Ministry of Education and Science of Ukraine
Taras Shevchenko National University of Kyiv
Faculty of Information Technology
Department of Information Systems and Technologies

SCI IST
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY SCIENTIFIC CONFERENCE

The 3rd international scientific and practical conference

«INFORMATION SYSTEMS AND TECHNOLOGY: RESULTS AND PROSPECTS»
(IST 2026)

March 10, 2026

КИЇВський ВІТІ університет 2026

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка
Факультет інформаційних технологій
Кафедра інформаційних систем та технологій

SCIIST
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGY SCIENTIFIC CONFERENCE

3-я Міжнародна науково-практична конференція

«ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ: РЕЗУЛЬТАТИ І ПЕРСПЕКТИВИ»
(IST 2026)

10 березня 2026 року

КИЇВСЬКИЙ ВІТЧ УНІВЕРСИТЕТ 2026

Proceedings of the 3rd international scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2026), March 10, 2026 (Kyiv, Ukraine). Kyiv: PPC "Kyiv University", 2026. 474 p.

ISBN 978-966-933-398-8

Proceedings of the conference include reports on such topics:

- Smart IoT technologies;
- Digital technology of project management;
- Network and internet technology;
- Security of information systems and networks;
- Systems and technologies of artificial intelligence;
- Cognitive modeling and knowledge engineering.

The collection will be useful to scientists, researchers, students and everyone who is interested in modern information systems and technology.

Submitted in the authors' edition.

The authors are fully responsible for the accuracy of the information in the article as for the compliance of the materials with the laws, morals and ethics.

© Faculty of Information Technologies, 2026
© Taras Shevchenko National University of Kyiv, PPC "Kyiv University", 2026

Матеріали 3-ї Міжнародної науково-практичної конференції «Інформаційні системи та технології: результати і перспективи» (IST 2026), 10 березня 2026 р. (Київ, Україна). К. : ВПЦ "Київський університет", 2026. 474 с.

ISBN 978-966-933-398-8

У матеріалах конференції наведено доповіді за напрямами:

- Розумні технології IoT;
- Цифрові технології управління проєктами;
- Мережеві та інтернет-технології;
- Безпека інформаційних систем та мереж;
- Системи та технології штучного інтелекту;
- Когнітивне моделювання та інженерія знань.

Видання буде корисне науковцям, дослідникам, здобувачам і всім, хто цікавиться сучасними інформаційними системами та технологіями.

Подано в авторській редакції

Автори матеріалів несуть повну відповідальність за достовірність інформації, що в них висвітлюється, а також за відповідність матеріалів нормам законодавства, моралі та етики.

© Факультет інформаційних технологій, 2026
© Київський національний університет імені Тараса Шевченка, ВПЦ "Київський університет, 2026

Scientific Committee

Head: Volodymyr ILCHENKO, Dr, Prof.
(Taras Shevchenko National University of Kyiv, Ukraine)
Deputy Head: Volodymyr DRUZHYNIN, DSc, Prof. (Taras Shevchenko National University of Kyiv, Ukraine)
Andreas PESTER, Prof., Dr.
(Carinthia University of Applied Sciences, Austria / The British University in Egypt, Egypt)
Vitaliy SNYTYUK , DSc, Prof.
(Taras Shevchenko National University of Kyiv, Ukraine)
Frédéric MALLET, Prof. des Universités, Dr.
(Côte d'Azur University, France)
Andrii BILOSHCHYTSKYI, DSc, Prof.
(Astana IT University, Kazakhstan)
Artūras MICKUS, Assoc. prof., Dr.
(Vytautas Magnus University, Lithuania)
Andriy ONYSHCHENKO, DEc, Prof.
(Taras Shevchenko National University of Kyiv, Ukraine)
Serhii TOLIUPA, DSc, Prof.
(Taras Shevchenko National University of Kyiv, Ukraine)
Volodymyr NAKONECHNYI, DSc, Prof.
(Taras Shevchenko National University of Kyiv, Ukraine)
Renata DANIELIENĖ, Assoc. prof. Dr.
(Vilnius University, Lithuania)
Nataliia FEDOROVA, DSc, Doc.
(National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine)
Serhii HRYBKOV, DSc, Prof.
(National University of Food Technologies, Ukraine)
Igor PARKHOMEY, DSc, Prof.
(Taras Shevchenko National University of Kyiv, Ukraine)
Kateryna NESTERENKO, DSc, Prof.
(State University of Information and Communication Technologies, Ukraine)
Kamila STORCHAK, DSc, Prof.
(State University of Information and Communication Technologies, Ukraine)
Kateryna KOLESNIKOVA, DSc, Prof.
(International IT University, Kazakhstan)
Karsten HENKE, Dr.-Ing. Prof. h. c.
(Ilmenau University of Technology, Germany)
Oded MAIMON, Prof., Dr.
(Tel Aviv University, Israel)
Miloš ULMAN, Assoc. prof., PhD
(Czech University of Life Sciences, Czechia)
Ievgen NASTENKO, DSc, Prof.
(National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine)
Sergiy GNATYUK, DSc, Prof.
(State University "Kyiv Aviation Institute", Ukraine)
Juliy BOIKO, DSc, Prof.
(Khmelnytskyi National University, Ukraine)
Roman ODARCHENKO, DSc, Prof.
(State University "Kyiv Aviation Institute", Ukraine)
Serhii ZYBIN, DSc, Prof.
(State University "Kyiv Aviation Institute", Ukraine)
Oleksandr SAMKOV, DSc, Prof.
(Institute of Electrodynamics, NAS of Ukraine, Ukraine)
Mykhailo STEPANOV, DSc, SrSci
(National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine)

Organizing Committee

Head: Myroslava GLADKA, PhD, Doc.
(Taras Shevchenko National University of Kyiv, Ukraine)
Deputy Head: Olha BONDARENKO
(Taras Shevchenko National University of Kyiv, Ukraine)
Mykola KOSTIKOV, PhD, Doc.
(Taras Shevchenko National University of Kyiv, Ukraine)
Iryna BORYSENKO, PhD
(Taras Shevchenko National University of Kyiv, Ukraine)

Програмний комітет

Голова: Володимир ІЛЬЧЕНКО, д.ф-м.н., проф. (Київський національний університет імені Тараса Шевченка, Україна)
Заступник голови: Володимир ДРУЖИНІН, д.т.н., проф. (Київський національний університет імені Тараса Шевченка, Україна)
Андреас ПЕСТЕР, д.т.н., проф.
(Каринтійський університет прикладних наук, Австрія / Британський університет Єгипту, Єгипет)
Віталій СНИТЮК, д.т.н., проф.
(Київський національний університет імені Тараса Шевченка, Україна)
Фредерік МАЛЄ, д.т.н., проф.
(Університет Кот де Азур, Франція)
Андрій БІЛОЩИЦЬКИЙ, д.т.н., проф.
(Астана IT університет, Казахстан)
Артурас МІЦКУС, д.т.н., проф.
(Університет Вітовта Великого, Литва)
Андрій ОНИЩЕНКО, д.е.н., проф.
(Київський національний університет імені Тараса Шевченка, Україна)
Сергій ТОЛЮПА, д.т.н., проф.
(Київський національний університет імені Тараса Шевченка, Україна)
Володимир НАКОНЕЧНИЙ, д.т.н., проф.
(Київський національний університет імені Тараса Шевченка, Україна)
Рената ДАНІЄЛІЄНЕ, д.т.н., проф.
(Вільнюський університет, Литва)
Наталья ФЕДОРОВА, д.т.н., доц.
(Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна)
Сергій ГРИБКОВ, д.т.н., проф.
(Національний університет харчових технологій)
Ігор ПАРХОМЕЙ, д.т.н., проф.
(Київський національний університет імені Тараса Шевченка, Україна)
Катерина НЕСТЕРЕНКО, д.т.н., проф.
(Державний університет інформаційно-комунікаційних технологій, Україна)
Каміла СТОРЧАК, д.т.н., проф.
(Державний університет інформаційно-комунікаційних технологій, Україна)
Катерина КОЛЕСНІКОВА, д.т.н., проф.
(Інтернаціональний IT університет, Казахстан)
Карстен ХЕНКЕ, д.т.н., проф.
(Технічний університет Ільменау, Німеччина)
Одед МАЙМОН, д.т.н., проф.
(Тель-Авівський університет, Ізраїль)
Мілош УЛЬМАН, д.т.н., проф.
(Чеський університет природничих наук, Чехія)
Євген НАСТЕНКО, д.б.н., проф.
(Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна)
Сергій ГНАТЮК, д.т.н., проф.
(Державний університет «Київський авіаційний інститут», Україна)
Юлій БОЙКО, д.т.н., проф.
(Хмельницький національний університет, Україна)
Роман ОДАРЧЕНКО, д.т.н., проф.
(Державний університет «Київський авіаційний інститут», Україна)
Сергій ЗИБІН, д.т.н., проф.
Державний університет «Київський авіаційний інститут», Україна)
Олександр САМКОВ, д.т.н., проф.
(Інститут електродинаміки НАН України, Україна)
Михайло СТЕПАНОВ, д.т.н., с.н.с.
(Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна)

Організаційний комітет

Голова: Мирослава ГЛАДКА, к.т.н., доц
(Київський національний університет імені Тараса Шевченка, Україна)
Заступник голови: Ольга БОНДАРЕНКО
(Київський національний університет імені Тараса Шевченка, Україна)
Микола КОСТІКОВ, к.т.н., доц.
(Київський національний університет імені Тараса Шевченка, Україна)
Ірина БОРИСЕНКО, к.т.н.
(Київський національний університет імені Тараса Шевченка, Україна)

Зміст

Section Smart IoT technologies 14

Секція Розумні технології IoT 14

1. **VECTOR SEARCH MODEL FOR ENERGY SAVING OFCOMMUNAL BUILDINGS Oleksandr Dervenko** 15
2. **IOT SOLUTION FOR MONITORING AND CONTROL OF RADIOACTIVE CARGO TRANSPORTATION Yaroslav Melashchenko, Iryna Borysenko** 17
3. **ІНТЕЛЕКТУАЛЬНА IOT-СИСТЕМА МОНІТОРИНГУ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИВАТНОГО БУДИНКУ Іван Базаров, Мирослава Гладка** 20
4. **IOT СИСТЕМА ЗАБЕЗПЕЧЕННЯ ПЕРЕВЕЗЕНЬ МОРСЬКИМ ТРАНСПОРТОМ Дмитро Безносюк, Ольга Кравченко** 24
5. **ДИСТАНЦІЙНИЙ МОНІТОРИНГ ПАРАМЕТРІВ МІКРОКЛІМАТУ ОФІСНИХ ПРИМІЩЕНЬ НА ОСНОВІ МОДУЛЬНИХ IOT-СЕНСОРІВ Олександр Березюк, Володимир Дружинін** 29
6. **ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СУЧАСНИХ СИСТЕМ РАДІОМОНІТОРИНГУ В АВТОМАТИЗОВАНИХ КІБЕРФІЗИЧНИХ СИСТЕМАХ Ольга Бондаренко** 32
7. **МЕТОДИ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА ТЕРМІЧНОЇ СТАБІЛЬНОСТІ МОБІЛЬНИХ ГРАФІЧНИХ СИСТЕМ ШЛЯХОМ ВОЛЬТ-ЧАСТОТНОЇ ОПТИМІЗАЦІЇ Роман Вагін** 35
8. **МЕТОД ВЕРИФІКАЦІЇ ТА КОНТЕКСТНОЇ ФІЛЬТРАЦІЇ ГЕТЕРОГЕННИХ ДАНИХ ЕКОЛОГІЧНОГО МОНІТОРИНГУ ДЛЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ Кирило Вадурін, Олексій Лелека, Максим Рубан** 38
9. **МОДЕЛЬ СИСТЕМИ ЖИТТЄЗАБЕЗПЕЧЕННЯ ОСОБИ З КАРДІОЛОГІЧНИМИ РОЗЛАДАМИ Єгор Винник, Володимир Дружинін** 43
10. **МЕТОД ДИСТАНЦІЙНОГО АНАЛІЗУ РЕЗУЛЬТАТІВ ГРИ В НАСТІЛЬНИЙ ТЕНІС Юлія Вознюк, Максим Трембовецький** 46
11. **ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНФІГУРУВАННЯ МОДУЛЬНИХ РОБОТІВ НА ОСНОВІ ГІБРИДНОГО АЛГОРИТМІЧНОГО ПІДХОДУ Денис Гаватюк, Катерина Сисак** 49
12. **МОДЕЛІ ДЕТЕКЦІЇ АНОМАЛІЙ В IOT-СИСТЕМАХ Євген Гаврасієнко, Володимир Дружинін** 52
13. **ІНТЕГРАЦІЯ IOT-ПРИСТРОЇВ В ІНФОРМАЦІЙНІ СИСТЕМИ УПРАВЛІННЯ СКЛАДОМ ДЛЯ МОНІТОРИНГУ В РЕАЛЬНОМУ ЧАСІ Антон Галай, Ірина Борисенко** 55
14. **ПІДХОДИ ДО АНАЛІЗУ МОНІТОРИНГОВИХ ДАНИХ ПОПУЛЯЦІЙ ШКІДНИКІВ В УМОВАХ ОБМЕЖЕНОГО СПОСТЕРЕЖЕННЯ Владислав Гнатієнко, Віталій Снитюк** 58
15. **ІНТЕЛЕКТУАЛЬНИЙ МЕРЕЖЕВИЙ БЕЗДРОТОВИЙ СЕНСОРНИЙ ПРИСТРІЙ ВИЯВЛЕННЯ РУХУ ОБ'ЄКТІВ Геннадій Дахно, Юрій Кравченко** 62
16. **IOT-СИСТЕМА МОНІТОРИНГУ ЕМОЦІЙНОГО СТАНУ ТА КОМФОРТУ ВІДВІДУВАЧІВ У ВЕЛИКИХ ГРОМАДСЬКИХ ПРОСТОРАХ Денис Д'яченко, Мирослава Гладка** 66
17. **УДОСКОНАЛЕННЯ СИСТЕМ РЕГУЛЯЦІЇ ДЛЯ УПРАВЛІННЯ IOT ПРИСТРОЯМИ НА БАЗІ МІКРОКОНТРОЛЕРІВ Олександр Жеребцов, Анатолій Переверзєв** 69

18. **ІОТ-СИСТЕМА ВИЯВЛЕННЯ ШАХРАЙСТВА У БАНКІВСЬКИХ ПЛАТЕЖАХ Артем Колесник, Віталій Михальчук, Ірина Борисенко** 72

19. **ПЛАНУВАННЯ РИЗИКІВ ПРОЄКТУВАННЯ ІТ СИСТЕМ МОНІТОРИНГУ ЕНЕРГОСПОЖИВАННЯ ОФІСНИХ ПРИМІЩЕНЬ ВЕЛИКОЇ ПЛОЩІ Тимур Комісар, Ігор Пархомей** 76

20. **ІОТ СИСТЕМА УПРАВЛІННЯ ПОЛІКЛІНІКОЮ Артем Копич** 78

21. **ІНТЕГРАЦІЯ ІОТ-РІШЕНЬ У ЦИФРОВІ СИСТЕМИ ВІДЕОВИРОБНИЦТВА Максим Котов, Віталій Михальчук** 80

22. **ІОТ СИСТЕМА МОНІТОРИНГУ І УПРАВЛІННЯ ОЧИСНИХ СПОРУД ВОДОКАНАЛУ Ілля Кохановський, Ірина Борисенко** 83

23. **МОНІТОРИНГ ТА АНАЛІЗ ТРЕНУВАЛЬНОГО НАВАНТАЖЕННЯ СПОРТСМЕНІВ У ІОТ-СИСТЕМАХ Андрій Кураш, Мирослава Гладка** 87

24. **ІОТ-ШАР ДЛЯ SCADA/PLC БІОГАЗОВОГО КОМПЛЕКСУ Максим Кривченко, Володимир Дружинін** 91

25. **ТЕХНОЛОГІЯ КЕРУВАННЯ РОЗУМНИМИ ПРИСТРОЯМИ РІДНОЮ МОВОЮ Богдан Куцуліма, Ольга Кравченко** 94

26. **ІОТ СИСТЕМА КОНТРОЛЮ ВИРОБНИЦТВА ВЕРШКОВОГО МАСЛА Вадим Лесь** 96

27. **АРХІТЕКТУРА БЕЗПЕЧНОЇ ІНТЕГРАЦІЇ ІОТ-ПРИСТРОЇВ У КРИТИЧНУ ІНФРАСТРУКТУРУ Олександр Лукашов, Павло Шабатін** 100

28. **ПРОГРАМНО-АПАРАТНА СИСТЕМА АКУСТИЧНОГО УПРАВЛІННЯ ОСВІТЛЕННЯМ У СЕРЕДОВИЩІ ІОТ Кирило Максименко, Володимир Дружинін** 103

29. **МЕТОДИ ТА ПІДХОДИ ДО ОБРОБКИ ПОДІЙ У РЕАЛЬНОМУ ЧАСІ В СИСТЕМАХ ІОТ-МОНІТОРИНГУ ДОСТУПУ Ярослав Мельник** 108

30. **ІОТ ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ТРЕНУВАНЬ З ПІЛАТЕСУ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ Софія Олефір** 110

