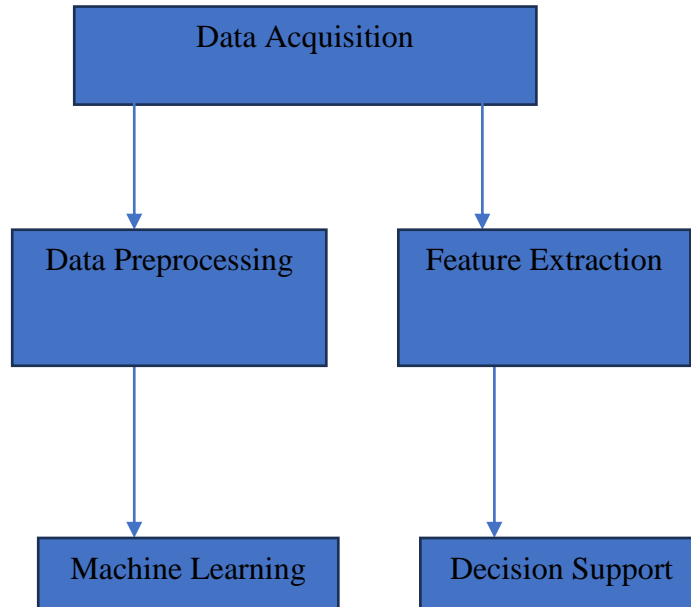


Figure 1 - expediting data processing and interpretation

Looking ahead, the future of acute leukemia diagnosis is ripe with potential and challenges alike. Exploring novel biomarkers, incorporating advanced imaging techniques, and leveraging emerging technologies like blockchain for data security represent promising avenues for advancement. However, addressing challenges such as regulatory compliance, ethical considerations, and the complexity of identifying suitable drug candidates remains pivotal for responsible evolution.

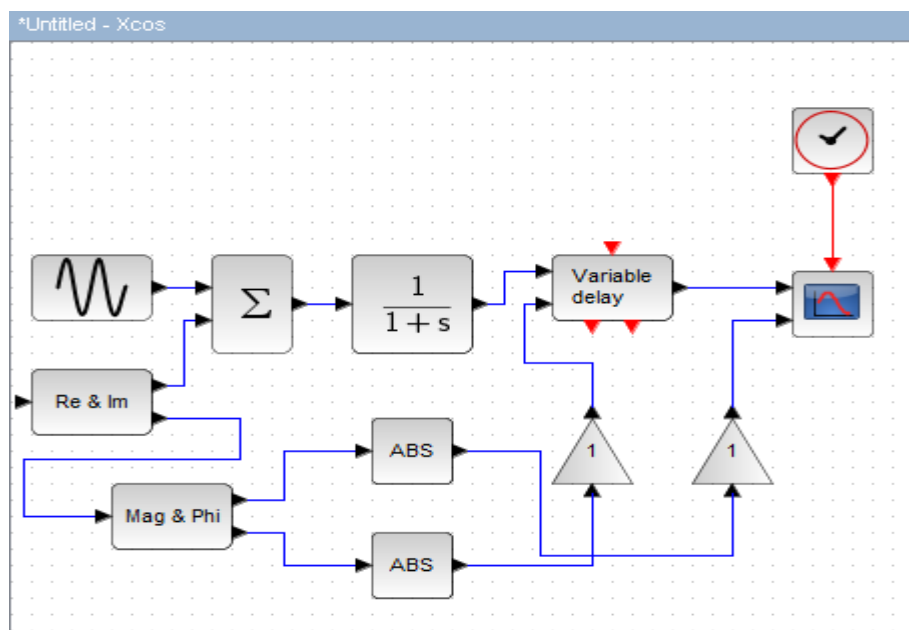


Figure 2 - The future of acute leukemia diagnosis

Pre-processing of Two-Dimensional Biomedical Images

Pre-processing of two-dimensional medical biomedical images is a key step in improving the quality and meaning of data for decision support at acute leukemia diagnosis. It is this critical step that uses various techniques such as filtering, contouring, and normalization to improve the quality of the images being studied (Rawat et al., 2015). Each of these techniques performs a different function in cleansing the dataset. It is an important step towards more precise and informed decision support. Pre-processing includes several operations that precede processing. The most important one is filtering, which gets rid of noise in biomedical images. However, the data can be distorted by noise, which often arises during image acquisition (Peters & Ansari, 2011). Filtering techniques pick out those features that scientists want to emphasize and suppress whatever noise is there, yielding a higher net signal-to-noise ratio. The final product is a more clean and accurate reflection of the underlying structures in those images. The figure 3 below shows the graph obtained from the processing of the results.

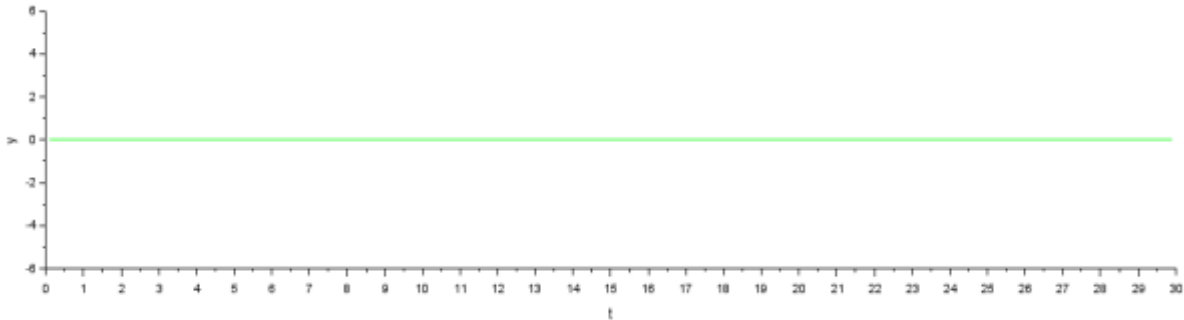


Figure 3 – Graph obtained from the processing of the results.

Another important technique in pre-processing is contouring, which identifies and delineates structures within biomedical images. Contouring defines the borders and structure of interest and makes possible a more in-depth analysis of specific areas (Peters & Ansari, 2011). This step is especially important in the case of acute leukemia diagnosis, where careful identification of abnormalities such as extra cell structures means that decision-making support systems can make more reasonable assessments. To ensure that intensity levels are always constant across different regions of the biomedical images, normalization is used. This is an important means of equalizing differences in illumination and contrast, resulting in a consistent dataset. Normalization reduces the chance that variations in imaging conditions will introduce biases. It levels out differences between images, helping to ensure accurate and reliable decision support (Rawat et al., 2015). These pre-processing techniques, taken together as a whole, create a refined dataset that serves as raw material for subsequent analysis. By cleaning out the noise, enriching through contouring, and normalizing this dataset to provide decision-support systems with a more accurate and stable formulation of biomedical information (Rawat et al., 2015). It improves the system's ability to detect fine patterns and oddities, allowing for better decision-making when it comes time to diagnose acute leukemia.

Contour Preparation and Formation of Templates - Masks of Bioobjects

The method of contour preparation and the formation of templates, also known as masks of bio-objects, are essential in the detailed analysis of biomedical images. Contours help delineate specific structures or anomalies, providing a basis for further examination (Peters & Ansari, 2011). Templates or masks are crafted to identify and isolate bio-objects of interest, such as leukemia cells or abnormal tissue (Rawat et al., 2015). This meticulous approach aids in creating a targeted and precise analysis, facilitating decision support by focusing on the most relevant information within biomedical images. The figure 4 below shows the frequencies of the different genders during data collection.

Development of the Architecture of a Fuzzy Expert Optical-Electronic System

The architecture of a fuzzy expert optical-electronic system plays a key role in analyzing biomedical images for leukemia diagnosis. Fuzzy logic, an approach that deals with uncertainty and imprecision, is integrated into the system's architecture. This enables the system to handle the inherent complexities and variations present in biomedical images more effectively (Rawat et al., 2015). The combination of optical and electronic components enhances the system's capability to capture, process, and interpret intricate details, contributing to a more nuanced decision-support mechanism in leukemia diagnosis. The development of such a sophisticated architecture aligns with the demand for advanced technological solutions in the field of medical imaging and diagnostic support. The figure below shows the frequency of the immune blood cells.

Frequencies

Frequencies of gender

gender	Counts	% of Total	Cumulative %
female	32	51.6 %	51.6 %
male	30	48.4 %	100.0 %

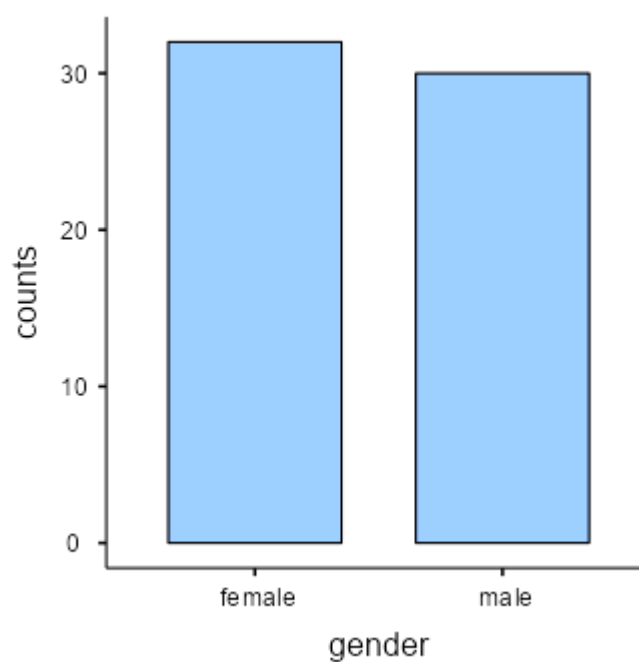


Figure 4 – Frequencies of the different genders during data collection.

Frequencies of peripheral blood immature cells

peripheral blood immature cells	Counts	% of Total	Cumulative %
0 .03	1	3.3 %	3.3 %
0 .04	1	3.3 %	6.7 %
0 .32	1	3.3 %	10.0 %
0.01	1	3.3 %	13.3 %
0.02	1	3.3 %	16.7 %
0.03	1	3.3 %	20.0 %
0.04	1	3.3 %	23.3 %
0.06	2	6.7 %	30.0 %
0.09	1	3.3 %	33.3 %
0.13	1	3.3 %	36.7 %
0.14	3	10.0 %	46.7 %
0.16	1	3.3 %	50.0 %

Frequencies of peripheral blood immature cells

peripheral blood immature cells	Counts	% of Total	Cumulative %
0.2	1	3.3 %	53.3 %
0.28	1	3.3 %	56.7 %
0.45	1	3.3 %	60.0 %
0.51	1	3.3 %	63.3 %
0.6	1	3.3 %	66.7 %
0.64	1	3.3 %	70.0 %
0.68	1	3.3 %	73.3 %
0.7	1	3.3 %	76.7 %
0.74	1	3.3 %	80.0 %
0.81	3	10.0 %	90.0 %
0.93	2	6.7 %	96.7 %
0.96	1	3.3 %	100.0 %

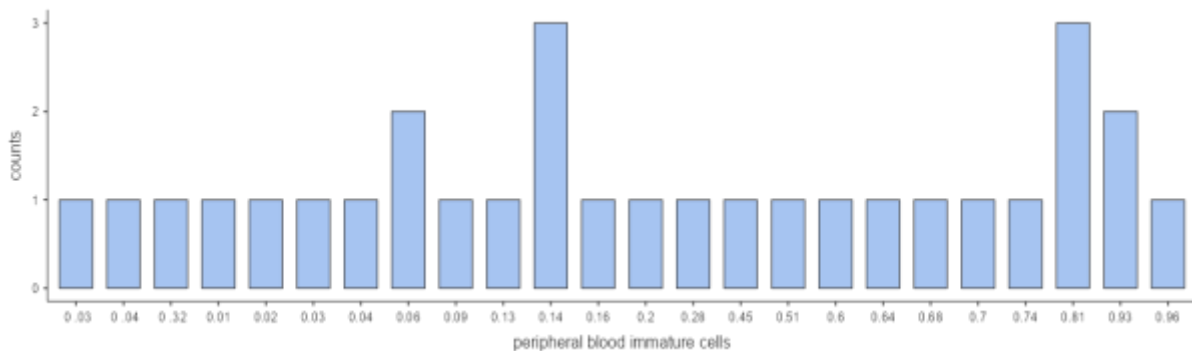


Figure 5 - The analysis of biomedical images in acute leukemia diagnosis

The analysis of biomedical images in acute leukemia diagnosis (fig 5) entails meticulous steps, from preprocessing to feature extraction and integration with clinical data. Image preprocessing ensures refined data quality, while feature extraction and classification algorithms identify distinctive cellular attributes. Integration with clinical data enriches the diagnostic process, contextualizing visual findings within the patient's broader health profile. Moreover, advancements in hardware, such as high-resolution imaging systems and GPU accelerators, enhance imaging clarity, expediting data processing and interpretation.

Conclusions

Looking ahead, the future of acute leukemia diagnosis is ripe with potential and challenges alike. Exploring novel biomarkers, incorporating advanced imaging techniques, and leveraging emerging technologies like blockchain for data security represent promising avenues for advancement. However, addressing challenges such as regulatory compliance, ethical considerations, and the complexity of identifying suitable drug candidates remains pivotal for responsible evolution.