31. **УЗАГАЛЬНЕНИЙ МЕТОД СИНТЕЗУ ТЕСТІВ КОМПОНЕНТІВ ІНТЕЛЕКТУАЛЬНОГО ШЛЮЗУ ВИСОКОЩІЛЬНОГО ІОТ Володимир Панченко** 113

32. **ПРОЄКТ ІОТ-ЕКОСИСТЕМИ МОНІТОРИНГУ МЕДИЧНИХ ПОКАЗНИКІВ НОВОБРАНЦІВ ПІД ЧАС ТРЕНУВАННЯ Олесій Рудий, Ірина Борисенко** 118

33. **EDGE COMPUTING ЯК ІНСТРУМЕНТ ОПТИМІЗАЦІЇ ТА СТІЙКОСТІ КРИТИЧНОЇ ІОТ-ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ Ярослава Семенова, Микола Пирог** 123

34. **ТЕСТУВАННЯ РЕСУРСОЕФЕКТИВНОГО МЕТОДУ ВИЯВЛЕННЯ ПОЛАМОК МЕХАНІЧНИХ ПРИСТРОЇВ ЗА АУДІОСИГНАЛАМИ Артем Сєрєбряков, Володимир Тарануха, Олександр Бушма** 126

35. **АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ СХОДЖЕННЯМ ТІСТА З ВИКОРИСТАННЯМ ІОТ-ПРИСТРОЇВ Віктор Скрипніков, Андрій Онищенко** 130

36. **МЕТОДИ МОНІТОРИНГУ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПАРАМЕТРАМИ АЕРОПОНІЧНОЇ СИСТЕМИ НА ОСНОВІ ІОТ РІШЕНЬ Андрій Ставніченко** 133

37. **КОНТЕКСТНО-ІНТЕРПРЕТОВАНИЙ ПІДХІД ДО МОДЕЛЕЙ АНАЛІЗУ СИГНАЛІВ У РЕАЛЬНОМУ ЧАСІ У СИСТЕМАХ ІОТ Ольга Ткаченко, Аліна Шевченко** 136

38. **ІНТЕЛЕКТУАЛЬНА П'ЄЗОЕЛЕКТРИЧНА СИСТЕМА АВТОНОМНОГО ЖИВЛЕННЯ СВІТЛОФОРНИХ ОБ'ЄКТІВ Павло Томусяк, Юлій Бойко, Леся Карпова** 140

39. **ІОТ-СИСТЕМА ЗАБЕЗПЕЧЕННЯ КОМФОРТНИХ УМОВ ПРОЖИВАННЯ ЛЮДЕЙ З ДОДАТКОВИМИ ПОТРЕБАМИ Софія Ушакова, Ольга Кравченко** 144

40. **RULE-BASED DIGITAL TWIN ДЛЯ ЗАБЕЗПЕЧЕННЯ НОРМАТИВНОЇ ВІДПОВІДНОСТІ У ВИБУХОНЕБЕЗПЕЧНИХ РОБОТАХ Даніїл Філатов** 148

41. **МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МОНІТОРИНГУ СТАНУ ПАЦІЄНТІВ В ІОТ СИСТЕМАХ Юрій Ярошенко, Володимир Дружинін** 151

Section Digital Technology of Project Management 154

Секція Цифрові технології управління проєктами 154

42. **A MOBILE APPLICATION FOR LEARNING FOREIGN LANGUAGES AS A SOLUTION FOR MICROLEARNING: APPLICATION CONCEPT AND GAMIFICATION TOOLS Viktoriia Bytska, Vadym Ziuziun** 155

43. **DIGITAL TRANSFORMATION MODELS OF PROJECT MANAGEMENT SYSTEMS IN DEVELOPMENT COMPANIES Volodymyr Kochuma** 159

44. **HYBRID BLOCKCHAIN ARCHITECTURE FOR TRUSTED DOCUMENT AUTHENTICATION: A THEORETICAL FRAMEWORK FOR ENTERPRISE IT SOLUTIONS Assylbek Muratbek, Yenlik Begimbayeva** 165

45. **PSYCHOLOGICAL DETERMINANTS OF ADDICTIVE BEHAVIOR IN YOUTH UNDER CONDITIONS OF DIGITALIZATION Vladlen Lisnevsky** 168

46. **DEVELOPMENT OF PROJECT RISK SIMULATOR USING THE MONTE CARLO METHOD Viktor Putrenko, Yuriy Oliyarnyk, Nataliia Pashynska** 172

47. **MODEL OF TECHNOLOGICAL MATURITY OF ARTIFICIAL INTELLIGENCE USE IN BANKING INFORMATION SYSTEMS Kristina Shostal, Vadym Ziuziun** 176

48. **BRIDGING THE CULTURAL GAP: THE ROLE OF COMMUNICATION TECHNOLOGIES AND STUDENT BOUNDARY SPANNERS IN UNIVERSITY-INDUSTRY COLLABORATION Andrii Utvenko, Vadym Ziuziun** 181

49. **ЦИФРОВІ ІНСТРУМЕНТИ ПІДТРИМКИ УПРАВЛІННЯ ПРОЄКТАМИ В СУЧАСНИХ ОРГАНІЗАЦІЯХ Ольга Бондаренко** 184

50. **РОЗРОБКА ПРОЄКТУ СТВОРЕННЯ CRM-СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ ДІЯЛЬНОСТІ МЕРЕЖІ КВІТКОВИХ МАГАЗИНІВ Лілія Гаркушко, Любов Кубявка** 187

51. **ІНТЕГРАЦІЯ FIGMA У ПРОЦЕС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: ЕТАП ПРОТОТИПУВАННЯ Маргарита Гладка, Ольга Бондаренко** 191

52. **КІБЕРБЕЗПЕКА ТА НАДІЙНІСТЬ ЯК ВБУДОВАНІ ПРОЦЕСИ ГІБРИДНОГО УПРАВЛІННЯ ІОТ-ПРОЄКТАМИ В ЕНЕРГОСИСТЕМАХ Дмитро Загородній, Ігор Пархомей** 196

53. **АНАЛІТИКА ПОВЕДІНКИ КОРИСТУВАЧІВ У СИСТЕМАХ ВИПАДКОВИХ ВИНАГОРОД: МЕТОДИ ПРОГНОЗУВАННЯ УТРИМАННЯ ТА ВІДТОКУ КОРИСТУВАЧІВ Любов Кубявка, Станіслав Ганчев** 200

54. **АВТОМАТИЗОВАНА СЕРІАЛІЗАЦІЯ (Е-АКЦИЗ) З ВИКОРИСТАННЯМ ІОТ-РІШЕНЬ Дмитро Неделько, Володимир Дружинін** 203

55. **ВИКОРИСТАННЯ МУЛЬТИМОДАЛЬНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ПРОТОТИПУВАННЯ ІНТЕРФЕЙСІВ КОРИСТУВАЧА Юрій Поліщук, Сергій Грибков** 206

56. **МАСШТАБОВАНІ AGILE-ФРЕЙМВОРКИ ЯК ІНСТРУМЕНТ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ В УМОВАХ ВІЙНИ В УКРАЇНІ Олена Фендьо, Микола Пирог** 210

Section Network and Internet Technology 214

Секція Мережеві та інтернет-технології 214

57. **TIME-WEIGHTED PAGERANK FOR MEASURING STRUCTURAL EMBEDDEDNESS IN LARGE-SCALE BIBLIOGRAPHIC COUPLING NETWORKS Zhanel Rymkhanova** 215

58. **INTEGRATED METHOD OF LOW-DETECTION REDUNDANCY MONITORING IN WIRELESS SENSOR NETWORKS Mykhaylo Sharapov, Yurii Kravchenko, Andrii Sobchuk** 220

59. **ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ ІОТ-ПРИСТРОЇВ Олексій Бичков, Володимир Петрівський, Денис Штома** 224

60. **КОНВЕРГЕНЦІЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ: CPU, GPU, NPU, CXL Андрій Бондарчук, Віталій Залива, Микола Лисенко** 228

61. **МОДЕЛЮВАННЯ ТА ЕКВАЛІЗАЦІЯ ШВИДКІСНИХ PAM4 СИГНАЛІВ Назар Гаврись, Євгеній Коновал** 232

62. **ІНТЕЛЕКТУАЛІЗАЦІЯ КЕРУВАННЯ ВІРТУАЛЬНИМИ МЕРЕЖЕВИМИ ФУНКЦІЯМИ В АРХІТЕКТУРАХ SDN/KDN ДЛЯ ВИСОКОНАВАНТАЖЕНИХ СЕРВІСІВ Дмитро Кульчицький** 236

63. **ВИКОРИСТАННЯ ЦИФРОВИХ ПЛАТФОРМ ДЛЯ АНАЛІЗУ ЗОВНІШНЬОПОЛІТИЧНИХ КОМУНІКАЦІЙ: КЕЙС ПУБЛІКАЦІЙ МЗС КНР У СОЦМЕРЕЖІ X ЩОДО КИТАЙСЬКО-ЯПОНСЬКИХ ВІДНОСИН (ГРУДЕНЬ 2025 Р.) Анна Кушнір, Галина Кучаковська** 239

64. **МЕТОДИ ТА АЛГОРИТМИ КООРДИНАЦІЇ РОЗПОДІЛЕНИХ МУЛЬТИАГЕНТНИХ СИСТЕМ У СЕРЕДОВИЩАХ З ОБМЕЖЕНОЮ НАВІГАЦІЄЮ Сергій Шевченко** .. 242

Section Security of information systems and networks 244

Секція Безпека інформаційних систем та мереж 244

65. **RISK-BASED MODEL FOR CRYPTOGRAPHIC MFA SELECTION Daulet Zhumat** .. 245

66. **АДАПТИВНІ МЕХАНІЗМИ ПРЕВЕНТИВНОГО ВИЯВЛЕННЯ АНОМАЛІЙ У РОБОТІ ЯДРА LINUX НА ОСНОВІ ТЕХНОЛОГІЇ EBPF Міхал Аг, Мирослава Гладка** 249

67. **ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА РАДІОТЕХНІЧНОГО МОНІТОРИНГУ Віталій Андрійчук, Юлій Бойко, Леся Карпова** 252

68. **СТІЙКІ ПІДХОДИ ДО ПОБУДОВИ ZERO TRUST АРХІТЕКТУР У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ Микита Гришко, Інна Розломій** 257

69. **СУЧАСНІ ЗАГРОЗИ БЕЗПЕЦІ ІОТ У СКЛАДІ КІБЕРФІЗИЧНИХ ТА КРИТИЧНИХ СИСТЕМ Дарина Джирма, Інна Розломій** 260

70. **МЕТОДИ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ Анна Квятковська** 263

71. **КОРЕЛЯЦІЯ МЕРЕЖЕВИХ ІНДИКАТОРІВ ЯК ОСНОВА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ OSINT-АНАЛІЗУ ФІШИНГОВИХ РЕСУРСІВ Валерія Кизима, Володимир Наконечний** 266

72. **РОЗШИРЕННЯ БАЗОВИХ МЕРЕЖНИХ ПОЛІТИК KUBERNETES ЗА ДОПОМОГОЮ SERVICE MESH ДЛЯ СЕГМЕНТАЦІЇ НА РІВНІ L7 Владислав Литвиненко, Сергій Бучик** 268

73. **КРИПТОГРАФІЧНІ ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЙНОГО ОБМІНУ В МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ 6G Захар Малига** 270

74. **БЕЗПЕКА ТА КОНТРОЛЬ ІНФОРМАЦІЙНИХ ПОТОКІВ У ВОЛОКОННО-ОПТИЧНИХ МЕРЕЖАХ Олександр Манько, Людмила Харлай, Ганна Мостович** 272

75. **БЕЗПЕКА ДАНИХ У МУЛЬТИХМАРНИХ ТА МІЖПЛАТФОРМНИХ МЕРЕЖЕВИХ АРХІТЕКТУРАХ Сергій Натура**..... 275

76. **ЗАХИСТ ПЕРСОНАЛЬНИХ І ЧУТЛИВИХ ДАНИХ У СИСТЕМАХ ІЗ ВБУДОВАНИМИ МЕХАНІЗМАМИ ШТУЧНОГО ІНТЕЛЕКТУ Максим Норенко, Інна Розломій** 277

77. **РИЗИК-ОРІЄНТОВАНА МОДЕЛЬ ІНТЕГРАЦІЇ ДАНИХ КІБЕРЗАГРОЗ ТА ОПТИМАЛЬНОГО АВТОМАТИЗОВАНОГО РЕАГУВАННЯ В МУЛЬТИХМАРНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ Світлана Рзаєва, Дмитро Рзаєв, Юлія Костюк** . 279

78. **ДОСЛІДЖЕННЯ ІНСТРУКЦІЇ БЕЗУМОВНОГО ПЕРЕХОДУ Олександр Рисований** 284

79. **МОДЕЛІ ДОСТУПУ ABAC/CAPBAC/HYBAC ДЛЯ IOT-КОНТРОЛЮ ДО СПЕЦОБ'ЄКТІВ Артем Рімек, Ольга Кравченко** 286

80. **МЕТРИКА ПОКРИТТЯ БЕЗПЕКИ ДЛЯ ХМАРНОЇ ІНФРАСТРУКТУРИ В ПАРАДИГМІ «ІНФРАСТРУКТУРА ЯК ПРОТЕСТОВАНИЙ КОД» Михайло Савонік** 289

81. **ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ СИСТЕМ СИНХРОНІЗАЦІЇ З ВИКОРИСТАННЯМ CESIUM CLOCK Олександр Самков, Валерій Коваль, В'ячеслав Вакась, Олег Піскун**..... 293

82. **ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ У ХМАРНИХ ТА ГІБРИДНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ Дар'я Ткаченко, Інна Розломій** 296

83. **ІНТЕГРАЦІЯ АДАПТИВНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ДАНИХ В МЕРЕЖУ МІКРОКОНТРОЛЛЕРІВ ТА МІКРОКОМП'ЮТЕРІВ Олександр Швидченко, Ігор Пархомей** 298

84. **МІНІМІЗАЦІЯ КІБЕРРИЗИКІВ ПРИ ВПРОВАДЖЕННІ НАЦІОНАЛЬНОЇ ЦИФРОВОЇ ВАЛЮТИ (НА ПРИКЛАДІ Е-ГРИВНІ) Ігор Шиленко, Володимир Наконечний**.... 301

85. **КОМПЛЕКСНА КРИПТОГРАФІЧНА АРХІТЕКТУРА ПІДВИЩЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ Людмила Шпорт, Юлія Сотніченко** 305

86. **ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ СИСТЕМ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ ТРИФАКТОРНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ Діана Язвінська, Анатолій Ніколенко** 309

Section Systems and technologies of artificial intelligence 313

Секція Системи та технології штучного інтелекту 313

87. **MODIFIED RADON PROJECTIONS FOR OVERLAP DETECION IN AGRICULTURAL LAND MAPPING Stepan Bilan, Dmytro Berezhnyi** 314

88. **INTELLIGENT MULTIMODAL DATA FUSION FOR ROBUST UAV DETECTION IN COMPLEX ENVIRONMENTS Stanislav Golouh, Vladyslav Shulga, Ihor Pishta** 318

89. **DIGITAL TWIN–BASED PERSONALIZATION SYSTEM FOR INTELLIGENT REHABILITATION Yaroslav Hladkyi, Volodymyr Druzhynin** 321

90. **USING DISTRIBUTED COMPUTING TO IMPROVE THE EFFICIENCY OF LARGE LANGUAGE MODELS: MODELS AND METHODS FOR ORGANIZING EFFECTIVE SCHEDULING IN PROBLEM-ORIENTED ENVIRONMENTS Oleksii Paharskyi** 324

91. **PRIVACY-PRESERVING MACHINE LEARNING IN THE AGE OF BIG DATA Bekzhan Seitov** 326

92. **PHYSICS-INFORMED GRAPH NEURAL NETWORKS FOR AGRO-RESOURCE MONITORING AND RECOVERY PREDICTION Kristina Silvanovych, Olena Hrynova** 330

93. **THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DIGITAL DESIGN PROCESSES: AI AS A TOOL, NOT A REPLACEMENT Anastasiia Slobodina, Mykola Kostikov** 335

94. **ВИЯВЛЕННЯ PROMPT-ІН'ЄКЦІЙ У ВЕЛИКИХ МОВНИХ МОДЕЛЯХ МЕТОДАМИ СЕМАНТИЧНОГО АНАЛІЗУ Володимир Ахрамович, Володимир Санченко** 337

95. **ВПЛИВ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ІТ-КОНСАЛТИНГУ В УКРАЇНІ ТА В СВІТІ Єлизавета Бабенко, Валентина Бабенко, Костянтин Бабенко** 341

96. **ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ УПРАВЛІННЯ ЗАПАСАМИ БУДІВЕЛЬНИХ МАТЕРІАЛІВ У БАГАТОПРОЄКТНОМУ СЕРЕДОВИЩІ НА ОСНОВІ MILP-МОДЕЛІ Владислав Балабась, Олена Федусенко** 343