References

- [1] Abdeldaim, A. M., Sahlol, A. T., Elhoseny, M., & Hassanien, A. E. (2018). Computer-aided acute lymphoblastic leukemia diagnosis system based on image analysis. *Advances in Soft Computing and Machine Learning in Image Processing*, 131-147.

- [2] Ahmed, I. A., Senan, E. M., Shatnawi, H. S. A., Alkhraisha, Z. M., & Al-Azzam, M. M. A. (2023). Hybrid techniques for the diagnosis of acute lymphoblastic leukemia based on fusion of CNN features. *Diagnostics*, 13(6), 1026.
- [3] Ansari, S., Navin, A. H., Sangar, A. B., Gharamaleki, J. V., & Danishvar, S. (2023). A customized efficient deep learning model for the diagnosis of acute leukemia cells based on lymphocyte and monocyte images. *Electronics*, 12(2), 322.
- [4] Arber, D. A., Borowitz, M. J., Cessna, M., Etzell, J., Foucar, K., Hasserjian, R. P., ... & Vardiman, J. W. (2017). Initial diagnostic workup of acute leukemia: guideline from the College of American Pathologists and the American Society of Hematology. *Archives of pathology & laboratory medicine*, 141(10), 1342-1393.
- [5] С. В. Павлов, Й. Р. Салдан, О. В. Карась, і С. В. Тимчик, «Аналіз методів і систем діагностики діабетичної ретинопатії», *Опт-ел. інф-енерг. техн.*, вип. 46, вип. 2, с. 135–141, 2023.
- [6] Л. Цзіньцун і С. Павлов «Експертна біоінформаційна система діагностики форм гострого лейкозу на основі аналізу біомедичної інформації», *ІТКІ*, вип. 58, вип. 3, с. 84–93, 2023.
- [7] Wójcik, W., Pavlov, S., Kalimoldayev, M. (2019). *Information Technology in Medical Diagnostics II*. London: Taylor & Francis Group, CRC Press, Balkema book. – 336 Pages, <https://doi.org/10.1201/9780429057618>.
- [8] Chen, K. X. (2020). Academician kai-xian chen talks about the development of traditional chinese medicine and global medicine. *World Journal of Traditional Chinese Medicine*, 6(1), 1-11.
- [9] Chiaretti, S., Zini, G., & Bassan, R. (2014). Diagnosis and subclassification of acute lymphoblastic leukemia. *Mediterranean journal of hematology and infectious diseases*, 6(1).
- [10] Cicconi, L., & Lo-Coco, F. (2016). Current management of newly diagnosed acute promyelocytic leukemia. *Annals of Oncology*, 27(8), 1474-1481.
- [11] Crow, H. (2012). 1 Scaling Technique for Web Based Management Systems in Bioinformatics. *Life Science Journal*, 9(3).
- [12] Davis, A. S., Viera, A. J., & Mead, M. D. (2014). Leukemia: an overview for primary care. *American family physician*, 89(9), 731-738.
- [13] Estey, E. H. (2012). Acute myeloid leukemia: 2012 update on diagnosis, risk stratification, and management. *American journal of hematology*, 87(1), 89-99.
- [14] Grimwade, L. F., Fuller, K. A., & Erber, W. N. (2017). Applications of imaging flow cytometry in the diagnostic assessment of acute leukaemia. *Methods*, 112, 39-45.
- [15] Haferlach, T., Kohlmann, A., Wiczorek, L., Basso, G., Te Kronnie, G., Béné, M. C., ... & Foa, R. (2010). Clinical utility of microarray-based gene expression profiling in the diagnosis and subclassification of leukemia: report from the International Microarray Innovations in Leukemia Study Group. *Journal of clinical oncology*, 28(15), 2529.
- [16] Harrison, C. J., & Johansson, B. (2015). Acute lymphoblastic leukemia. *Cancer Cytogenetics: Chromosomal and Molecular Genetic Aberrations of Tumor Cells*, 198-251.

Видано за грантової підтримки Національного фонду досліджень України в рамках проекту 2022.01/0135 "Розробка лазерно-фотонного лікувально-діагностичного комплексу медичної реабілітації пацієнтів з політравмами різного ступеня важкості"

Li Jinqiong – postgraduated student of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

Pavlov Sergii – D.Sc., Professor of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

Stakhov Oleksii - Ph.D., Senior lector of software Department of Vinnytsia National Technical University,

Лю Цзіньцун, Сергій Павлов, Олексій Стахов

ЕКСПЕРТНА БІОІНФОРМАЦІЙНА СИСТЕМА ДІАГНОСТИКИ ФОРМ ГОСТРОГО ЛЕЙКОЗУ НА ОСНОВІ АНАЛІЗУ БІМЕДИЧНОЇ ІНФОРМАЦІЇ

Вінницький національний технічний університет

УДК 004.738

А. Я. Кулик¹, В. І. Ревенок¹, Я. А. Кулик², О. І. Нікольський¹

РОЗРОБКА, ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ ПРОГРАМ-СИМУЛЯТОРІВ ЛАБОРАТОРНИХ РОБІТ З МЕДИЧНОЇ ТА БІОЛОГІЧНОЇ ФІЗИКИ

¹ Вінницький національний медичний університет ім. М.І. Пирогова, Вінниця² Вінницький національний технічний університет, Вінниця

Анотація. В статті розглянута важливість симуляційної освіти, яка допомагає студентам-медикам набути реального досвіду та навичок, необхідних для подальшого професійного розвитку. Особлива увага приділена комп'ютерним симуляторам при проведенні практичних і лабораторних занять. Розроблено і використовується в навчальному процесі сім програм-симуляторів лабораторних робіт з дисципліни «Медична та біологічна фізика». В статті в якості прикладу представлена програма-симулятор лабораторної роботи «Вивчення в'язкості рідини». Проведено аналіз варіантів формування результатів експерименту програмою-симулятором проти вимірювання значень цих результатів безпосередньо на екрані комп'ютера. Запропоновано методику для визначення діапазону генератора випадкових чисел з метою формування індивідуальних результатів експерименту програмою-симулятором на основі обчислення довірчого інтервалу. Доведено, що мінімальне і максимальне значення для генератора випадкових чисел доцільно вибирати з довірчих інтервалів, імовірність яких вища 0,95.

Ключові слова: симулятори, програми-симулятори, медична освіта, біологічна фізика, медична фізика.

Abstract. The article considers the importance of simulation education, which helps medical students acquire real experience and skills necessary for further professional development. Special attention is paid to computer simulators during practical and laboratory classes. Seven simulator programs for laboratory work in the discipline "Medical and Biological Physics" have been developed and are used in the educational process. As an example, the article presents a program-simulator of laboratory work "Study of liquid viscosity". An analysis of the options for forming the results of the experiment using a simulator program versus measuring the values of these results directly on the computer screen was carried out. A technique for determining the range of the random number generator for the purpose of forming individual results of the experiment by the simulator program based on the calculation of the confidence interval is proposed. It has been proven that the minimum and maximum values for the random number generator should be chosen from confidence intervals, the probability of which is higher than 0.95.

Key words: simulators, simulator programs, medical education.

DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-165-172>.

Вступ

Для встановлення правильного діагнозу захворювання і вибору відповідного напрямку лікування необхідна наявність високотехнологічного обладнання і кваліфікованого медичного персоналу. В процесі навчання в медичних закладах освіти студенти опановують теоретичну базу і набувають певного практичного досвіду. Саме останнє поглиблює і розширює теоретичні знання та формує необхідні вміння та навички [1].

Однією з основних технологій практичної підготовки сучасних медичних фахівців є симуляційна освіта. Вона використовує модель професійної діяльності з метою надання можливості кожному студенту виконати професійну діяльність або її елемент відповідно до професійних стандартів та/або порядками (правилами) надання медичної допомоги [2, 3]. В якості симуляторів широко використовуються фантоми, муляжі, анатомічні моделі, тренажери, комп'ютеризовані манекени, система ситуаційних завдань та інші засоби навчання, які допомагають створити реалістичне середовище для навчання та тренування студентів в різних галузях знань. Ці симулятори і засоби навчання розширюють можливості традиційного класичного навчання, дозволяючи студентам активно займатися практичною діяльністю і відчувати себе частинами реального процесу.

Фантоми, анатомічні моделі та муляжі допомагають студентам медикам вивчати анатомію та виконувати різні медичні процедури на практиці без ризику для пацієнтів. Тренажери і комп'ютеризовані манекени відтворюють складні сценарії, допомагаючи підготувати фахівців для відповіді на випадкові ситуації, які можуть виникнути в реальному житті. Системи ситуаційних завдань навчають студентів приймати рішення в стресових ситуаціях та адаптуватися до нових обставин.

З використанням віртуальної реальності та розширеної реальності студенти можуть зануритися в імітовані середовища для навчання та віртуальних тренувань, що робить навчання більш захоплюючим та практичним. Моделюючі програми допомагають майбутнім фахівцям випробовувати нові рішення та ідеї без супутнього ризику для пацієнта.

Загалом, симулятори та інші засоби навчання створюють можливості для більш інтерактивного, практичного та ефективного освітнього процесу, допомагаючи студентам набути реального досвіду та навичок, необхідних для подальшого професійного розвитку [4].

Особливо спочатку в період пандемії, а потім повномасштабної війни, коли значна доля аудиторних занять перейшла в режим дистанційного навчання, подальший розвиток отримала комп'ютерна симуляція. Наявність ноутбука або монітора і комп'ютера з клавіатурою і мишею дозволяє працювати з моделями реальних процесів, віртуальними пацієнтами, тренажерами віртуальної реальності, зокрема, з ефектом присутності. Однак, слід зазначити, що симуляційні технології мають ширше використання на старших курсах медичних навчальних закладів. На молодших курсах, де викладають дисципліни теоретичного профілю, в основному обмежуються класичними прийомами – використання лабораторних макетів, наочних зразків і т. п. В умовах дистанційного навчання лекції, семінари, практичні та лабораторні заняття проводяться з використанням відомих сервісів, таких як MS Teams, Google Meet, Zoom інших хмарних сервісів [5, 6]. А знання оцінюються за допомогою сформованих текстових завдань, тестів. Стоєвню підготовки і проведення лекцій, семінарів і певних видів практичних занять, дані платформи мають в наявності необхідні інструменти: відео конференції, блокнот, чат та інші. Щодо практичних робіт з проведенням експерименту в середовищі MS Teams, Google Meet, Zoom можна застосовувати презентації або відео, де представлені прилади та інші технічні засоби, і демонстрацію їх роботи як в статичній, так і динамічній. Результатом виконання експерименту є таблиця з даними, яка передається студентам для подальшого опрацювання і формування висновків. Студенти, на жаль, за таких умов, не мають можливості безпосередньо приймати участь у проведенні експериментів і виступають у ролі спостерігачів.

Серед відомих програм симуляторів, зокрема з фізики, слід зазначити PhET - це понад 60 відкритих інтерактивних моделювань природничих і математичних концепцій, створене Університетом Колорадо в Боулдері [7]. Студенти можуть запускати симуляції, маніпулюючи різними аспектами даних, щоб зрозуміти природу того чи іншого явища. В Україні даний проект з успіхом використовують на уроках фізики, хімії в загальноосвітніх школах. У вищих навчальних закладах PhET є менш поширеним скоріше по причині вивчення не стільки суті явищ, скільки застосування їх у практичному аспекті.

Також відомі безкоштовні інтерактивні ресурси, STEM-заходи, де представлені наочні симулятори, відеофільми, текстова інформація. LabXchange – онлайн-платформа для наукової освіти від Гарвардського університету, яка включає розділи з фізики, математики і біології [8], Concord Consortium - онлайн-платформа для освіти з фізики, хімії, математики, науки про життя, Землю і космос [9], Merlot (hub) [10] - база даних від медичного інституту Говарда Хьюза, яка включає симуляції з фізики, хімії, біології, сільського господарства, інформатики, інженерії, астрономії, математики та статистики.

Віртуальні лабораторні симуляційні кейси від Labster нагадують справжню лабораторію [11]. За допомогою мишки студент переміщується у віртуальній лабораторії та проводить лабораторні дослідження. Віртуальний лаборант або лабораторний майданчик дає поради на цьому шляху. Віртуальні експерименти перериваються питаннями з декількома варіантами відповідей, на які необхідно правильно відповісти, перш ніж приступити до них. При цьому студент заробляє бали за правильні відповіді на запитання. Викладач може слідкувати за індивідуальними відповідями студентів, а також за тим, чи пройшли вони всі етапи симуляції. Під час віртуальних експериментів з'являються анімації хімічних або молекулярних процесів. Проведені дослідження [12] довели, що використання віртуальних лабораторних симуляцій сприяє підвищенню дослідницької активності студентів і мотивації, а також є ефективним доповненням до традиційної навчальної діяльності.

Мета

Розробка програм симуляторів лабораторних робіт з дисципліни «Медична та біологічна фізика».

Результати роботи

Симулятори реалізують завдання у відповідності до лабораторного практикуму з медичної та біологічної фізики [13]. Алгоритм виконання практичної роботи з показаний на рис.1.