97. **СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ БАГАТОАГЕНТНИХ АРХІТЕКТУР У ДИНАМІЧНИХ СОЦІОТЕХНІЧНИХ СЕРЕДОВИЩАХ Едуард Бовда, Юрій Самохвалов** 347

98. **МЕХАНІЗМИ УВАГИ В ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖАХ ДЛЯ ПРОГНОЗУВАННЯ КОРОТКОСТРОКОВОЇ ВОЛАТИЛЬНОСТІ ФІНАНСОВИХ РИНКІВ Олексій Вовченко, Микола Костіков** 352

99. **МЕТОДИ ОБ'ЄДНАННЯ РЕГІОНІВ ІНТЕРЕСУ ДЛЯ ЕФЕКТИВНОЇ ОБРОБКИ НЕЙРОННИМИ МЕРЕЖАМИ ДОВІЛЬНОГО ФОРМАТУ Ярослав Гозак, Сергій Палій** 354

100. **ДОСЛІДЖЕННЯ МЕТАЕВРИСТИЧНИХ АЛГОРИТМІВ ДЛЯ ОПТИМІЗАЦІЇ МАРШРУТІВ В ДИНАМІЧНОМУ СЕРЕДОВИЩІ ДЛЯ ПОТРЕБ ДОСТАВКИ МАЛИХ ПІДПРИЄМСТВ Єгор Гузь, Олена Федусенко** 357

101. **ЗАСТОСУВАННЯ АЛГОРИТМІВ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ІДЕНТИФІКАЦІЇ РАДІОІЗОТОПІВ НА ОСНОВІ СИНТЕТИЧНИХ ДАНИХ Юрій Забулонов, Тетяна Носенко** 361

102. **МУЛЬТИАГЕНТНИЙ ПІДХІД ДО ФОРМУВАННЯ РОЗКЛАДУ ЗАНЯТЬ З ДЕЦЕНТРАЛІЗОВАНИМ УЗГОДЖЕННЯМ РІШЕНЬ Ганна Красовська, Ольга Ізмайлова, Олег Іларіонов** 364

103. **МОДЕЛЬ DT-DEC-POMDP ДЕЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ РОЄМ БПЛА З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ ТА СТОХАСТИЧНИМИ ПОРУШЕННЯМИ ЗВ'ЯЗКУ Єгор Мєзєнцев, Юрій Кравченко** 367

104. **ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ У ВЕБЗАСТОСУНКАХ ПОШУКУ РОБОТИ В ІТ Павло Мосієнко** 371

105. **МЕТОД ПРОГНОЗУВАННЯ ТРАНСПОРТНОГО ТРАФІКУ В МІСТІ НА ОСНОВІ ВІДКРИТИХ ДАНИХ ТА ГІБРИДНИХ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ Григорій Пономаренко, Мирослава Гладка** 375

106. **АРХІТЕКТУРНА МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОЇ АДАПТИВНОЇ ОСВІТНЬОЇ ПЛАТФОРМИ З БАГАТОРІВНЕВОЮ ПЕРСОНАЛІЗАЦІЄЮ Богдан Скочинський** 378

107. **ЗАСТОСУВАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ РОЗКЛАДУ КОНСУЛЬТАЦІЙ ВИКЛАДАЧА Олена Федусенко, Анатолій Федусенко** 382

108. **МЕТОД УНІФІКОВАНОЇ ІНТЕГРАЦІЇ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ У КРОСПЛАТФОРМНІ ПРОГРАМНІ СИСТЕМИ НА ОСНОВІ ONNX ТА**

КОНТЕЙНЕРИЗОВАНОГО INFERENCE Даниіл Фуркало, Володимир Петрівський 385

109. **ДОСЛІДЖЕННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ ПОПИТУ НА МОЛОЧНУ ПРОДУКЦІЮ Катерина Чорнобай, Сергій Грибков**..... 388

110. **ЖАНРОВА КЛАСИФІКАЦІЯ МУЗИЧНИХ КОМПОЗИЦІЙ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ Антон Шаповалов, Ганна Красовська**..... 391

111. **ПРОГРАМНА СИСТЕМА ФОРМУВАННЯ НАВЧАЛЬНИХ НАБОРІВ ДАНИХ ДЛЯ СТРУКТУРНОЇ СЕГМЕНТАЦІЇ МУЗИЧНИХ СИГНАЛІВ Дар'я Шкуратовська, Анастасія Ніколаєнко**..... 393

112. **СТОХАСТИЧНЕ МОДЕЛЮВАННЯ ФІНАНСОВИХ ЧАСОВИХ РЯДІВ: ВІД ГЕОМЕТРИЧНОГО БРОУНІВСЬКОГО РУХУ ДО НЕЙРОННОЇ ДИФУЗІЙНО-СТРИБКОВОЇ МОДЕЛІ Юрій Юрченко, Олександр Заковортний**..... 397

Section Cognitive modeling and knowledge engineering..... 402

Секція Когнітивне моделювання та інженерія знань 402

113. **ABOUT ONE RECOMMENDATION MODEL FOR DATA PREDICTION BASED ON FUZZY LOGIC Eugene Ivokhin, Glib Shelyakin**..... 403

114. **CONSIDERING PSYCHOLOGICAL CHARACTERISTICS OF STUDENTS FOR ADAPTIVE E-LEARNING Mykola Kostikov, Vladlen Lisnevskyi** 405

115. **IDENTIFYING RESEARCHERS' SCIENTIFIC AREAS BASED ON PUBLICATION CLUSTERING Alisher Shaimuran** 408

116. **ОСОБЛИВОСТІ ТА ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНИХ ДАНИХ ПРИ ПЛАНУВАННІ ГУМАНІТАРНОГО РОЗМІНУВАННЯ В УКРАЇНІ Дмитро Аеров**..... 414

117. **КОГНІТИВНА МОДЕЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАСТОСУВАННІ СУДОВОЇ ЕКСПЕРТИЗИ ТА ПИТАНЬ ВИКЛИКІВ ЩОДО КІБЕРБЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ Єлизавета Бабенко**..... 417

118. **КОНЦЕПТУАЛЬНА СХЕМА ПРИЙНЯТТЯ РІШЕНЬ В СИТУАЦІЇ ПЕРЕСЛІДУВАННЯ ЦІЛІ ГРУПОЮ ГРАВЦІВ З ОДНАКОВИМИ ТАКТИКО-ТЕХНІЧНИМИ ХАРАКТЕРИСТИКАМИ Леся Барановська, Григорій Гнатієнко**..... 420

119. **КОГНІТИВНЕ МОДЕЛЮВАННЯ N-РІВНЕВИХ МІРКУВАНЬ LLM-АГЕНТІВ: АРХІТЕКТУРА ДИНАМІЧНОЇ ВЕРИФІКАЦІЇ ТА САМОКОРИГУВАННЯ Єгор Башкевич, Любов Кубявка**..... 424

120. **КЛАСИФІКАЦІЯ КОГНІТИВНИХ ВИКРИВЛЕНЬ У ПРОЦЕСІ ПРОЄКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ Владислав Безуглий, Ольга Кравченко** 427

121. **МЕТОДОЛОГІЯ ВИЯВЛЕННЯ ВРАЗЛИВИХ ГРУП НАСЕЛЕННЯ ДЛЯ РИЗИКОРІЄНТОВАНОГО МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ Кирило Вадурін, Артем Васильєв, Іван Перекрест** 430

122. **ПРО ОДНУ УЗАГАЛЬНЕНУ МОДЕЛЬ ЗАДАЧІ КОМІВОЯЖЕРА ЗА НАЯВНІСТЮ ОБМЕЖЕНЬ ВИПЕРЕДЖЕННЯ Валерій Гавриленко, Катерина Івохіна**..... 434

123. **ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ І ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ ТЕХНІЧНОГО ДІАГНОСТУВАННЯ І МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ Сергій Глухов, Олександр Бабій, Сергій Семеха** 436

124. **ПРОГРАМНИЙ МОДУЛЬ ВИЯВЛЕННЯ ОЗНАК МАНІПУЛЮВАННЯ В НАУКОМЕТРИЧНІЙ БАЗІ SCOPUS Григорій Гнатієнко, Артур Домбровський**.. 439

125. **СТРУКТУРА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ Олексій Гнатієнко, Владислав Сингаївський** 443

126. **КРИТЕРІЇ ОЦІНКИ ВІЗУАЛЬНОГО ІНТЕРФЕЙСУ СИСТЕМИ ВІДДАЛЕНОГО КЕРУВАННЯ ДИНАМІЧНИМИ ОБ'ЄКТАМИ Олексій Губський, Ігор Попов, Олександр Бушма** 447

127. **ФОРМАЛІЗАЦІЯ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАДАЧІ ЕКСПЕРТИЗИ НА ОСНОВІ КОНЦЕПТІВ OPENALEX Ірина Доманецька, Ярослав Хроленко** 451

128. **СИСТЕМА МОНІТОРИНГУ ЕМОЦІЙНОГО СТАНУ ТА САМОСВІДОМОСТІ ДИТИНИ ЗА ДОПОМОГОЮ ПСИХОЛОГІЧНИХ ІНСТРУМЕНТІВ Катерина Жукова, Мирослава Гладка** 454

129. **ПРО ОДНУ ГІБРИДНУ АВТОМАТНО-АГЕНТНУ МОДЕЛЬ ПРОЦЕСІВ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ Євген Івохін, Лариса Аджубей, Дмитро Афонін** 457

130. **ПРО ОДИН ПРИКЛАД ОПТИМІЗАЦІЇ МАРШРУТІВ ДОСТАВКИ ВАНТАЖІВ НА ОСНОВІ МЕТОДУ ІМІТАЦІЇ ВІДПАЛУ Євген Івохін, Дмитро Івохін** 459

131. **ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА EDTECH-ПЛАТФОРМ ТА UI-АНАЛІЗАТОРІВ Карина Конвісар, Анна Пилипенко** 461

132. **ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ПІДТРИМКИ ІНВЕСТИЦІЙНИХ РІШЕНЬ У ЗАДАЧАХ ФОРМУВАННЯ ПОРТФЕЛЯ ВАЛЮТНИХ АКТИВІВ Ярослав Кошулько, Ганна Красовська** 465

133. **ТИПОЛОГІЯ ПОМИЛОК МАШИННОГО ПЕРЕКЛАДУ В ІГРОВИХ ТЕКСТАХ ТА СТРАТЕГІЇ ЇХ ПОСТРЕДАГУВАННЯ (PEMT) Ольга Солодка** 468

134. **МОДЕЛІ ТА МЕТОДИ АПРОКСИМАЦІЇ ДАНИХ З ВИКОРИСТАННЯМ ТРИГОНОМЕТРИЧНИХ СПЛАЙНІВ У ЗАДАЧАХ КОМП'ЮТЕРНОГО ЗОРУ Ганна Терещук, Микола Пирог** 471

Section

Smart IoT technologies

Секція

Розумні технології IoT

VECTOR SEARCH MODEL FOR ENERGY SAVING OFCOMMUNAL BUILDINGS

Oleksandr Derevenko

Annotation. *Current research discusses about energy saving and possible solutions that could improve it for communal facilities. The research suggests usage of web-applications, vector search and available data to improve energy saving of the buildings. The model was created based on available tools. The model solutions can be applied to other facilities as long as solutions for these devices are matching.*

Keywords: vector search, internet technologies, web-application, communal buildings, energy saving.

I. INTRODUCTION

Nowadays many communal enterprises critically depend on constant energy supply for uninterrupted work. Many` ongoing conflicts, changes in resource trade relationships and stability to maintain those trades to supply needed energy production for ever increasing demand. Currently many critical infrastructures are equipped with automatic switches to change the energy production from main grid to installed power generators. Such procedure is needed to prevent work interruption of facilities in case of energy supply loss or grid system malfunction. Due to many limitations of available technologies communal buildings may end up using high energy consumption devices. While communal building is ensured to be powered by all means but it becomes a liability on consuming limited resources and strain to energy grid. It is suggested to have system to find better way in finding solutions to ensure energy saving. The solution was proposed to utilize the web-applications and vector search. Many cloud services provide web-applications that can be used for various goals. For example, research determined that digital platforms, web apps, or internet-supported intervention can directly provide family caregivers on-demand support and care solutions in real time [1]. Some web-application services can provide access to different tools to analyse relevant data. Apex Oracle is one those services that provides vector path search which will be utilized in the model. Vector search can be used to transform data into vectors and perform search that will find closest requested solution. Vector search can be applied to other types of information besides text. One of researches states that any object, be it a document or query, that contains text, images, speech, or a mix of these modalities, is often represented as a vector [2].

II. DATA AND METHODS

To improve energy saving is to use vector search to find currently available solutions based on market data and data of energy consumption of devices in other buildings. Web-applications will be used to have access to vector search and accessibility for other facilities. Current developed model is displayed in Figure 1.

The main idea of this model is to use vector search to find direct answers for communal building. This can be performed by collecting data from available devices on market, energy consumption of devices and types of devices. The collected data can be stored as a reference for future solutions. Current model can be applied to other communal buildings. But all solutions have to apply to only types and models of devises that solution was generated for. Meaning if solution was generated for devices in one communal building it is only applicable for exact type of device and factors in other.

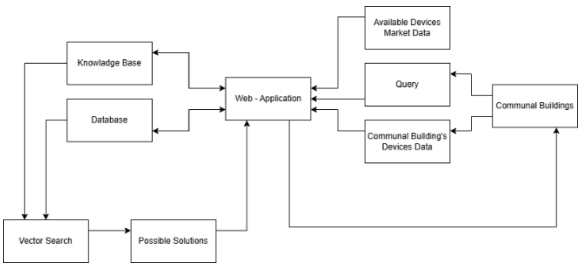


Figure 1. *Energy saving vector search model*

III. RESULTS AND ANALYSIS

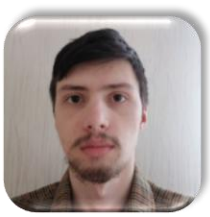
Current model advantages and disadvantages have been analyzed. One main advantage of such model is accessibility to web-application and easy use with right configurations. Using vector search can find direct solutions for energy savings in communal buildings by having access to available data. By using web-application, communal facilities can be connected to one application and database and receive solutions based on data collected from devices and their energy consumption. One of potential risk of using such model is possible data poisoning. Data breach is also a possibility. Even if web-application services can ensure that data is secure but security of data is also depended on data security of communal buildings and during transfer operations of data. Current model can apply solutions to existing in database devices and to improve it requires more data on different devices. The solutions for unknow devices can be suggested by cannot guarantee effectiveness of these solutions. Current model work has to be specified in further research to address those issues and transparency on its inner workings.

IV. DISCUSSION AND CONCLUSION

There is relevance of energy saving performance improvement for communal facilities. Despite current solutions to maintain the uninterrupted work of facilities there is more room to ensure energy saving. Usage of web-applications and vector search was proposed. The model for communal builds energy saving with vector search was proposed. The advantages and disadvantages were analyzed. Further work with proposed model is required. saving. Usage of web-applications and vector search was proposed. The model for communal builds energy saving with vector search was proposed. The advantages and disadvantages were analyzed. Further work with proposed model.

REFERENCES

1. Laura N. G., Eric J., Catherine P., Sokha K., Taylor S., Melinda J. W., Rachel N. B., David L. R. (2026) Plans4Care, a web application providing caregivers personalized solutions to manage dementia-related care challenges: Proof of concept and efficacy trial. Contemporary Clinical Trials Communications, Volume 49.
2. Sebastian B. (2025) Advances in Vector Search. Association for Computing Machinery, 995–997.



OLEKSANDR DEREVENKO
3rd year PhD Student, Department of Information Systems and Technologies, Kyiv
ORCID: 0009-0009-4645-4386
E-mail: alextitagle@gmail.com
Currently pursuing the Ph.D. degree in program technologies of the internet of things from Taras Shevchenko National University of Kyiv. His research interests include models of energy efficiency and energy supply systems, personnel training and assistance systems.

IOT SOLUTION FOR MONITORING AND CONTROL OF RADIOACTIVE CARGO TRANSPORTATION

Yaroslav Melashchenko, Iryna Borysenko

Abstract. *These theses consider an IoT-based solution for monitoring and controlling the transportation of radioactive cargo. The proposed solution is based on a network of embedded sensors that provide continuous monitoring of radiation levels, temperature, humidity, door opening status, and vehicle geolocation. The system ensures prompt detection of deviations from regulatory transportation parameters and automatically notifies responsible personnel in the event of emergencies, thereby increasing transportation safety and reducing risks to personnel and the environment.*

Keywords: IoT, sensors, monitoring, radiation safety, logistics.

I. INTRODUCTION

Under current conditions, the transportation of radioactive materials is an integral part of industrial and logistics processes. Such transportation is always associated with increased responsibility, as even minor violations of transportation conditions may cause radiation hazards for personnel, the population, and the environment. Ensuring continuous cargo condition monitoring, compliance with regulatory requirements, and the ability to respond promptly to emergency situations help prevent negative consequences.

The implementation of an IoT system involves the integration of sensor modules for measuring ionizing radiation levels, temperature, humidity, mechanical loads, and geolocation. The data are transmitted to a server where they are stored and subsequently processed, analyzed, and visualized. If permissible values are exceeded, the system automatically generates notifications for responsible personnel, enabling timely preventive measures.