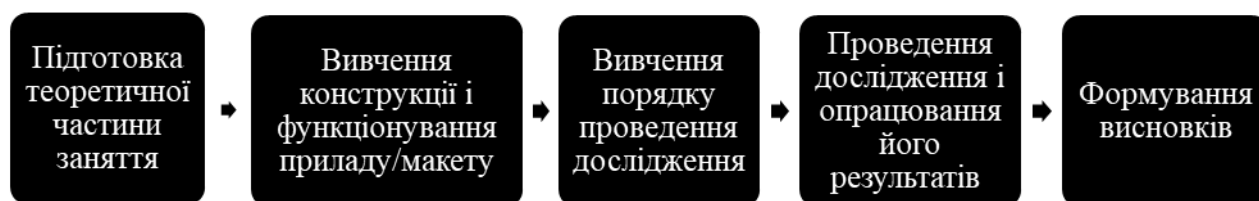


Рисунок 1 – Алгоритм виконання практичної роботи з дисципліни «Медична та біологічна фізика»

Враховуючи, що використання симуляторів передбачає застосування інтернет-браузерів, для розробки була обрана мова розмітки гіпертексту html, каскадні таблиці стилів css і мова програмування JavaScript. В цілому розроблено і використовується в навчальному процесі сім програм-симуляторів лабораторних робіт з дисципліни «Медична та біологічна фізика» [14-19].

В якості прикладу розглянемо виконання лабораторної роботи «Вивчення в'язкості рідини» з дисципліни «Медична та біологічна фізика» з використанням програми симулятора.

Відповідно до методичних вказівок з лабораторного практикуму [13] і алгоритму представленому на рис. 1, студентам пропонується вивчити теоретичний матеріал з методів вимірювання коефіцієнта динамічної в'язкості рідини, а також ознайомитись з конструкцією і принципом роботи віскозиметра Оствальда. Ознайомитися з будовою віскозиметра Оствальда можливо (рис 2), натиснувши кнопку «Довідка» на основному екрані симулятора безпосередньо після його завантаження (рис 3).

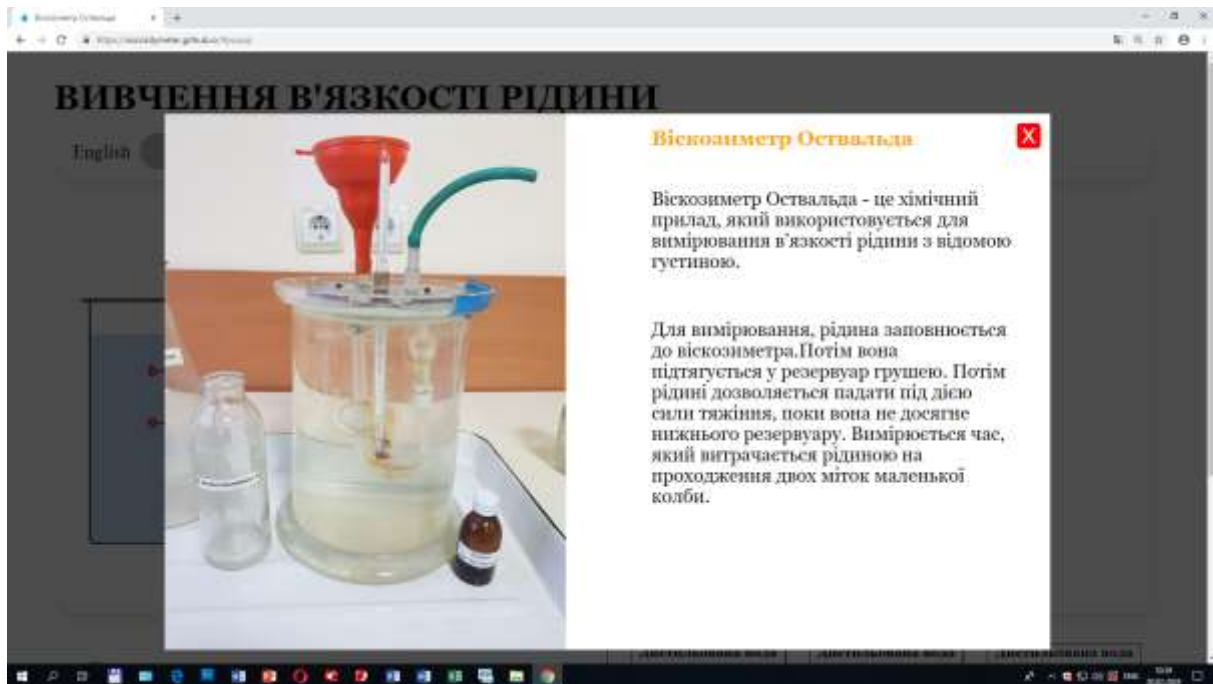


Рисунок 2 – Інтерфейс довідки програми-симулятора віскозиметра Оствальда

Далі симулятор відповідно до порядку виконання роботи [13] реалізує наступні завдання.

ЗАВДАННЯ 1. ВИМІРЮВАННЯ ЧАСУ ВИТІКАННЯ РІДИН ЧЕРЕЗ КАПІЛЯР ВІСКОЗИМЕТРА.

1.1. На основному екрані симулятора (рис. 3) вибрати в якості досліджуваної рідини дистильовану воду при температурі 24°C і підтвердити вибір, натиснувши кнопку «Підтвердити».

1.2. Залити дистильовану воду в віскозиметр, натиснувши кнопку «Залити рідину».

1.3. Підтягнути рідину гумовою грушою вище мітки 8, використавши кнопку «Підтягнути рідину».

1.4. Виміряти час τ_0 витікання дистильованої води через капіляр між мітками 8 і 9, натиснувши кнопку «Почати експеримент». Провести 5 таких вимірів і результати автоматично будуть занесені в таблицю.

1.5. Завершити експеримент з дистильованою водою, натиснувши кнопку «Злити воду».

1.6. Вибрати досліджувану рідину дистильована вода зі спиртом при температурі 24°C і натиснути кнопку «Підтвердити».

1.7. Провести 5 вимірювань часу τ_{x1} витікання досліджуваної рідини при температурі $t_1=24^{\circ}\text{C}$ аналогічно пунктам 2.2 – 2.5. Результати автоматично будуть занесені в таблицю.

1.8. Значення ρ_0 , η_0 , ρ_x наведені в таблиці для температури $t_1=24^{\circ}\text{C}$.

ЗАВДАННЯ 2. ВИВЧЕННЯ ВПЛИВУ ТЕМПЕРАТУРИ НА В'ЯЗКІСТЬ РІДИНИ.

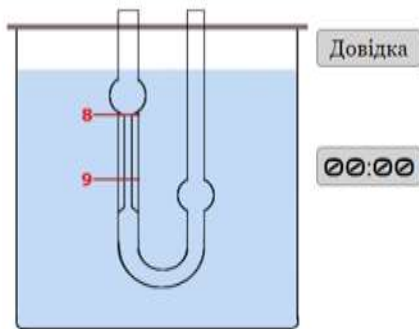
2.1. На основному екрані симулятора (рис. 3) вибрати в якості досліджуваної рідини дистильовану воду зі спиртом при температурі 32°C і натиснути кнопку «Підтвердити».

2.2. Провести 5 вимірювань часу τ_{x2} витікання досліджуваної рідини при температурі $t_2=32^{\circ}\text{C}$ аналогічно пунктам 1.2 – 1.5. Результати автоматично будуть занесені в таблицю.