Thus, the development and implementation of such a solution aim to enhance radiation safety, minimize human factor risks, ensure transparency of logistics processes, and create a unified digital environment for monitoring the transportation of hazardous materials.

II. DATA AND METHODS

The developed system is based on an architecture that includes a hardware component, a server for data storage and processing, and a web application for user interaction, which enables monitoring of all active transportation operations.

The hardware component is built around the ESP32 microcontroller, which collects data from the sensors.

The following sensors were selected:

- A Geiger–Müller counter-based ionizing radiation sensor – measures background radiation levels, allowing control of container integrity in accordance with permissible standards [1].
- BME280 – a temperature, humidity, and atmospheric pressure sensor for comprehensive monitoring of transportation conditions [2].
- NEO-6M – determines the coordinates of the vehicle transporting the cargo [3].
- MC-38 – a magnetic contact sensor that detects whether contacts are in a closed or open state [4].

All sensors are connected to the microcontroller, which transmits processed data to the server via Wi-Fi. Users of the web application can send requests to retrieve sensor data stored on the

server, allowing convenient access to all necessary information for monitoring the current transportation status, as shown in Figure 1.

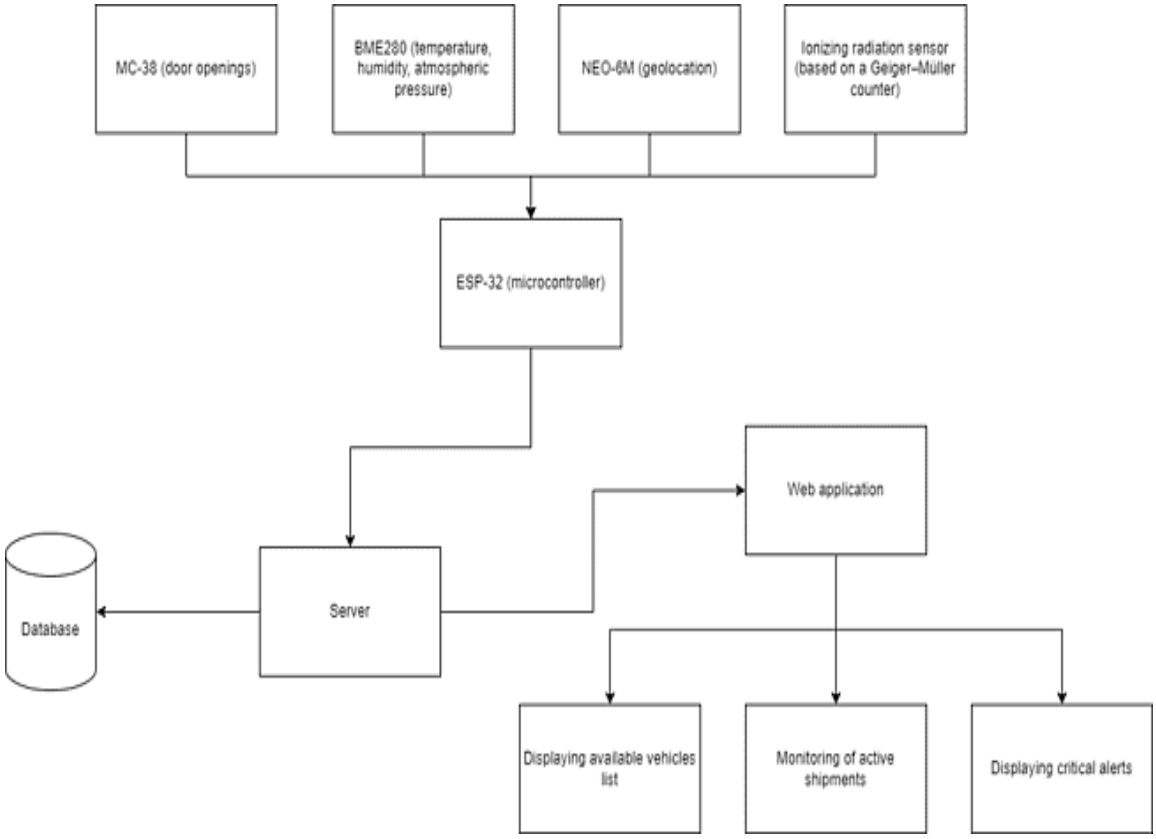


Figure 1. *Architecture of the IoT solution for monitoring and control of radioactive cargo transportation*

III. RESULTS AND ANALYSIS

The developed IoT solution enables continuous real-time monitoring of key transportation parameters. By integrating sensors for radiation background, temperature, humidity, geolocation, and container opening control, a comprehensive approach to transportation safety is achieved.

The implementation of this system provides the following advantages:

- Continuous radiation monitoring – timely detection of excessive ionizing radiation levels enables rapid response to potential container integrity violations.
- Monitoring of transportation conditions – control of temperature, humidity, and mechanical impacts reduces the risk of cargo or packaging damage.
- Container access control – detection of container opening makes it possible to identify unauthorized interference and record the event with a timestamp and coordinates.
- Real-time route tracking – GPS monitoring ensures adherence to the planned route and rapid response in case of deviations.

At the same time, certain limitations and implementation challenges exist:

- Dependence on communication stability – loss of network coverage may temporarily delay data transmission.
- Cybersecurity concerns – the need to protect data from unauthorized access or sensor data manipulation.

Thus, the analysis demonstrates that the application of IoT technologies significantly increases the level of control and transparency in the transportation of radioactive materials.

IV. DISCUSSION AND CONCLUSION

The study established that implementing such an IoT solution is a promising direction in the digitalization of the transport sector. The proposed solution provides comprehensive real-time monitoring of critically important parameters, significantly enhancing radiation and overall technological safety.

Integration of sensor modules with a server platform and web application creates a unified information control environment in which responsible personnel can promptly receive data, analyze situations, and make informed management decisions. Automation of the notification process minimizes risks associated with the human factor and reduces response time to emergency situations.

In the future, the system's functionality may be expanded through the implementation of risk prediction algorithms, the use of machine learning technologies for anomaly detection, and integration with governmental hazardous cargo monitoring systems. This will further improve the efficiency, safety, and reliability of radioactive material transportation.

REFERENCES

1. Geiger Counter Radiation Detector Kit ver.2 Datasheet. URL: http://f4fdw.free.fr/geiger/DIY%20Geiger%20Counter%20Radiation%20Detector%20Kit%20ver.2.pdf
2. BME280 Combined humidity and pressure sensor Datasheet. URL: https://www.bosch-sensortec.com/media/boschsensortec/downloads/datasheets/bst-bme280-ds002.pdf
3. NEO-6 u-blox 6 GPS Modules Datasheet. URL: https://content.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf
4. Door & Window Magnetic Sensor Switch Datasheet. URL: https://naylampmechatronics.com/img/cms/Datasheets/Datasheet%20MC-38.pdf



YAROSLAV MELASHCHENKO
4th-year bachelor's student in Internet of Things Software Technologies, Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine E-mail: melashchenkoya@fit.knu.ua
The scientific interest is focused on the development of an IoT solution for monitoring and controlling the transportation of radioactive materials.



IRYNA BORYSENKO
PhD in Technical Sciences, Associate Professor of the Department of Information Systems and Technologies, Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0009-0005-8350-6422
E-mail: borysenkoi@fit.knu.ua
The scientific interest is focused on the study of information systems, information security, and programming.

ІНТЕЛЕКТУАЛЬНА IOT-СИСТЕМА МОНІТОРИНГУ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИВАТНОГО БУДИНКУ

Іван Базаров, Мирослава Гладка

Анотація. *У тезах представлено підхід до побудови інтелектуальної IoT-системи безпеки приватного будинку, що поєднує моніторинг подій, централізоване журналювання та автоматичне реагування на інциденти. Запропоновано багаторівневу архітектуру з сенсорним рівнем, edge-обробкою та серверним модулем керування, а також механізми захисту обміну даними для зниження ризиків компрометації розумного будинку. Розглянуто сценарії виявлення проникнення, пожежної небезпеки та витоку газу, а також підходи до зменшення хибних спрацювань.*

Ключові слова: IoT, розумний будинок, безпека, моніторинг, MQTT, edge computing, IDS.

I. ВСТУП

Розумний будинок на базі IoT підвищує комфорт, однак одночасно збільшує площину атак та ризики для приватності: пристрої з датчиками, камерами та керуванням доступом стають цілями для несанкціонованого доступу, перехоплення трафіку й підміни команд. Сучасні огляди підкреслюють, що для smart home критичними є автентифікація, контроль доступу, захист протоколів обміну та виявлення аномалій у мережевій активності [1], [3].

Метою роботи є розробка моделі інтелектуальної IoT-системи, що забезпечує моніторинг станів будинку, фіксацію подій та автоматичну реакцію на загрози з урахуванням вимог кібербезпеки.

II. ДАНІ ТА МЕТОДИ

Запропонована система реалізується як багаторівнева архітектурна модель, що забезпечує розподіл функцій між компонентами відповідно до принципів масштабованості та відмовостійкості. На сенсорному рівні функціонують датчики руху та відкриття дверей/вікон, датчики диму і температури, витоку газу або чадного газу, а також сенсори протікання води. Окрім засобів збору даних, цей рівень включає виконавчі модулі, зокрема сирену, керовані реле освітлення та електромагнітні клапани, які забезпечують фізичне реагування на виявлені загрози.

Запропонована архітектура передбачає використання гетерогенного набору сенсорних пристроїв, що забезпечують моніторинг різних параметрів середовища. Кожен сенсор формує телеметричні дані, які відображають стан контрольованих об’єктів у режимі реального часу. Наприклад, датчики руху фіксують переміщення в контрольованих зонах, сенсори відкриття дверей і вікон сигналізують про несанкціонований доступ, а датчики диму та температури дозволяють оперативно виявляти ознаки пожежної небезпеки. Використання декількох типів сенсорів створює можливість комплексного спостереження за станом будинку та формує основу для кореляції подій у межах інтелектуальної системи безпеки.

Зібрані сенсорні дані передаються до локального контролера через бездротові або дротові канали зв’язку залежно від типу пристрою та умов розгортання системи. На цьому етапі виконується попередня агрегація та нормалізація даних, що дозволяє уніфікувати інформаційні потоки від різних сенсорів. Такий підхід забезпечує ефективну інтеграцію різнорідних пристроїв у єдину систему моніторингу та спрощує подальшу обробку інформації. Крім того, використання стандартизованих протоколів взаємодії між компонентами дозволяє забезпечити масштабованість системи та можливість підключення додаткових пристроїв без значної зміни її архітектури.

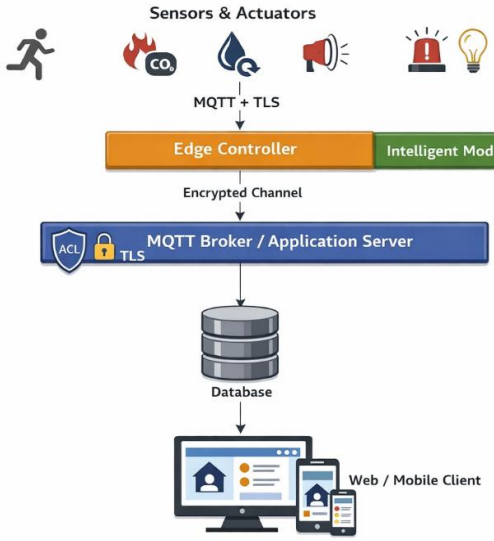


Рисунок 1. *Архітектура інтелектуальної IoT-системи безпеки приватного будинку*

Як показано на Рисунку 1, система побудована за принципом багаторівневої взаємодії компонентів із розподілом функцій між edge та серверним рівнями. Обробка даних первинного рівня здійснюється на edge-рівні за допомогою локального контролера. Тут реалізується фільтрація та дедуплікація подій, застосування базових правил реагування, а також буферизація даних у випадку втрати мережевого з'єднання. Такий підхід дозволяє забезпечити автономність функціонування системи та мінімізувати залежність від зовнішніх серверних ресурсів.

Подальша централізована обробка та зберігання інформації здійснюються на серверному рівні, який відповідає за управління подіями, реалізацію сценаріїв типу "умова–дія", контроль доступу користувачів та аудит дій. Серверний модуль забезпечує збереження історії інцидентів у базі даних і формування сповіщень у режимі реального часу. Клієнтський рівень представлений веб- або мобільним інтерфейсом, що надає користувачеві доступ до поточного стану системи, історії подій та засобів налаштування правил реагування.

Для передачі телеметрії та подій використовується протокол MQTT як легковаговий механізм публікації та підписки, оптимізований для IoT-середовищ із обмеженими ресурсами [4]. З метою підвищення рівня кіберзахисту застосовується транспортне шифрування TLS, механізми контролю доступу на рівні брокера (ACL), ізоляція тематичних каналів та принцип мінімально необхідних привілеїв для пристроїв. Усі критичні події та спроби несанкціонованого доступу фіксуються у журналі безпеки, що забезпечує можливість подальшого аналізу інцидентів.

Окрему увагу приділено забезпеченню відмовостійкості системи. У разі втрати зв'язку із сервером edge-контролер продовжує виконувати базові сценарії реагування автономно, а накопичені події передаються на сервер після відновлення з'єднання. Такий механізм дозволяє зберігати цілісність журналів подій та підтримувати безперервність функціонування системи навіть у нестабільних мережевих умовах.

Інтелектуальний компонент системи спрямований на зменшення кількості хибних спрацювань шляхом кореляції подій та аналізу контексту. Формування тривожного сигналу відбувається на основі поєднання декількох факторів, наприклад, фіксації руху разом із відкриттям дверей у нічному режимі. Перспективним напрямом розвитку є інтеграція алгоритмів детекції аномалій для аналізу поведінкових шаблонів пристроїв і мережевого трафіку [3,5].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті розробки запропоновано модель інтелектуальної IoT-системи безпеки приватного будинку, що поєднує сенсорний моніторинг, локальну обробку даних та централізоване управління подіями. Архітектурний підхід забезпечує розподіл навантаження між рівнями системи та дозволяє підвищити її стійкість до відмов і мережевих збоїв. Запропонована структура відповідає сучасним принципам побудови розподілених систем, де функціональні модулі ізольовані, але взаємодіють через захищені канали обміну даними.

Реалізація edge-рівня дає можливість виконувати первинну обробку подій без необхідності постійного підключення до серверної частини. Це дозволяє мінімізувати затримки реагування на критичні ситуації та забезпечити автономність функціонування системи у разі тимчасової втрати мережевого з'єднання. Локальні правила реагування зменшують навантаження на сервер та оптимізують обсяг переданих даних. Крім того, такий підхід сприяє зменшенню вимог до пропускної здатності мережі та дозволяє використовувати систему в умовах нестабільного або обмеженого інтернет-з'єднання.

Серверний рівень забезпечує централізоване зберігання подій, контроль доступу та аудит дій користувачів. Використання моделі "умова–дія" дозволяє формувати гнучкі сценарії реагування залежно від режиму роботи системи. Такий підхід сприяє підвищенню адаптивності рішення та зручності його налаштування. Централізована база подій створює можливість подальшого аналізу інцидентів, формування статистичних звітів та оцінювання ефективності роботи системи безпеки у довгостроковій перспективі.

Застосування протоколу MQTT у поєднанні із шифруванням TLS та механізмами контролю доступу підвищує рівень захисту обміну даними між компонентами системи. Реалізація принципу мінімально необхідних привілеїв та журналювання інцидентів створює додатковий рівень кіберстійкості. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу до інфраструктури розумного будинку та забезпечити відповідність сучасним вимогам інформаційної безпеки.

Запропонований інтелектуальний механізм кореляції подій дозволяє зменшити кількість хибних спрацювань та підвищити точність формування тривожних сигналів. Комплексний аналіз декількох параметрів і контексту функціонування системи забезпечує більш обґрунтоване прийняття рішень порівняно з використанням окремих датчиків без взаємної перевірки. Використання механізмів аналізу поведінкових шаблонів відкриває можливості для подальшої інтеграції алгоритмів машинного навчання [5] з метою адаптивного налаштування порогів спрацювання та виявлення аномалій.

З точки зору масштабованості система може бути розширена шляхом додавання нових сенсорів або інтеграції з іншими підсистемами розумного будинку, зокрема системами відеоспостереження, контролю доступу або енергоменеджменту. Модульна архітектура дозволяє здійснювати поетапне впровадження та модернізацію без необхідності повної реконфігурації всієї інфраструктури. Це підвищує практичну цінність запропонованого рішення та робить його придатним для впровадження як у приватних будинках, так і в малих комерційних об'єктах.

Таким чином, запропонована модель демонструє можливість створення масштабованої, автономної та кіберстійкої IoT-системи для забезпечення безпеки приватного будинку. Отримані результати підтверджують доцільність застосування багаторівневої архітектури з використанням edge-обробки, захищених протоколів обміну даними та механізмів інтелектуальної кореляції подій як основи сучасних систем безпеки розумних середовищ.