Симулятор може бути встановлений на сервері, а студенти – виконувати роботу через інтернет-браузер.

ВИВЧЕННЯ В'ЯЗКОСТІ РІДИНИ

English Українська



Оберіть рідину та температуру

- Дистильована вода при $t = 24^{\circ}\text{C}$
- Дистильована вода + спирт при $t = 24^{\circ}\text{C}$
- Дистильована вода + спирт при $t = 32^{\circ}\text{C}$

Підтвердити

- Залити рідину
- Підтягнути рідину
- Почати експеримент
- Злити воду

№	Дистильована вода		Дистильована вода + спирт		Дистильована вода + спирт	
	$t_1 = 24^{\circ}\text{C}$		$t_1 = 24^{\circ}\text{C}$		$t_2 = 32^{\circ}\text{C}$	
	$\tau_0,$ с	$\tau_{\text{ж}},$ с	$\tau_{\text{ж}},$ с	$\tau_{\text{ж}},$ с	$\tau_{\text{ж}},$ с	$\tau_{\text{ж}},$ с
	$\rho_0 =$ 0,99733 кг/м ³	$\eta_0 =$ 0,00091 Н·с/м ²	$\rho_{\text{ж}} =$ 0,80741 кг/м ³	$\eta_{\text{ж}} =$?		

Рисунок 3 – Інтерфейс “Вивчення в’язкості рідини” програми-симулятора віскозиметра Оствальда

Таким чином, студенти після виконання лабораторної роботи на симуляторі отримають індивідуальні результати проведення експерименту.

При проектуванні симуляторів виникають різні питання як щодо методики проведення експерименту, так і програмно-технічної його реалізації. Результати експерименту можуть автоматично записуватись, наприклад, у таблицю, а можуть вимірюватись студентом з екрану. У вищенаведеному прикладі вбудований секундомір кожного разу автоматично вимірює час протікання досліджуваної рідини між мітками у віскозиметрі Оствальда і результат програмно записується в таблицю. Роль студента у даному випадку полягає у налаштуванні вхідних параметрів (вибір рідини, заливка її у віскозиметр, підтягуванні рідини вище відповідних міток і запуск експерименту). Результати експерименту студент візьме з таблиці для подальшого опрацювання. Другий варіант, який передбачає самостійне вимірювання результатів експерименту з екрану, є більш наближеним до реальності в плані залучення студента до виконання лабораторної роботи. Для наведеної вище роботи студент має самостійно вимірювати час протікання рідини між мітками 8 і 9. Але, з іншої сторони, існує велика ймовірність фальсифікації або використання результатів, отриманих іншими студентами. Тому формування результатів експерименту програмою є більш прийнятним варіантом. Крім того, результат обробки експериментальних даних в цьому випадку може бути перевірений програмою-симулятором і відповідно оцінений. В табл. 1 наведена порівняльна характеристика варіантів отримання даних під час проведення експерименту.

Використання програм-симуляторів передбачає індивідуальне виконання лабораторних робіт студентами, а, відповідно, формування індивідуальних результатів експериментів. Для цього на основі реально проведеного експерименту генератору випадкових чисел програмно задається діапазон зміни вихідних даних – мінімальне і максимальне значення. Виходячи з концепції загального підходу обробки даних і статистичного аналізу у випадку експериментального дизайну [20], слід врахувати мінімальне і максимальне значення, які вже отримали.

Таблиця 1 – Порівняльна характеристика варіантів отримання даних під час проведення експерименту

Варіант отримання експериментальних даних	Наближеність до реальних умов проведення експерименту	Можливість підміни результатів експерименту	Об'єктивність результатів обробки експериментальних даних
За допомогою програми-симулятора	ні	ні	так
Візуально з екрану комп'ютера	так	так	ні – у випадку підміни експериментальних даних

Нехай в результаті експерименту є 5 значень: 6,5, 7,0, 7,5, 6,0, 6,2. Мінімальне значення 6,0. Вибираємо мінімальне значення як 6,0 або трохи менше, наприклад, 5,5, щоб врахувати можливу варіацію. Максимальне значення 7,5. Вибираємо максимальне значення як 7,5 або трохи більше, наприклад, 8,0, щоб врахувати можливу варіацію. Отже, якщо вибрати мінімальне значення 5,5 і максимальне значення 8,0, то можна використовувати генератор випадкових чисел для отримання нових випадкових значень у межах цього діапазону.

Ще один спосіб, який можна використати для визначення діапазону генератора випадкових чисел – це обчислення інтервалу довіри. Інтервал довіри або довірчий інтервал можна розглядати як інтервал значень випадкової величини, що є сумісними з даними дослідів і не суперечать їм. У межах довірчого інтервалу з заданою довірчою імовірністю можна отримати значення шуканої випадкової величини [21]. Для вищенаведених результатів експерименту у випадку нормального закону їх розподілу і кількості випробувань n менше 30 (випадок малої вибірки) знайдемо наступні показники [22]:

- середнє значення вибірки: $\bar{x} = \frac{\sum_{i=1}^n x_i}{n} = 6,6$
- стандартне відхилення вибірки: $S = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n-1}} = 0,6$
- стандартну помилку середнього: $SE = \frac{S}{\sqrt{n}} = 0,3$
- табличні значення t-розподілу для імовірностей 0,95, 0,98, 0,99, 0,999 і $n=5$: $t_{0,95}=2,8$, $t_{0,98}=3,7$, $t_{0,99}=4,6$, $t_{0,999}=8,6$
- похибку для імовірностей 0,95, 0,98, 0,99, 0,999 : $\delta_{0,95} = t_{0,95} \cdot SE = 0,8$,
 $\delta_{0,98} = t_{0,98} \cdot SE = 1,0$, $\delta_{0,99} = t_{0,99} \cdot SE = 1,2$, $\delta_{0,999} = t_{0,999} \cdot SE = 2,3$
- довірчий інтервал для імовірностей 0,95, 0,98, 0,99, 0,999:
 $\bar{x} \pm \delta_{0,95} = 6,6 \pm 0,8$, $\bar{x} \pm \delta_{0,98} = 6,6 \pm 1,0$, $\bar{x} \pm \delta_{0,99} = 6,6 \pm 1,2$,
 $\bar{x} \pm \delta_{0,999} = 6,6 \pm 2,3$.

І нарешті ми можемо визначити межі інтервалів довіри для різних імовірностей (табл. 2).

Таблиця 2 – Межі інтервалів довіри для різних значень імовірностей

Імовірність	Мінімальне значення	Мінімальне значення
0,95	5,9	7,4
0,98	5,6	7,6
0,99	5,4	7,8
0,999	4,3	8,9

Порівнюючи розкид даних експерименту (6,5, 7,0, 7,5, 6,0, 6,2) з граничними значеннями довірчих інтервалів для різних імовірностей, можна констатувати, що довірчі інтервали з імовірністю вище 0,95 повністю охоплюють експериментальні дані. Таким чином, мінімальне і максимальне значення для генератора випадкових чисел доцільно вибрати з довірчих інтервалів імовірності яких вища 0,95.