Перспективним напрямом подальшого розвитку є експериментальна оцінка ефективності запропонованої моделі в реальних умовах експлуатації. Доцільним є аналіз затримки реагування, рівня хибних спрацювань та стійкості до мережевих збоїв і кібератак. Отримані результати дозволять уточнити параметри налаштування системи та підвищити її адаптивність до різних сценаріїв використання.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі запропоновано модель інтелектуальної IoT-системи моніторингу та забезпечення безпеки приватного будинку, що базується на багаторівневій архітектурі з розподілом функцій між сенсорним, edge та серверним рівнями. Такий підхід дозволяє забезпечити автономність функціонування, зменшити затримки реагування на критичні події та підвищити відмовостійкість системи.

Практична значущість запропонованого рішення полягає у можливості інтеграції доступних апаратних компонентів із сучасними механізмами захищеного обміну даними та централізованого управління. Використання MQTT у поєднанні з TLS, контроль доступу та журналювання подій підвищують рівень кіберстійкості системи, що є критично важливим для IoT-середовищ[4]. Реалізація механізму кореляції подій сприяє зменшенню хибних спрацювань та підвищує ефективність реагування.

Перспективами подальших досліджень є впровадження алгоритмів детекції аномалій на основі методів машинного навчання, удосконалення механізмів захисту від мережевих атак та проведення експериментальної оцінки ефективності системи в умовах реальної експлуатації. Розвиток таких підходів сприятиме підвищенню рівня безпеки розумних домогосподарств та розширенню можливостей застосування IoT-технологій.

ДЖЕРЕЛА

1. Vardakis, G., Zafeiropoulos, A., Panaousis, E. Review of Smart Home Security Using Internet of Things Technologies. Electronics, 2024, 13(16), 3343.
2. Sabit, H., Al-Anni, M., Kadhim, M. Artificial Intelligence-Based Smart Security System Using IoT. Electronics, 2025, 14(3), 608.
3. Rahman, M. M., et al. Intrusion Detection Systems for IoT-Based Smart Home Networks: A Survey. Journal of Information Security and Applications, 2024, 78, 103652.
4. Bangare, P. S., et al. Enhancing MQTT Security for Internet of Things Applications Using Lightweight Cryptography. Internet of Things, 2024, 26, 101178.
5. Adamova, A., et al. Machine Learning Algorithms for Intrusion Detection in IoT Networks. Procedia Computer Science, 2024, 232, 210–219.



ІВАН БАЗАРОВ
Студент 4 курсу освітньої програми «Програмні технології інтернет речей» Факультету інформаційних технологій.
E-mail: bazarovivan@knu.ua
Наукові інтереси: проєктування та адміністрування інформаційних систем, IoT-архітектури, кібербезпека мережевих середовищ, розподілені обчислення та інфраструктурні рішення для забезпечення відмовостійкості систем.



МИРОСЛАВА ГЛАДКА
Кандидат технічних наук, доцент, доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка
ORCID: 0000-0001-5233-2021,
E-mail: gladkam@fit.knu.ua
Наукова діяльність пов’язана з розробкою моделей та методів управління ІТ-проєктами в умовах невизначеності, застосуванням мультиагентних систем, інтелектуальних інформаційних технологій та IoT-рішень. Дослідження спрямовані на поєднання методів управління проєктами, аналітики даних та архітектур розподілених систем.

IOT СИСТЕМА ЗАБЕЗПЕЧЕННЯ ПЕРЕВЕЗЕНЬ МОРСЬКИМ ТРАНСПОРТОМ

Дмитро Безносюк, Ольга Кравченко

Анотація. *У рамках даного дослідження було розроблено систему управління контейнерами для морської логістики з інтеграцією IoT-технологій, що дозволяє здійснювати моніторинг і управління перевезенням вантажів на всіх етапах його доставки. Застосування датчиків для моніторингу стану контейнерів, а також використання технологій обміну даними через IoT, сприяють зниженню витрат на логістику та оптимізації перевезень. Розробка включає архітектуру для управління контейнерами, інтеграцію з реальними серверами та базами даних, а також адміністрування на веб-платформі для користувачів і адміністраторів. Впровадження IoT системи сприяє значному покращенню ефективності та зручності процесу транспортування вантажів.*

Ключові слова: морська логістика, управління контейнерами, IoT, Laravel, Vue.js, Kafka.

I. ВСТУП

Морська логістика є однією з основних складових глобальної економіки, забезпечуючи транспортування вантажів між континентами та країнами. Однак, сучасні процеси управління контейнерами вимагають удосконалення для підвищення ефективності та зниження витрат. Використання технологій Інтернету Речей (IoT) дозволяє інтегрувати реальний моніторинг вантажів у процес логістики, що забезпечує автоматизацію та оперативне реагування на зміну умов. [1]

У даній роботі запропоновано рішення для управління контейнерами в морській логістиці, яке включає використання датчиків для моніторингу стану контейнерів, інтеграцію з веб-платформою для адміністрації та використання IoT для реального часу збору даних. Таке рішення дозволяє знизити витрати на управління та забезпечити більш точне планування маршруту та часу доставки, що є критичним для ефективної роботи логістичних компаній. [2]

Метою цієї роботи є розробка автоматизованої системи управління контейнерами, що інтегрує IoT-технології для підвищення ефективності, безпеки та зручності процесу перевезення вантажів.

II. ДАНІ ТА МЕТОДИ

Запропонована система управління контейнерами в морській логістиці використовує IoT-технології для моніторингу стану вантажів та оптимізації перевезень. Система базується на зборі даних через датчики, що вимірюють температуру, вологість, вібрацію та GPS-координати контейнерів. Дані з сенсорів передаються через протокол брокерів повідомлень, що забезпечує ефективний обмін даними між пристроями та сервером. [3]

Обробка даних здійснюється за допомогою Apache Kafka, що гарантує надійну обробку великих обсягів даних в реальному часі та забезпечує масштабованість системи. Для зберігання даних використовується база данних зі швидким заповненням та пошуком, що забезпечує надійність зберігання інформації про стан контейнерів і логістичні операції. В якості додаткового інструменту для кешування і підвищення швидкості доступу до часто використовуваних даних застосовуються Redis та Horizon. [4]

Веб-інтерфейс для адміністрування побудований на базі Laravel та Vue.js, що дозволяє користувачам ефективно моніторити стан контейнерів і здійснювати управлінські операції в реальному часі. Автоматизація процесів здійснюється через застосування алгоритмів

обробки даних, що дозволяють оперативно реагувати на зміни стану контейнерів і вносити необхідні коригування в умови перевезення без втручання людини.

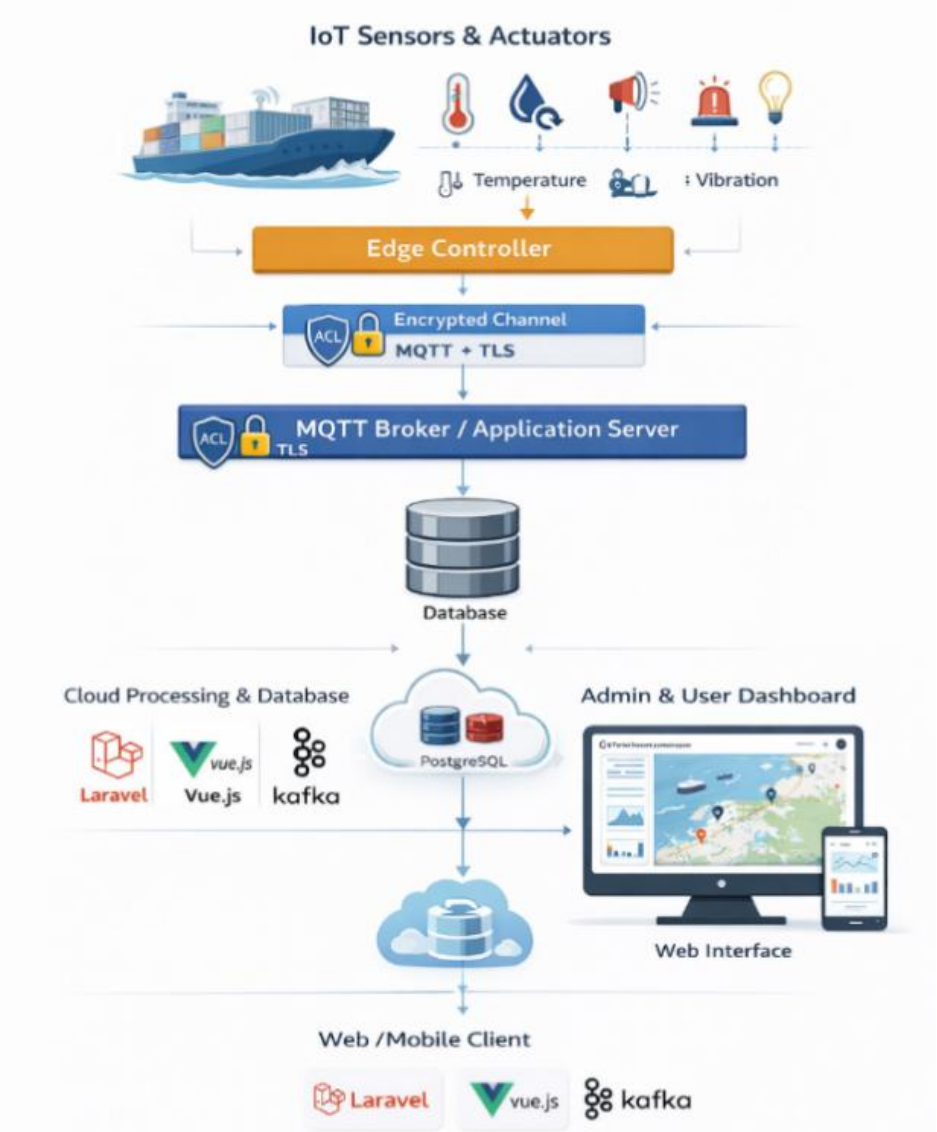


Рисунок 1. *Архітектура інтелектуальної IoT-системи забезпечення перевезень морським транспортом*

Для управління контейнерами в морській логістиці використовуються IoT-технології для моніторингу стану вантажів. Температурні, вологісні та вібраційні датчики, вбудовані в контейнери, передають дані через Wi-Fi модулі на судні, а потім через Starlink до хмарного сервера для обробки.

Дані обробляються через Apache Kafka, що забезпечує ефективну передачу великих обсягів інформації, а також зберігаються в PostgreSQL для основного зберігання та в Redis для кешування для швидкого доступу.

Управління контейнерами здійснюється через веб-інтерфейс, розроблений на Laravel та Vue.js, що дозволяє користувачам моніторити та управляти контейнерами в реальному часі. Всі зміни параметрів, такі як температура чи вологість, здійснюються через веб-панель, де запит передається на сервер і потім до Edge Controller на судні. Далі за допомогою брокера повідомлення команда відправляється на Arduino Uno плату, який контролює реле для активації відповідних механічних пристроїв, таких як зволожувачі чи обігрівачі.

Зворотний зв'язок від Arduino передається на сервер і оновлюється на веб-панелі. Це забезпечує автоматизоване управління контейнерами та точне виконання управлінських рішень у реальному часі.

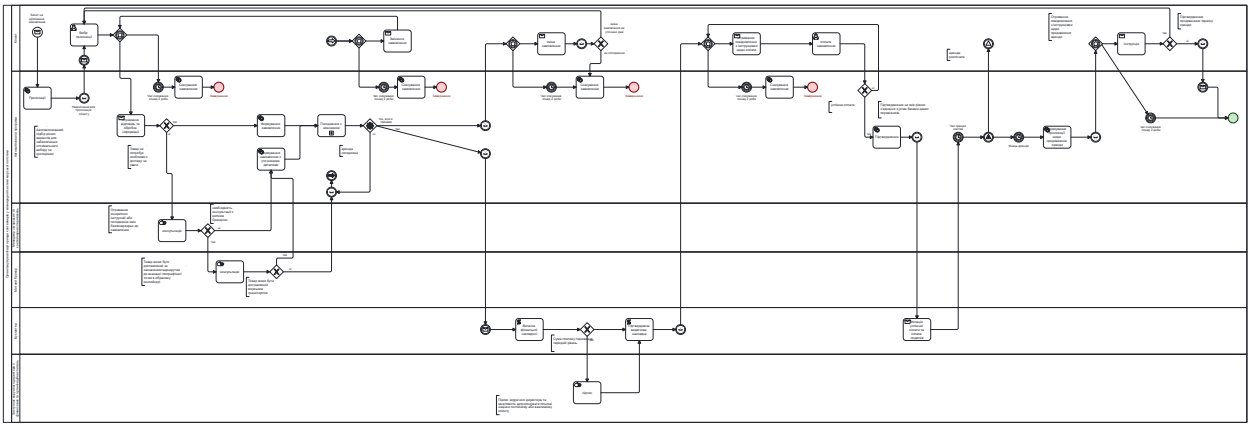


Рисунок 2. *BPMN модель процесу оренди контейнера морським транспортом*

BPMN модель на Рисунку 2 відображає процес оренди контейнера та узгодження перевезення вантажу між користувачем і менеджером. Процес починається з ініціації запиту на оренду, де користувач вибирає контейнер і подає заявку. Система перевіряє доступність контейнера та надає користувачу інформацію про умови оренди. Після цього менеджер отримує сповіщення про запит і узгоджує умови перевезення, такі як час доставки та тариф.

Після підтвердження менеджером, система формує кінцеву угоду, що завершується підтвердженням оренди користувачем. У разі відмови або необхідності зміни умов, система повертає користувача на етап уточнення деталей.

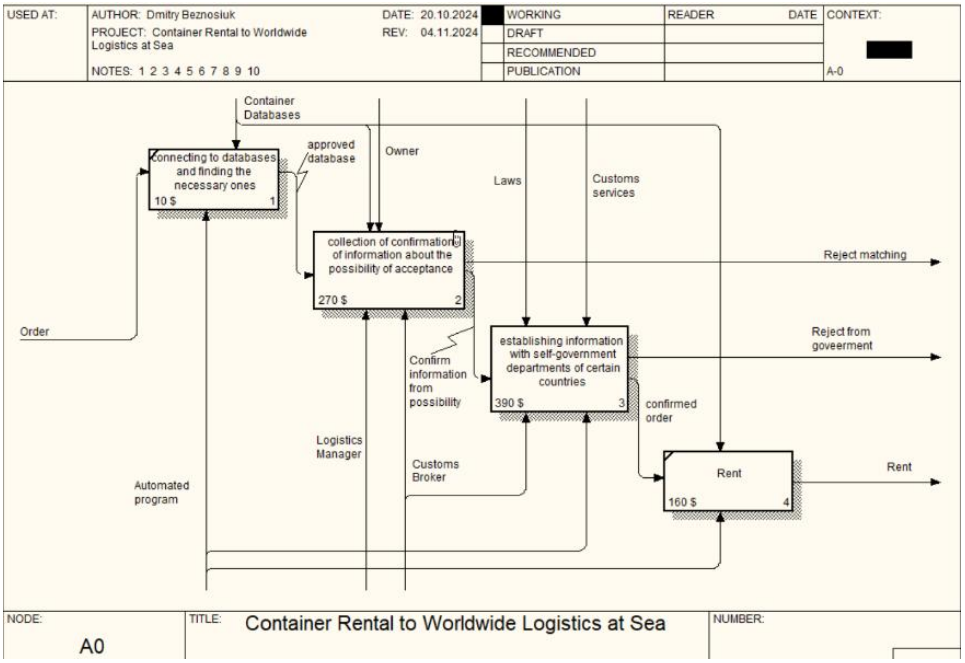


Рисунок 3. *IDEF0 - Деталізація процесу оренди контейнера*

Модель IDEF0 описує процес оренди контейнерів у морській логістиці, визначаючи ключові функції та їх взаємозв'язки. Процес починається з перевірки доступності контейнерів у базах даних, що дозволяє забезпечити відповідність замовленням і вимогам клієнта.

Далі проводиться підтвердження інформації від власників контейнерів та митних органів щодо їх відповідності технічним вимогам і дозволам на перевезення. Це мінімізує ризики митних затримок і забезпечує правильність вибору контейнера для транспортування.

Наступним етапом є узгодження умов оренди з органами самоврядування для дотримання регуляторних норм країн, через які проходитиме перевезення. Це необхідно для забезпечення відповідності міжнародним стандартам і нормам.

Завершенням процесу є підтвердження оренди та передача контейнера клієнту, що завершує формалізацію угоди і дозволяє розпочати перевезення вантажу.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Запропонована система управління контейнерами в морській логістиці з використанням IoT технологій має ряд ключових переваг, що значно підвищують ефективність і безпеку перевезень вантажів. Головною метою системи є автоматизація процесів моніторингу і управління станом контейнерів, що дозволяє значно знизити витрати на обслуговування і оперативно реагувати на зміни в умовах перевезення. [5]

Однією з основних переваг є візуалізація даних в реальному часі. Завдяки інтеграції з веб-інтерфейсами користувач отримує наочну інформацію про стан контейнерів, включаючи параметри, такі як температура, вологість, вібрація. Це дозволяє оперативно виявляти потенційні проблеми, наприклад, перевищення температурних норм або ризик пошкодження вантажу, і своєчасно вживати коригувальних заходів. Така наочність значно полегшує управлінські рішення, дозволяючи уникнути ручного моніторингу та помилок у прийнятті рішень.

Прогнозованість і звітність є ще однією важливою перевагою. Всі дані, що збираються сенсорами, можуть бути використані для формування звітів і прогнозів. Це дозволяє не лише аналізувати поточний стан контейнерів, але й передбачати можливі проблеми на основі історичних даних. Такий підхід дозволяє здійснювати більш точне планування перевезень, оцінювати можливі ризики та зменшити ймовірність виникнення непередбачених ситуацій. [6]

Система є масштабованою, що дає можливість адаптувати її до потреб різних компаній та операційних масштабів. Вона ефективно працює як для невеликих підприємств, так і для великих міжнародних логістичних компаній, забезпечуючи зручний доступ до актуальної інформації про кожен контейнер у реальному часі.

Завдяки автоматизації збору та обробки даних, система знижує людську залежність і помилки, пов'язані з ручними операціями. У результаті цього підвищується загальна ефективність перевезень і надійність процесу логістики, що особливо важливо для перевезення вантажів, що потребують точного контролю умов транспортування.

Запровадження цієї системи є технологічним проривом у галузі морської логістики, оскільки дозволяє ефективно поєднати автоматизацію, аналітику та прогнозування для забезпечення більш безпечних і економічно вигідних перевезень вантажів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі запропоновано модель інтелектуальної IoT-системи для управління контейнерами в морській логістиці, яка базується на багаторівневій архітектурі з розподілом функцій між сенсорним, edge та серверним рівнями. Такий підхід забезпечує високий рівень автономності системи, дозволяючи зменшити затримки у реагуванні на зміни стану контейнерів та оперативно коригувати умови перевезення в реальному часі. Використання технологій для моніторингу температури, вологості і вібрацій забезпечує максимальний

контроль за вантажами, що особливо важливо для чутливих товарів, таких як медикаменти або харчові продукти.

Практична значущість запропонованої системи полягає у можливості інтеграції різноманітних IoT сенсорів з потужними сервісами для зберігання та обробки даних, що включають Apache Kafka, PostgreSQL та Redis. Таке поєднання дозволяє забезпечити високу швидкість обробки великих обсягів даних та їх миттєве збереження, що дає змогу забезпечити оперативне реагування на критичні зміни умов транспортування. Веб-інтерфейс, що забезпечує зручний доступ до управлінських функцій, дозволяє адміністраторам ефективно моніторити і змінювати параметри контейнерів, що значно підвищує ефективність управління логістичними операціями.

Перспективами подальших досліджень є вдосконалення системи через застосування алгоритмів машинного навчання для покращення аналізу зібраних даних та передбачення можливих аномалій у процесі перевезення. Крім того, розвиток технологій безпеки, таких як підвищене шифрування даних і контроль доступу через TLS і MQTT, дозволить зменшити ризики кіберзагроз і забезпечить додаткову надійність системи в реальних умовах експлуатації. Це сприятиме розвитку системи і дозволить її масштабувати на різні етапи логістичних операцій, що відкриває нові можливості для оптимізації перевезень і підвищення рівня безпеки у морській логістиці. [6]

ДЖЕРЕЛА

1. Bashiri, M., & Wright, K. (2020). Internet of Things (IoT) in Maritime Logistics: A Review. Journal of Maritime Technology and Engineering, 12(2), 45-60.
2. He, H., & Liu, Y. (2019). Real-time Container Tracking and Monitoring Using IoT Technologies. International Journal of Logistics Management, 30(3), 255-267.
3. Mell, P., & Grance, T. (2018). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Special Publication 800-145.
4. Chien, C. F., & Chen, M. (2021). Application of IoT in Transportation and Logistics: Challenges and Opportunities. Journal of Transportation Systems Engineering, 17(1), 35-49.
5. Kepner, A. (2017). Big Data and IoT in Maritime Industry: The Future of Smart Shipping. Journal of Intelligent Transportation Systems, 21(5), 503-515.
6. Sundararajan, V. (2020). The Rise of the Internet of Things: Implications for Logistics and Supply Chain Management. Journal of Supply Chain Management, 56(4), 30-44.



ДМИТРО БЕЗНОСЮК
Студент 4 курсу освітньої програми «Програмні технології інтернет речей» Факультету інформаційних технологій.
E-mail: dmitrybeznosiukcode@gmail.com
Навчаюся в Київському національному університеті імені Тараса Шевченка. Серед наукових інтересів: інтеграція IoT в соціальні сфери життя та економіку, логістика, автоматизація складських систем, високонавантажені системи обміну даними, радіоелектроніка та робототехніка.



ОЛЬГА КРАВЧЕНКО
К.т.н., доцент, доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка (Київ, Україна).
ORCID: 0000-0002-9669-2579
E-mail: olha.kravchenko@knu.ua
Серед наукових інтересів - побудова інформаційних технологій прийняття рішень в соціосистемах в умовах поведінкової економіки. Моделювання прикладних задач для дискретних пристроїв комп’ютерних систем.

ДИСТАНЦІЙНИЙ МОНІТОРИНГ ПАРАМЕТРІВ МІКРОКЛІМАТУ ОФІСНИХ ПРИМІЩЕНЬ НА ОСНОВІ МОДУЛЬНИХ IOT-СЕНСОРІВ

Олександр Березюк, Володимир Дружинін

Анотація. *У тезах представлено ідею та прототип програмно-апаратної системи дистанційного моніторингу параметрів мікроклімату офісних приміщень на прикладі компанії Onisoft. Рішення базується на модульних IoT-вузлах, які підтримують гнучкий вибір сенсорів (температура, відносна вологість, CO_2, пилові частинки, леткі органічні сполуки тощо) та передавання даних у хмарний бекенд для зберігання, обробки й візуалізації. Користувацький застосунок забезпечує перегляд показників у режимі, наближеному до реального часу, історичний аналіз, сповіщення про відхилення та експорт даних для подальшої аналітики.*

Ключові слова: Інтернет речей; мікроклімат; якість повітря в приміщеннях; офісні будівлі; IoT-сенсори.

I. ВСТУП

Сучасні організації дедалі більше залежать від якості внутрішнього середовища будівель, адже показники мікроклімату та ширше, IEQ (Indoor Environmental Quality), пов'язані з комфортом, самопочуттям і працездатністю людей в офісах. Оглядові дослідження підкреслюють, що IEQ є мультидоменним поняттям (тепловий комфорт, якість повітря, акустика, освітлення), а його погіршення може мати негативні наслідки для здоров'я та продуктивності.

Паралельно відбувається перехід від епізодичних вимірювань (перевірки «час від часу») до безперервного моніторингу на основі IoT-мереж. Практика реального-часу (або близького до нього) моніторингу дозволяє бачити короткочасні коливання, які виникають внаслідок активності людей, особливостей вентиляції або зовнішніх умов, і тим самим підтримувати керування будівлею більш «даними-керованим».

II. ДАНІ ТА МЕТОДИ

Концепція рішення спирається на розподілену архітектуру «сенсорні вузли, далі, транспорт даних, далі, обробка/зберігання, далі, клієнтський застосунок», як показано на Рисунку 1. Подібні багаторівневі підходи є типовими для систем моніторингу мікроклімату та IAQ/IEQ, оскільки дають змогу масштабувати кількість точок вимірювання, централізовано керувати даними та будувати зручні інтерфейси для користувачів і відповідальних за експлуатацію.

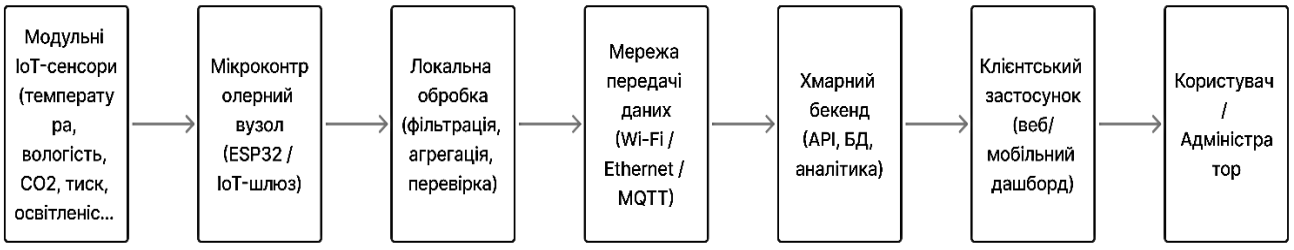


Рисунок 1. *Узагальнена архітектура системи дистанційного моніторингу мікроклімату*

У межах цієї роботи виділено такі основні компоненти системи: сенсорний рівень (edge-вузли), комунікаційний рівень, хмарний рівень (backend) та клієнтський рівень (застосунок/дашборд).

Сенсорний рівень реалізується на базі мікроконтролерів класу ESP32 або аналогічних пристроїв із можливістю підключення сенсорних модулів через цифрові інтерфейси. У практичних реалізаціях систем моніторингу мікроклімату такі контролери використовуються разом із сенсорами температури, вологості, освітленості та концентрації пилу (PM).

Комунікаційний рівень забезпечує передавання телеметрії за допомогою легковагого протоколу обміну повідомленнями MQTT, який працює за моделлю publish/subscribe. Для підвищення безпеки передавання даних застосовується TLS-шифрування.

Хмарний рівень відповідає за прийом, нормалізацію та зберігання даних (наприклад, у реляційній або time-series базі даних), формування агрегованих показників (хвилинних, годинних, добових) і надання API для клієнтських застосунків.

Клієнтський рівень реалізується у вигляді дашборду для відображення поточних значень, часових трендів і виявлення проблемних зон у приміщеннях. Подібні інтерфейси дозволяють користувачам швидко оцінювати стан мікроклімату та приймати рішення щодо покращення умов середовища.

Оскільки система підтримує модульність сенсорів, передбачається зберігання метаданих про сенсори (одиниці вимірювання, діапазони значень, частота вимірювань, пороги попереджень). Подібний підхід відповідає сучасним тенденціям розвитку систем моніторингу якості повітря, де поряд із збором даних застосовуються методи аналізу, виявлення аномалій та прогнозування, детальніший приклад, показано в Таблиці 1.

Таблиця 1. *Приклад параметрів мікроклімату та відповідних сенсорних категорій*

Сенсорна категорія	**Параметр**	**Практичне значення для офісу**	**Примітка щодо інтеграції**
Температура/ вологість	T, RH	Базовий тепловий комфорт; контроль сухості/ надмірної вологості	Стандартизовані інтерфейси; низька вартість інтеграції
CO_2	CO_2	Непрямий індикатор якості вентиляції/ завантаженості приміщення	Потребує коректного розміщення сенсора; чутливий до людей/ повітрообміну
Пилові частинки	PM2.5, PM10	Індикатор запиленості; важливий для IAQ та гігієнічного контролю	Можливі вимоги до обслуговування/ очищення; залежить від потоків повітря
ЛОС (TVOC/VOC)	TVOC/VOC	Додатковий індикатор якості повітря (побутова хімія, матеріали тощо)	Проблема відмінність показів від лабораторних приладів; потрібна валідація/ калібрування

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У бакалаврській роботі сформовано та реалізовано прототип рішення, що об’єднує IoT-вузли збору даних і прикладний рівень віддаленого моніторингу. Практична цінність підходу полягає у тому, що система не «жорстко прив’язана» до одного фіксованого сенсора, а підтримує масштабування набору параметрів та кількості приміщень, що відповідає типовим вимогам до IEQ-моніторингу (просторова неоднорідність, різні сценарії використання зон, динаміка в часі).

Функціонально прототип реалізує: реєстрацію об’єктів моніторингу (будівля/поверх/кімната) та прив’язку сенсорів до локацій, що підтримує подальшу просторову інтерпретацію даних (порівняння зон, пошук джерел дискомфорту). Подібний акцент на «просторово-часовій картині» є характерним для сучасних IEQ-мереж.

Потокову доставку телеметрії та збереження історії вимірювань для трендової аналітики. У практиках IEQ-моніторингу зустрічаються сценарії з високою частотою (наприклад, 1 хв), що дозволяє бачити короткі епізоди погіршення стану середовища.

IV. ВИСНОВКИ

Запропонований у бакалаврській роботі підхід до дистанційного моніторингу мікроклімату офісних приміщень узгоджується з сучасним трендом переходу до частого/безперервного IEQ-спостереження та використання IoT-мереж як основи для керування комфортом і прийняття експлуатаційних рішень. Зокрема, реальний-час моніторинг у дослідженнях показує користь для виявлення джерел дискомфорту та підтримки енергоефективних стратегій в офісних будівлях.

ДЖЕРЕЛА

1. Fissore, V. I., Fasano, S., Puglisi, G. E., et al. Indoor Environmental Quality and Comfort in Offices: A Review. Buildings, 2023, 13(10), 2490. https://www.mdpi.com/2075-5309/13/10/2490
2. Tsang, T.-W., Mui, K.-W., Wong, L.-T., et al. Real-Time Indoor Environmental Quality (IEQ) Monitoring Using an IoT-Based Wireless Sensing Network. Sensors, 2024, 24(21), 6850. https://www.mdpi.com/1424-8220/24/21/6850
3. Shoukry, F., Goubran, S., Tarabieh, K.. Enhanced Indoor Air Quality Dashboard Framework and Index for Higher Educational Institutions. Buildings, 2024, 14(6), 1640. https://www.mdpi.com/2075-5309/14/6/1640



ОЛЕКСАНДР БЕРЕЗЮК
Здобувач 4 курсу програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка, Київ, Україна
E-mail: berez_sasha@ukr.net
Науковий напрям/інтерес, IoT, моніторинг мікроклімату, системи збору даних, дашборди/аналітика, UX/UI дизайн у сфері IoT та промисловості.



ВОЛОДИМИР ДРУЖИНІН
д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@fit.knu.ua.
З 2023 року працює в КНУ ім. Тараса Шевченка. Має понад 100 наукових праць, серед яких 7 навчально-методичних посібників та 6 монографій.
Коло наукових інтересів: методи та алгоритми машинного навчання в радіолокаційних системах, радіомоніторинг та радіочастотний менеджмент, багатопозиційна радіолокація.

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СУЧАСНИХ СИСТЕМ РАДІОМОНІТОРИНГУ В АВТОМАТИЗОВАНИХ КІБЕРФІЗИЧНИХ СИСТЕМАХ

Ольга Бондаренко

Анотація. *У роботі розглянуто особливості функціонування сучасних систем радіомоніторингу в автоматизованих кіберфізичних системах. Проаналізовано роль радіомоніторингу як інформаційної підсистеми контролю електромагнітного середовища, що сприяє забезпеченню стабільності безпроводових комунікацій та підвищенню надійності технологічних процесів. Визначено основні технічні характеристики радіомоніторингових комплексів, зокрема параметри приймальних трактів, завадостійкість та апаратну архітектуру. Розглянуто принципи організації розподілених багатосенсорних систем спостереження, інтеграції сенсорних даних та їх значення для підвищення точності оцінки спектральної обстановки і підтримки прийняття рішень у системах контролю радіочастотного середовища.*

Ключові слова: кіберфізичні системи, мультисенсорні системи, системи радіомоніторингу, інтеграція сенсорних даних, підтримка прийняття рішень, спектральний аналіз, радіочастотне середовище.

I. ВСТУП

Системи радіомоніторингу посідають важливе місце в архітектурі сучасних автоматизованих і кіберфізичних систем, де забезпечення цілісності даних, стійкості каналів зв’язку та керованості технологічних процесів безпосередньо залежить від якості радіочастотного середовища. Збільшення кількості безпроводних пристроїв, розширення спектра технологій і ускладнення електромагнітної обстановки вимагають створення засобів контролю, здатних забезпечувати постійний збір, аналіз і інтерпретацію даних про стан спектра.

У структурі кіберфізичних виробничих систем радіомоніторинг виступає інформаційною підсистемою, що підтримує стабільність роботи промислових мереж, засобів керування та сенсорних вузлів. Уточнення спектральної обстановки дає змогу зменшувати кількість комунікаційних збоїв, підвищувати стійкість обміну даними та оптимізувати роботу завадостійких протоколів передачі інформації. Крім того, наявність моніторингових засобів дозволяє виявляти несанкціоновані випромінювання, які можуть впливати на безпеку процесів або створювати загрозу порушення технологічного циклу [1].

II. ТЕХНІЧНІ ХАРАКТЕРИСТИКИ СИСТЕМ РАДІОМОНІТОРИНГУ

Інформаційні можливості систем радіомоніторингу значною мірою визначаються параметрами електромагнітної сумісності радіоелектронних засобів, що працюють у спільному частотному діапазоні. Вплив взаємних завад, побічних випромінювань та нестабільності частоти може ускладнювати сприйняття спектральних даних, створювати хибні індикатори перевантаженості або приховувати важливі сигнали керування. Під час проєктування систем радіомоніторингу необхідно враховувати низку технічних характеристик приймальних трактів.

До ключових параметрів належать

- вибірковість;
- чутливість;
- стабільність робочої частоти;
- рівень власних шумів приймача.

Саме вони визначають здатність системи коректно сприймати сигнали у складному радіочастотному середовищі [2].