Висновки

1. В дослідженні зазначено важливість сучасної комп'ютерної симуляційної освіти для практичної підготовки медичних фахівців не тільки на старших, але й на молодших курсах.
2. Особливу актуальність програми-симулятори набувають під час вимушеної дистанційної освіти, спровокованою пандемією і широкомасштабною війною.
3. В статті наведений приклад роботи програми-симулятора з дисципліни «Медична і біологічна фізика». Проведено аналіз варіантів формування результатів експерименту програмою-симулятором проти вимірювання значень цих результатів безпосередньо на екрані комп'ютера. Встановлена суттєва перевага першого варіанту.
4. Запропоновано методику для визначення діапазону генератора випадкових чисел з метою формування індивідуальних результатів експерименту програмою-симулятором на основі обчислення довірчого інтервалу. Доведено, що мінімальне і максимальне значення для генератора випадкових чисел доцільно вибирати з довірчих інтервалів, імовірність яких вища 0,95.

Список літератури

- [1] Sellberg C., Lindmark O., Rystedt H. "Learning to navigate: the centrality of instructions and assessments for developing students' professional competencies in simulator-based training", *WMU J Marit Affairs*, no 17, pp. 249-265, 2018.
- [2] Ольга Ковальова "Впровадження симуляційних технологій навчання в медичну освіту", *Неперервна професійна освіта: теорія і практика (серія: педагогічні науки)*, випуск 1(58), с. 36-41, 2019. doi:10.28925/1609-8595.2019.1.3641.
- [3] So H.Y., Chen P.P., Wong G.K., Chan T.T. "Simulation in medical education", *JR Coll Physicians Edinb.*, no 49, pp. 52-57, 2019.
- [4] Elshama S.S. "How to apply Simulation-Based Learning in Medical Education?" *Iberoamerican Journal of Medicine*, no 2, pp. 79-86, 2020.
- [5] Іванькова Н. А. "Модель педагогічної системи електронного дистанційного навчання на базі хмарних сервісів", *Медична освіта*, N 3, с. 34-42, 2020. doi: 10.11603/me.2414-5998.2020.3.11439.
- [6] Кириленко В. І., Чалюк Ю. О. "Оцінка готовності країн до дистанційного навчання", *Приазовський економічний вісник*, випуск 1(30), с. 24-33, 2022. doi:10.32840/2522-4263/2022-1-4.
- [7] Interactive Simulations for Science and Math. [Online]. Available: <https://phet.colorado.edu/>. Accessed on: February 17, 2024.
- [8] Dive into a world of interactive learning. [Online]. Available: <https://www.labxchange.org/>. Accessed on: February 17, 2024.
- [9] Interactive STEM activities, free for your classroom. [Online]. Available: <https://learn.concord.org/>. Accessed on: February 17, 2024.
- [10] SmartSearch. [Online]. Available: <https://www.merlot.org/merlot/index.htm>. Accessed on: February 17, 2024.
- [11] Inspire Students with Immersive STEM Learning. [Online]. Available: <https://www.labster.com/>. Accessed on: February 17, 2024.
- [12] Lisbeth Elvira de Vries, Michael May "Virtual laboratory simulation in the education of laboratory technicians—motivation and study intensity", *Biochemistry and Molecular Biology Education*, Volume 47, Issue 3, pp. 213-362, 2019. doi:10.1002/bmb.21221.
- [13] А.У. Кулик, N.S. Nazarenko, P.P. Kovalchuk, V.I. Revenok, K.V. Dobrovolskaya Laboratory workshop on medical and biological physics, Vinnitsya: VNMU the name of M. I. Pyrogoва, 2019, 146 p.
- [14] Кулик А.Я., Ревенок В.І., Кулик Я.А., Нікольський О.І., Добровольська К.В. Комп'ютерна програма «Вивчення радіоактивного випромінювання за допомогою радіометра», свідоцтво про реєстрацію авторського права на твір 108095 Україна, 21.09.21.
- [15] Кулик А.Я., Ревенок В.І., Кулик Я.А., Нікольський О.І., Побережняк О.Р., Добровольська К.В. Комп'ютерна програма «Вивчення в'язкості рідини», свідоцтво про реєстрацію авторського права на твір 113407 Україна, 22.06.22.
- [16] Кулик А.Я., Ревенок В.І., Кулик Я.А., Нікольський О.І., Якимчук М.М., Добровольська К.В. Комп'ютерна програма «Вивчення закономірностей гемодинаміки на фізичній моделі», свідоцтво про реєстрацію авторського права на твір 114579 Україна, 01.09.22.
- [17] Кулик А.Я., Ревенок В.І., Кулик Я.А., Нікольський О.І., Подолянин В.І., Добровольська К.В. Комп'ютерна програма «Дослідження спектрів випромінювання з допомогою спектроскопа», свідоцтво про реєстрацію авторського права на твір 114580 Україна, 01.09.22.

- [18] Кулик А.Я., Ревенок В.І., Кулик Я.А., Нікольський О.І., Салецький О.В., Добровольська К.В. Комп'ютерна програма «Вивчення поверхневого натягу рідини», свідоцтво про реєстрацію авторського права на твір 114578 Україна, 01.09.22.
- [19] Кулик А.Я., Назаренко Н.С., Ревенок В.І., Добровольська К.В. Комп'ютерна програма «Collection tasks and questions on medical and biological physics», свідоцтво про реєстрацію авторського права на твір 117804 Україна, 04.04.23.
- [20] John A. Rice *Mathematical Statistics and Data Analysis*, Third Edition, Duxbury, an imprint of Thomson Brooks/Cole, a part of The Thomson Corporation, 2007, 685 p.
- [21] Сеньо П. С. *Теорія ймовірностей та математична статистика* : підручник, Київ : Знання, 2007, 556 с.
- [22] Robert S. Witte, John S. Witte *Statistics*, 11th Edition, Wiley, 2017, 486 p.