Окреме значення має завадостійкість апаратних засобів. У практичних умовах можливий вплив різних типів активних завад, зокрема спрямованих шумових сигналів або перешкод складної часово-частотної структури. У таких ситуаціях система контролю повинна зберігати спроможність виділяти інформативні параметри сигналів навіть тоді, коли співвідношення сигнал/завада є зниженим. Це важливо як для технологічних систем керування, так і для об'єктів, де критичною є надійність каналів обміну [3].

У процесі функціонування систем радіомоніторингу важливу роль відіграє організація збору, передавання та централізованої обробки вимірювальних даних від приймальних вузлів до центрів опрацювання інформації. Для цього застосовуються сучасні мережеві технології, що забезпечують синхронізацію вимірювань, передачу спектральної інформації та узгодження параметрів роботи розподілених елементів системи [4]. Особливе значення має забезпечення часової узгодженості вимірювань, оскільки результати аналізу спектра можуть значною мірою залежати від точності синхронізації приймальних модулів.

Використання сучасних інформаційно-комунікаційних протоколів дозволяє підвищити швидкість обміну даними між вузлами системи та забезпечити їх узгоджену роботу у реальному масштабі часу. Завдяки цьому стає можливим оперативне отримання інформації про стан радіочастотного середовища та швидке реагування на зміни електромагнітної обстановки [5].

Важливою умовою ефективного функціонування таких систем є також забезпечення достовірності, цілісності та захищеності переданої інформації, оскільки результати радіомоніторингу використовуються для підтримки прийняття управлінських рішень щодо оптимізації роботи безпроводових мереж, підвищення ефективності використання радіочастотного ресурсу та контролю електромагнітної обстановки [6].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Апаратні рішення сучасних радіомоніторингових комплексів включають широкосмугові приймачі, модульні антенно-фідерні системи, цифрові трактові підсистеми та обчислювальні модулі для високошвидкісної обробки сигналів. Від вибору апаратної архітектури залежить точність вимірювань, швидкість сканування спектра, стійкість до імпульсних завад та можливість забезпечення повного спектрального покриття в режимі реального часу. Розглянуті у технічних матеріалах [7-8] приклади підкреслюють, що збільшення смуги огляду супроводжується підвищеною чутливістю до параметрів динамічного діапазону, тому застосовуються комбіновані та багатоканальні схеми аналізу сигналів.

Додатковим фактором ефективності систем радіомоніторингу є використання сучасних програмно-алгоритмічних засобів аналізу сигналів. Застосування цифрових методів обробки сигналів дозволяє автоматизувати процес виявлення радіовипромінювань, оцінювання їх параметрів та класифікацію джерел сигналів. У сучасних комплексах використовуються методи спектрального аналізу, часово-частотного представлення сигналів, а також статистичні підходи до оцінювання рівнів завад і шумів [5]. Це забезпечує більш точне визначення параметрів сигналів навіть у складних електромагнітних умовах. Крім того, використання програмних засобів обробки даних дозволяє інтегрувати результати радіомоніторингу з інформаційними системами керування, що сприяє підвищенню ефективності функціонування автоматизованих кіберфізичних систем.

Організація розподілених систем радіомоніторингу спирається на принципи багатосенсорного спостереження, що передбачає просторове рознесення вузлів збору даних, синхронізацію каналів та інтеграцію інформаційних потоків у єдиному центрі опрацювання.

Така архітектура підвищує точність оцінки спектральних характеристик, дозволяє локалізувати джерела випромінювання, зменшує ризик втрати даних через завади або фізичні перешкоди та підвищує стійкість усієї інформаційно-керуючої системи [4-6].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отже, сучасні системи радіомоніторингу слід розглядати як складові частини інформаційних та інтелектуальних систем керування. Вони відіграють роль сенсорної підсистеми, що забезпечує функції контролю, діагностики та прогнозування стану радіочастотного середовища, сприяє стабільності безпроводових технологій і підтримує роботу автоматизованих виробничих та організаційно-технічних комплексів.

Розвиток таких систем пов’язаний зі зростанням вимог до швидкості аналізу, точності вимірювань і здатності працювати у складних спектральних умовах, що визначає актуальність подальших досліджень у галузі інтегрованих інформаційних систем керування, мультисенсорних систем радіомоніторингу та методів підтримки прийняття рішень на основі інтеграції сенсорних даних.

ДЖЕРЕЛА

1. Aksu, M. and Candell, R., 2017. Requirements for spectrum monitoring in industrial environments. NIST Interagency/Internal Report (NISTIR) 8195. Gaithersburg, MD: National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.IR.8195
2. Ільченко, М.Ю., Наритник, Т.М., Капштик, С.В., Авдєєнко, Г.Л., Корсун, В.І. та Присяжний, В.І., 2023. Планування та електромагнітна сумісність в безпроводових інфокомунікаціях. Навчальний посібник. Київ: КПІ ім. Ігоря Сікорського
3. Шолохов, С.М., Самборський, І.І., Вакуленко, О.В. та Ніколаєнко, Б.А., 2021. Завадозахист радіоелектронних засобів. Частина 1: Основи завадозахисту систем зв’язку. Навчальний посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського.
4. Elmenreich, W., 2002. Sensor fusion in time-triggered systems. PhD dissertation. Vienna University of Technology, Vienna.
5. Толюпа, С.В., Дружинін, В.А., Наконечний, В.С., Цьопа, Н.В. та Батрак, Є.О., 2014. Методи та алгоритми обробки та захисту радіолокаційної інформації у багатопозиційних системах зі змінною просторовою конфігурацією. Монографія. Київ: Логос.
6. Український державний центр радіочастот, 2020. Український державний центр радіочастот: Історія та сучасність. URL: https://www.ucrf.gov.ua/about/storinki-istoriyi/kniga-ukrayinskij-derzhavnij-centr-radiochastot-istoriya-ta-suchasnist
7. International Telecommunication Union, 2020. Handbook on spectrum monitoring. Geneva: International Telecommunication Union.
8. RSWM GmbH, 2021. Modern radio spectrum monitoring: trade-off between bandwidth and dynamic range. White paper. Stuttgart: RSWM GmbH.



ОЛЬГА БОНДАРЕНКО
асистент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-0024-8789
E-mail: olha.bondarenko@knu.ua
Фахівець у галузі інформаційних систем, телекомунікацій та радіомовлення. Практичний досвід роботи у сфері телекомунікацій та медіаінфраструктури понад 8 років. Досвід викладання в університетах України понад 3 роки.
Наукові інтереси – інформаційно-комунікаційні системи, системи радіомоніторингу, мультисенсорні технології та IoT.

МЕТОДИ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА ТЕРМІЧНОЇ СТАБІЛЬНОСТІ МОБІЛЬНИХ ГРАФІЧНИХ СИСТЕМ ШЛЯХОМ ВОЛЬТ-ЧАСТОТНОЇ ОПТИМІЗАЦІЇ

Роман Вагін

Анотація. *Досліджено процес вольт-частотної оптимізації (андерволтингу) мобільного графічного процесора RTX 4060. Проаналізовано методику корекції кривої напруги для досягнення максимальної стабільності та продуктивності чипа. Встановлено, що фіксація напруги на рівні 0.9 В дозволяє отримати 10 053 бали в бенчмарку FurMark, що перевищує показники заводських налаштувань. Запропонована методика є універсальною для оптимізації та підвищення ресурсу сучасних комп'ютерних систем.*

Ключові слова: андервольтинг, RTX 4060 Laptop, V-f curve, MSI Afterburner, вольт-частотна характеристика, енергоефективність, FurMark.

I. ВСТУП

Експлуатація сучасних мобільних графічних систем у заводському стані часто супроводжується подачею надлишкової напруги на ядро графічного процесора (ГП). Виробники встановлюють універсальні параметри напруги живлення для забезпечення стабільної роботи будь-якого екземпляра кремнію, незалежно від його індивідуальної якості. Це призводить до підвищеного енергоспоживання та передчасного досягнення термічних лімітів (троттлінгу), що особливо критично для ігрових ноутбуків з обмеженим внутрішнім простором.

Актуальність даного дослідження полягає в необхідності пошуку методів підвищення енергоефективності без втрати чистої продуктивності системи. Основним інструментом для вирішення цієї задачі є андервольтинг — процес індивідуального налаштування вольт-частотної характеристики (V-f curve). Такий підхід дозволяє не лише знизити температуру кристала, а й стабілізувати тактові частоти на вищих показниках завдяки вивільненню запасу потужності.

II. ДАНІ ТА МЕТОДИ

Дослідження проводилося на базі ноутбука ASUS TUF Gaming A15, оснащеного ГП NVIDIA GeForce RTX 4060 (архітектура Ada Lovelace) з повним теплопакетом (TGP 140W). Для маніпуляцій з вольт-частотною характеристикою використовувався редактор кривих (Curve Editor) у програмному комплексі MSI Afterburner. Тестування стабільності та вимірювання продуктивності проводилося у бенчмарку FurMark (роздільна здатність 1920x1080). Методика полягала у покроковому зниженні напруги ядра при збереженні цільової частоти 2500 МГц.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У процесі експериментальної корекції вольт-частотної характеристики графічного процесора NVIDIA GeForce RTX 4060 (мобільна версія) було встановлено оптимальне значення напруги для частоти 2500 МГц на рівні 0.9 В, що відображено на Рисунку 1. Така фіксація дозволила суттєво знизити енергоспоживання та тепловиділення кристала без втрати цільової продуктивності. Як показано на Рисунку 2, застосування обраного профілю напруги запобігає надмірному нагріву GPU та повністю виключає термічний троттлінг навіть

під тривалим навантаженням. Це особливо критично для мобільних систем з обмеженим внутрішнім простором, де ефективність охолодження є ключовим фактором стабільної роботи. В результаті оптимізації вдалося не лише знизити температуру, але й стабілізувати тактові частоти на вищих показниках завдяки вивільненню запасу потужності.

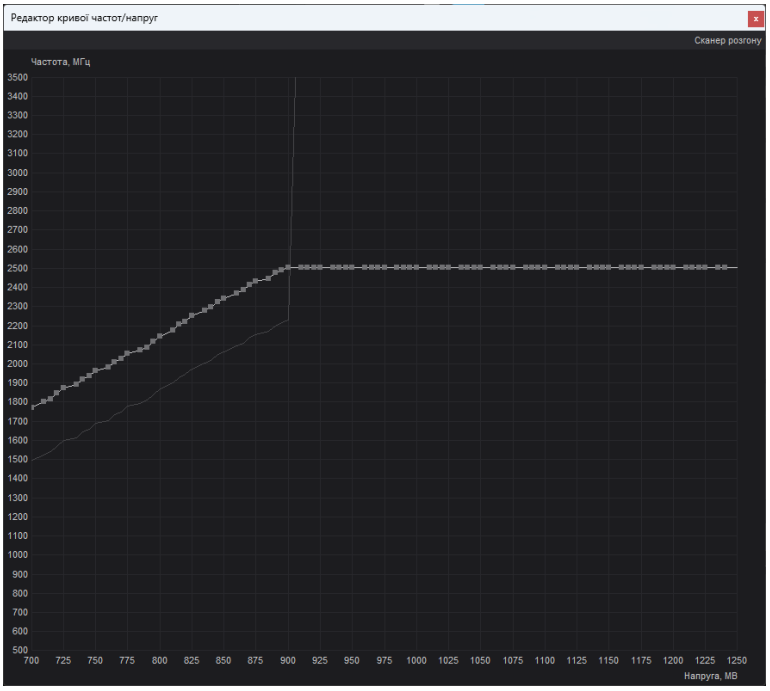


Рисунок 1. *Редактор кривої частот/напруг*

GPU0	NVIDIA GeForce RTX 4060 Laptop GPU
PCI IDs	DEV: 10DE-28E0 - SUB: 1043-19DD - REV: A1
graphics driver	591.59
max core usage	99 %
max core temperature	86 °C
core clock	min: 2250 MHz - max: 2506 MHz
max power	140 W

Рисунок 2. *Технічні параметри та показники стану графічного процесора під час тестування*

Кількісна оцінка ефективності запропонованого методу підтверджується результатами тестування у бенчмарку FurMark (роздільна здатність 1920×1080), де графічний процесор досяг показника 10 053 балів (Рисунок 3). Цей результат перевищує продуктивність системи з заводськими налаштуваннями, що свідчить про успішне вивільнення додаткового потенціалу чипа. Варто зазначити, що подальше зниження напруги нижче 0.85 В у даному тестовому сценарії призводило до нестабільності роботи, артефактів зображення та падінь частоти. Це підтверджує існування індивідуальної межі вольт-частотної характеристики для конкретного зразка графічного процесора при пікових навантаженнях, що робить процедуру

андервольтингу унікальною для кожного екземпляра кремнію. Таким чином, знайдений баланс між напругою 0.9 В та частотою 2500 МГц є оптимальним для даного чипа, забезпечуючи максимальну стабільність, продуктивність та енергоефективність.

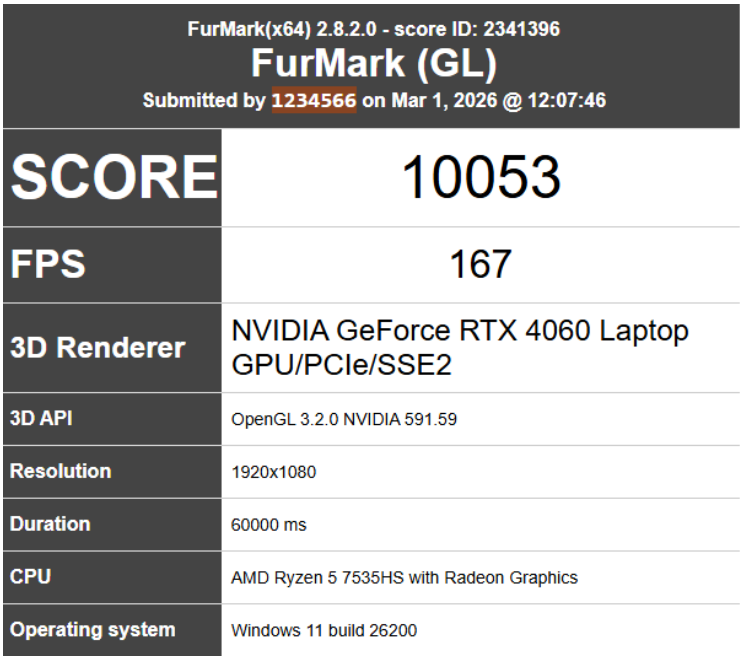


Рисунок 3. *Результати тестування*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Андервольтинг є найбільш ефективним методом програмної оптимізації сучасних комп'ютерних систем. Встановлення фіксованої напруги 0.9 В забезпечує максимальну продуктивність та термічну стабільність, що робить мобільне рішення ефективнішим за середньобюджетні десктопні системи. Результати дослідження мають пряме практичне значення для сервісного обслуговування та модернізації високопродуктивної техніки, дозволяючи подовжити термін її безвідмовної експлуатації.

ДЖЕРЕЛА

1. MSI Afterburner User Guide. URL: https://www.msi.com/page/afterburner
2. NVIDIA Ada Lovelace Architecture Whitepaper. NVIDIA Corporation, 2022. 45 p.
3. Стрельніков, В. І., & Бондарчук, А. П. (2025). Комплексний підхід до інтелектуального управління, моделювання та виявлення мережних аномалій на основі ентропійних та нейромережевих підходів. Телекомунікаційні та інформаційні технології, (2), 100-107.
4. Geeks3D FurMark Benchmarking Tool. URL: https://geeks3d.com/furmark/



РОМАН ВАГІН
лаборант кафедри комп'ютерних наук, Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0009-4577-9920
E-mail: roman.education000@gmail.com
Наукові інтереси: комп'ютерні системи.

МЕТОД ВЕРИФІКАЦІЇ ТА КОНТЕКСТНОЇ ФІЛЬТРАЦІЇ ГЕТЕРОГЕННИХ ДАНИХ ЕКОЛОГІЧНОГО МОНІТОРИНГУ ДЛЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Кирило Вадурін, Олексій Лелека, Максим Рубан

Анотація. *Робота присвячена підвищенню надійності інформаційної систем підтримки прийняття рішень у сфері муніципального екологічного моніторингу шляхом попередньої обробки потокових даних з IoT-пристроїв. Запропоновано метод верифікації даних, що базується на кореляційному аналізі взаємозв'язків між параметрами мікроклімату та концентрацією забруднюючих речовин. Розроблено та протестовано алгоритм трирівневої фільтрації, який включає компенсацію впливу вологості на оптичні сенсори, виявлення перехресної чутливості електрохімічних датчиків та контекстну класифікацію джерел забруднення. Експериментальна апробація на масиві даних обсягом понад 2100 годин спостережень продемонструвала здатність методу автоматично ідентифікувати та відфільтрувати 10,4% технічних збоїв, а також класифікувати 0,5% подій як такі, що вимагають управлінського втручання, що значно знижує навантаження на операторів системи.*

Ключові слова: СППР, IoT-сенсори, якість повітря, кореляційний аналіз, верифікація даних, перехресна чутливість, PM2.5.