Стаття надійшла: 20.03.2024

References

- [1] Sellberg C., Lindmark O., Rystedt H. "Learning to navigate: the centrality of instructions and assessments for developing students' professional competencies in simulator-based training", *WMU J Marit Affairs*. no 17, pp. 249-265, 2018.
- [2] Olha Kovalova "Vprovadzhennia symuliatyinykh tekhnolohii navchannia v medychnu osvitu", *Neperervna profesiina osvita: teoriia i praktyka (seriia: pedahohichni nauky)*, vypusk 1(58), s.36-41, 2019. doi:10.28925/1609-8595.2019.1.3641 [in Ukrainian].
- [3] So H.Y., Chen P.P., Wong G.K., Chan T.T. "Simulation in medical education", *JR Coll Physicians Edinb.*, no 49, pp. 52-57, 2019.
- [4] Elshama S.S. "How to apply Simulation-Based Learning in Medical Education?" *Iberoamerican Journal of Medicine*, no 2, pp. 79-86, 2020.
- [5] Ivankova N. A. "Model pedahohichnoi systemy elektronnoho dystantsiinoho navchannia na bazi khmarnykh servisiv", *Medychna osvita*, N 3, s. 34-42, 2020. doi: 10.11603/me.2414-5998.2020.3.11439 [in Ukrainian].
- [6] Kyrylenko V. I., Chaliuk Yu. O. "Otsinka hotovnosti krain do dystantsiinoho navchannia", *Pryazovskyi ekonomichniy visnyk*, vypusk 1(30), s. 24-33, 2022. doi:10.32840/2522-4263/2022-1-4 [in Ukrainian].
- [7] Interactive Simulations for Science and Math. [Online]. Available: <https://phet.colorado.edu/>. Accessed on: February 17, 2024.
- [8] Dive into a world of interactive learning. [Online]. Available: <https://www.labxchange.org/>. Accessed on: February 17, 2024.
- [9] Interactive STEM activities, free for your classroom. [Online]. Available: <https://learn.concord.org/>. Accessed on: February 17, 2024.
- [10] SmartSearch. [Online]. Available: <https://www.merlot.org/merlot/index.htm>. Accessed on: February 17, 2024.
- [11] Inspire Students with Immersive STEM Learning. [Online]. Available: <https://www.labster.com/>. Accessed on: February 17, 2024.
- [12] Lisbeth Elvira de Vries, Michael May "Virtual laboratory simulation in the education of laboratory technicians—motivation and study intensity", *Biochemistry and Molecular Biology Education*, Volume 47, Issue 3, pp. 213-362, 2019. doi:10.1002/bmb.21221.
- [13] A.Y. Kulik, N.S. Nazarenko, P.P. Kovalchuk, V.I. Revenok, K.V. Dobrovolskaya *Laboratory workshop on medical and biological physics*, Vinnytsya: VNMU the name of M. I. Pyrogorova, 2019, 146 p.
- [14] Kulyk A.Y., Revenok V.I., Kulyk Y.A., Nikolskyi O.I., Dobrovolska K.V. *Kompiuterna prohrama «Vyvchennia radioaktyvnoho vyprominiuvannia za dopomohoiu radiometra»*, cvidotstvo pro reiestratsiiu avtorskoho prava na tvir 108095 Ukraina, 21.09.21[in Ukrainian].
- [15] Kulyk A.Y., Revenok V.I., Kulyk Y.A., Nikolskyi O.I., Poberezhniak O.R., Dobrovolska K.V. *Kompiuterna prohrama «Vyvchennia viazkosti ridyny»*, svidotstvo pro reiestratsiiu avtorskoho prava na tvir 113407 Ukraina, 22.06.22 [in Ukrainian].
- [16] Kulyk A.Y., Revenok V.I., Kulyk Y.A., Nikolskyi O.I., Yakymchuk M.M., Dobrovolska K.V. *Kompiuterna prohrama «Vyvchennia zakonomirnostei hemodynamiky na fizychnii modeli»*, cvidotstvo pro reiestratsiiu avtorskoho prava na tvir 114579 Ukraina, 01.09.22 [in Ukrainian].
- [17] Kulyk A.Y., Revenok V.I., Kulyk Y.A., Nikolskyi O.I., Podolianyn V.I., Dobrovolska K.V. *Kompiuterna prohrama «Doslidzhennia spektriv vyprominiuvannia z dopomohoiu spektroskopu»*, cvidotstvo pro reiestratsiiu avtorskoho prava na tvir 114580 Ukraina, 01.09.22 [in Ukrainian].
- [18] Kulyk A.Y., Revenok V.I., Kulyk Y.A., Nikolskyi O.I., Saletskyi O.V., Dobrovolska K.V. *Kompiuterna prohrama «Vyvchennia poverkhnevoho natiahu ridyny»*, cvidotstvo pro reiestratsiiu avtorskoho prava na tvir 114578 Ukraina, 01.09.22 [in Ukrainian].

- [19] Kulyk A.Y., Nazarenko N.S., Revenok V.I., Dobrovolska K.V. Kompiuterna prohrama «Collection tasks and questions on medical and biological physics», cvidotstvo pro reiestratsiiu avtorskoho prava na tvir 117804 Ukraina, 04.04.23 [in Ukrainian].
- [20] John A. Rice Mathematical Statistics and Data Analysis, Third Edition, Duxbury, an imprint of Thomson Brooks/Cole, a part of The Thomson Corporation, 2007, 685 p.
- [21] Seno P. S. Teoriia ymovirnostei ta matematychna statystyka : pidruchnyk, Kyiv : Znan-nia, 2007, 556 c [in Ukrainian].
- [22] Robert S. Witte, John S. Witte Statistics, 11th Edition, Wiley, 2017, 486 p.

Відомості про авторів

Кулик Анатолій Ярославович – доктор технічних наук, професор, завідувач кафедри біологічної фізики, медичної апаратури та інформатики ВНМУ ім. М.І. Пирогова

Ревенок Віктор Іванович – кандидат технічних наук, доцент, доцент кафедри біологічної фізики, медичної апаратури та інформатики ВНМУ ім. М.І. Пирогова

Кулик Ярослав Анатолійович – кандидат технічних наук, доцент, доцент кафедри автоматизації та інтелектуальних інформаційних технологій ВНТУ

Нікольський Олександр Іванович – кандидат технічних наук, доцент, доцент кафедри біологічної фізики, медичної апаратури та інформатики ВНМУ ім. М.І. Пирогова

Kulyk Anatoly – Doctor of Technical Sciences, Professor, Professor of the Department of Automation and Intelligent Information Technology, Vinnytsia National Technical University, head of the Department of Biophysics, Informatics and medical equipment, National Pirogov Memorial Medical University, Vinnytsya

Revenok Viktor – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Biophysics, Informatics and medical equipment, National Pirogov Memorial Medical University, Vinnytsya

Kulyk Yaroslav – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of of Automation and Intelligent Information Technologies, Vinnytsia National Technical University

Nikolskyy Oleksandr – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Biophysics, Informatics and medical equipment, National Pirogov Memorial Medical University

A.Y. Kulyk¹, V.I. Revenok¹, Y.A. Kulyk², O.I. Nikolskyy¹

DEVELOPMENT, IMPLEMENTATION AND USE OF SIMULATOR PROGRAMS FOR LABORATORY WORK IN MEDICAL AND BIOLOGICAL PHYSICS

¹National Pirogov Memorial Medical University, Vinnytsya

²Vinnytsia National Technical University, Vinnytsya