I. ВСТУП

Стрімка урбанізація та цифровізація міського управління у 2025–2026 роках актуалізують питання впровадження інтелектуальних систем підтримки прийняття рішень (СППР) для екологічного моніторингу. Сучасні концепції Smart City передбачають розгортання щільних мереж сенсорів низької вартості, які генерують масиви різнорідних даних у реальному часі. Як зазначають у статті [1], інтеграція таких даних з методами штучного інтелекту відкриває нові можливості для оперативного реагування на екологічні загрози. Водночас дослідники [2] вказують на проблему низької селективності та високого рівня шуму бюджетних вимірювальних пристроїв, що призводить до значної кількості хибних спрацювань та ефекту «втоми від тривог» у диспетчерів муніципальних служб.

Існуючі підходи до побудови СППР, розглянуті у роботі [3], часто зосереджуються на візуалізації агрегованих показників або використанні складних моделей машинного навчання без достатньої уваги до фізичної верифікації вхідних сигналів. Проблемою залишається відсутність стандартизованих алгоритмів попередньої обробки, здатних у режимі реального часу розрізняти апаратні збої сенсорів, вплив метеорологічних факторів та реальні епізоди забруднення. Метою даної роботи є розробка та експериментальна перевірка методу кореляційного аналізу та фільтрації даних для підвищення достовірності інформації в системах муніципального моніторингу атмосферного повітря.

II. ДАНІ ТА МЕТОДИ

Об'єктом дослідження обрано масиви часових рядів параметрів якості повітря, отримані з мультисенсорних пристроїв моніторингу. Для експериментальної перевірки гіпотез використано набір даних «2023 Indoor Air Quality Dataset Germany» [4], що містить 63 632 записи з дискретністю вимірювань близько 120 секунд. Дані охоплюють період з березня по липень 2023 року та включають вимірювання у двох різних середовищах: лабораторному приміщенні з контрольованими умовами та житловому приміщенні з високою антропогенною активністю. Набір змінних включає концентрації твердих часток (PM1,

PM2.5, PM10), газів (CO, CO2, NO2, SO2, O3), летючих органічних сполук (TVOC) та метеопараметри (температура, відносна та абсолютна вологість, атмосферний тиск).

Методологія дослідження базується на послідовному застосуванні розвідувального аналізу даних, кореляційного аналізу та сценарного моделювання роботи СППР. На першому етапі проведено очищення даних від фізично неможливих значень, спричинених дрейфом нуля сенсорів. Зокрема, для показників концентрації газів SO2, NO2 та твердих часток застосовано процедуру відсікання від'ємних значень, які виникають внаслідок температурних флуктуацій електроліту в електрохімічних комірках. Для забезпечення порівнянності різнорідних даних виконано ресемплінг часових рядів до годинних середніх значень, що відповідає стандарту звітності муніципальних систем моніторингу.

Основний етап дослідження включав перевірку трьох ключових гіпотез щодо взаємозв'язків між параметрами. Перша гіпотеза стосувалася впливу гігроскопічного росту частинок на покази оптичних сенсорів PM2.5. Для її перевірки розраховано коефіцієнти кореляції між вологістю та концентрацією пилу, а також побудовано регресійні моделі для визначення порогу відсікання. Друга гіпотеза перевіряла наявність перехресної чутливості електрохімічних сенсорів SO2 до чадного газу, що є типовою проблемою бюджетних пристроїв. Третя гіпотеза розглядала можливість ідентифікації джерел забруднення (зв'язок зовнішніх викидів та вентиляції) через аналіз синхронності динаміки CO2 та TVOC. На основі підтверджених гіпотез сформовано вектор правил для автоматичної класифікації станів системи. Обробка даних та візуалізація результатів здійснювалися у середовищі Python з використанням бібліотек Pandas, NumPy, Matplotlib та Seaborn.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Первинний статистичний аналіз виявив суттєві відмінності у структурі даних між локаціями. У житловому приміщенні середній рівень TVOC становив 1888 ppb проти 367 ppb у лабораторії, що підтверджує вплив побутової активності. Водночас аналіз часових рядів показав наявність аномальних сплесків концентрації діоксиду сірки до 1750 мкг/м³, що значно перевищує гранично допустимі концентрації та несумісне з життям.

Детальний кореляційний аналіз дозволив виявити природу цих аномалій. Розрахунок матриці кореляцій Спірмена для газової групи показав сильний позитивний зв'язок між CO та SO2 ($r = 0,46$) при відсутності кореляції SO2 з маркерами транспортних викидів, такими як NO2. Візуалізація динаміки цих показників, наведена на Рисунку 1, демонструє повну синхронність піків SO2 та CO. Це підтверджує гіпотезу про апаратну помилку селективності: сенсор реагує на чадний газ, генеруючи хибні дані про наявність сірчистого ангідриду. Впровадження правила блокування даних SO2 при одночасному зростанні CO дозволило відфільтрувати 225 годин хибних тривог, що становить 10,4% від загального часу спостережень.

Аналіз залежності показів оптичних пиломірів від вологості підтвердив наявність інтерференції. У лабораторних умовах коефіцієнт кореляції між вологістю та PM2.5 склав 0,37. На діаграмі розсіювання на Рисунку 2 чітко виділяється точка біфуркації на рівні 55% відносної вологості, після якої дисперсія показів PM2.5 зростає експоненційно. На основі цього спостереження в алгоритм СППР введено правило нелінійної корекції показників PM при вологості >55%. Розрахункове середнє завищення показників через вологу склало 0,09 мкг/м³, проте в окремі періоди високої вологості коригування досягало 15–20 мкг/м³, запобігаючи помилковій класифікації метеорологічних явищ як епізодів забруднення.



Рисунок 1. *Синхронна динаміка CO2 та TVOC як індикатор недостатньої вентиляції*



Рисунок 2. *Кореляція між показами SO2 та CO*

Дослідження взаємозв'язку CO2 та TVOC виявило найсильнішу кореляцію в наборі даних r = 0,52. Синхронна динаміка цих параметрів, проілюстрована на Рисунку 3, свідчить про те, що основним джерелом погіршення якості повітря є метаболічна активність людей та недостатній повітрообмін. Це дозволило сформувати правило контекстної діагностики: перевищення порогів по обох параметрах класифікується системою не як «токсичне забруднення», а як подія «порушення режиму вентиляції». За період експерименту виявлено 11 годин таких подій, з яких 6 годин залишилися у фінальному звіті як пріоритетні рекомендації для користувача.

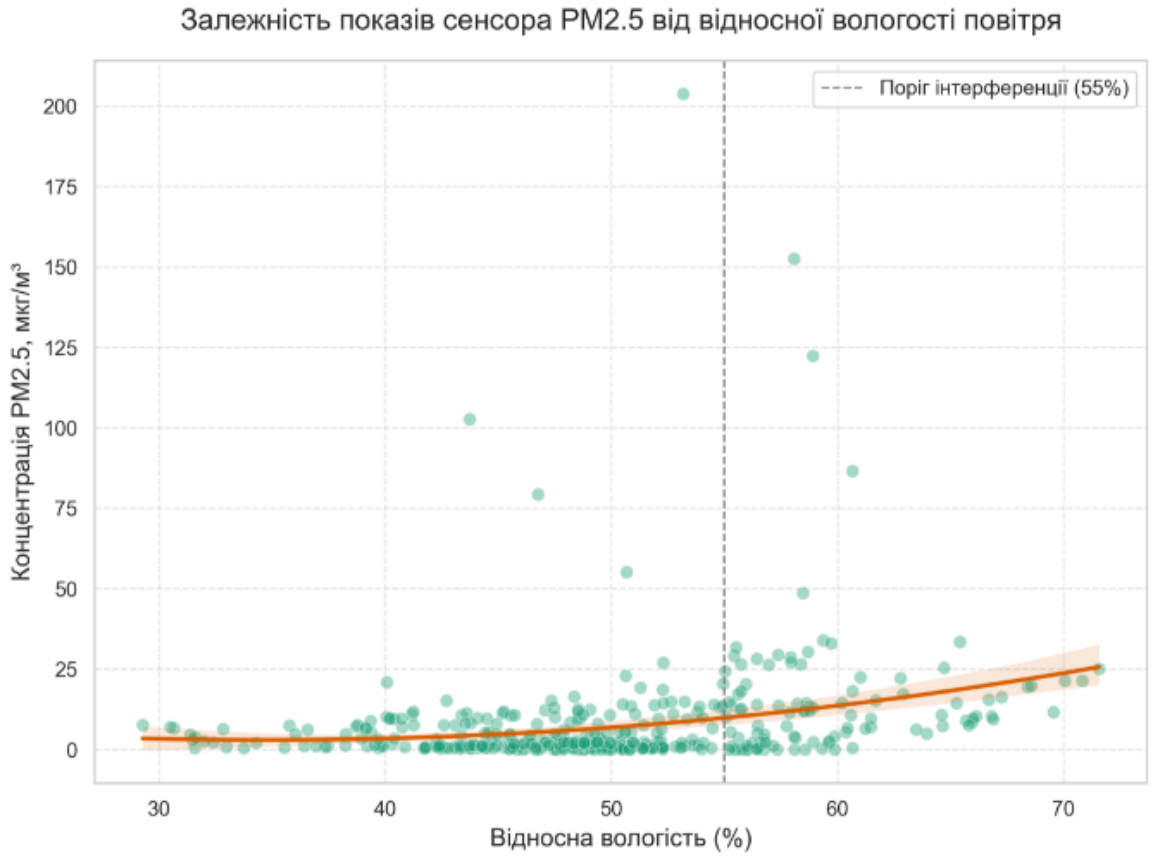


Рисунок 3. *Залежність показів сенсора PM2.5 від відносної вологості повітря*

Загальна ефективність запропонованого методу оцінювалася за розподілом статусів системи після обробки [5]. Із 2154 годин спостережень 1908 годин (88,6%) класифіковано як нормальний стан, 225 годин (10,4%) – як технічний збій сенсорів, 15 годин (0,7%) – як реальне перевищення нормативів забруднення PM2.5, і 6 годин (0,3%) – як потреба у вентиляції. Такий розподіл свідчить про високу селективність методу та здатність відсіювати переважну більшість хибних сигналів, які в традиційних системах призводять до помилкових управлінських рішень.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати свідчать про те, що використання «сирих» даних з бюджетних IoT-сенсорів для прийняття управлінських рішень є неприпустимим через високу ймовірність хибних спрацювань. Експериментально доведено, що без алгоритмічної компенсації перехресної чутливості електрохімічні сенсори можуть генерувати показники, що імітують техногенні аварії. Запропонований підхід, який базується на перевірці фізичної узгодженості даних, дозволяє нівелювати апаратні недоліки сенсорів програмними засобами.

Дослідженням встановлено, що інтеграція різнорідних даних (газовий склад + метеопараметри) дозволяє не лише фіксувати факт забруднення, а й визначати його контекст. Розділення подій на категорії «Забруднення» (зовнішній вплив) та «Порушення вентиляції» (внутрішній вплив) є вагомим для формування адекватних рекомендацій у СППР. Застосування розроблених правил дозволило досягти мети роботи – створити метод попередньої обробки даних, який підвищує інформативність моніторингу без необхідності заміни апаратного забезпечення.

Перспективи подальшого розвитку методу полягають у переході від детермінованих правил до адаптивних моделей машинного навчання.

ДЖЕРЕЛА

1. Balogun A.-L., Marks D., Sharma R. [et al.]. Assessing the Potentials of Digitalization as a Tool for Climate Change Adaptation and Sustainable Development in Urban Centres // Sustainable Cities and Society. 2020. Vol. 53. Art. 101888. URL: https://doi.org/10.1016/j.scs.2019.101888.
2. Ali R., Hussain A., Nazir S. [et al.]. Intelligent Decision Support Systems—An Analysis of Machine Learning and Multicriteria Decision-Making Methods // Applied Sciences. 2023. Vol. 13, no. 22. Art. 12426. URL: https://doi.org/10.3390/app132212426.
3. Alamanos A., Rolston A., Papaioannou G. Development of a Decision Support System for Sustainable Environmental Management and Stakeholder Engagement // Hydrology. 2021. Vol. 8, no. 1. Art. 40. URL: https://doi.org/10.3390/hydrology8010040.
4. Welfposer. 2023 Indoor Air Quality Dataset Germany. [Data set] // Kaggle. 2023. URL: https://www.kaggle.com/datasets/welfposer/2023-indoor-air-quality-dataset-germany.
5. Babbar H., Rani S. AI-Driven integration of remote sensing and geospatial data for Enhanced environmental monitoring and decision-making // International Journal of Remote Sensing. 2025. P. 1–17. URL: https://doi.org/10.1080/01431161.2025.2514820.



КИРИЛО ВАДУРІН
асистент кафедри комп'ютерної інженерії та електроніки у Кременчуцького національного університету імені Михайла Остроградського, Кременчук, Україна.
ORCID: 0000-0001-7781-5783
E-mail: kir3337@gmail.com
Займаюся проєктуванням складних апаратних комплексів із побудовою прогностичних моделей на основі нейронних мереж для цифровізації різних об'єктів.



ОЛЕКСІЙ ЛЕЛЕКА
аспірант 1-го курсу кафедри екології та біотехнології Кременчуцького національного університету імені Михайла Остроградського, Кременчук, Україна.
ORCID: 0009-0008-8298-6286
E-mail: LelekaOleksii@proton.me
Мій науковий інтерес полягає у створенні засобів підтримки прийняття рішень у системах моніторингу атмосферного повітря з різнорідними екологічними даними.



МАКСИМ РУБАН
здобувач 4-го курсу спеціальності 123 Комп'ютерна інженерія у Кременчуцькому національному університеті імені Михайла Остроградського, Кременчук, Україна.
E-mail: rumaksim4@gmail.com
Працюю над розробкою концепцій об'єднання квантових та класичних методів обчислень для підвищення точності прогнозування складних екологічних показників.

МОДЕЛЬ СИСТЕМИ ЖИТТЄЗАБЕЗПЕЧЕННЯ ОСОБИ З КАРДІОЛОГІЧНИМИ РОЗЛАДАМИ

Єгор Винник, Володимир Дружинін

Анотація. *У роботі представлено модель системи життєзабезпечення особи з кардіологічними розладами, спрямовану на безперервний контроль життєво важливих показників та своєчасне реагування на критичні стани. Описано структуру системи, що включає сенсорні модулі збору фізіологічних даних, засоби передавання інформації та аналітичний блок обробки показників. Розглянуто принципи інтеграції інтелектуальних алгоритмів аналізу для прогнозування ризиків та підтримки прийняття медичних рішень. Запропонована модель підвищує рівень безпеки пацієнта, забезпечує оперативність медичного втручання та сприяє покращенню якості медичного супроводу.*

Ключові слова: IoT, система життєзабезпечення, кардіологічні розлади.

I. ВСТУП

Серцево-судинні захворювання залишаються ключовою проблемою сучасної медицини та однією з основних причин смертності населення. За статистичними оцінками World Health Organization, вони спричиняють понад 17 млн смертей щороку, що становить приблизно третину всіх летальних випадків у світі [1]. Така ситуація вимагає розроблення нових технологічних підходів до контролю стану пацієнтів із кардіологічними розладами, особливо тих, хто потребує постійного медичного спостереження. Традиційні методи діагностики базуються на періодичних обстеженнях у медичних закладах, що не дозволяє своєчасно фіксувати короткочасні або раптові патологічні зміни.

Одним із перспективних напрямів вирішення цієї проблеми є створення інтелектуальних систем життєзабезпечення, які здійснюють безперервний моніторинг фізіологічних показників людини в реальному часі. Такі системи поєднують технології сенсорики, бездротового зв’язку, обробки великих даних і штучного інтелекту. Вони дають змогу не лише спостерігати за станом пацієнта, а й прогнозувати ризики розвитку критичних станів, що особливо важливо для осіб із серцевими патологіями. Метою цієї роботи є розроблення моделі системи життєзабезпечення особи з кардіологічними розладами та аналіз її функціональних можливостей.

II. ДАНІ ТА МЕТОДИ

Запропонована модель базується на багаторівневій архітектурі, що складається із сенсорного, комунікаційного, обчислювального та користувацького рівнів.

Сенсорний рівень включає набір біомедичних датчиків, які фіксують життєво важливі параметри: електрокардіограму, частоту серцевих скорочень, артеріальний тиск, рівень насичення крові киснем і температуру тіла. Використання носимих пристроїв дозволяє отримувати дані безперервно та без дискомфорту для пацієнта. Згідно з клінічними рекомендаціями American Heart Association, тривалий моніторинг серцевого ритму значно підвищує ймовірність раннього виявлення аритмій і запобігання серйозним ускладненням [2].

Комунікаційний рівень відповідає за передавання інформації від датчиків до центру обробки. Для цього застосовуються енергоефективні бездротові технології, такі як Bluetooth Low Energy, ZigBee або NB-IoT. Стандарти передавання даних регламентуються технічними рекомендаціями IEEE, які визначають вимоги до надійності, безпеки та стабільності медичних телеметричних систем [3].

Обчислювальний рівень представлений сервером або хмарною платформою, де здійснюється зберігання та аналіз інформації. Обробка даних включає фільтрацію шумів, статистичний аналіз, побудову трендів і прогнозування. Для цього використовуються алгоритми машинного навчання, які навчаються на історичних медичних записах пацієнта.

Рівень взаємодії з користувачем реалізується у вигляді програмного інтерфейсу для лікаря та пацієнта. Система відображає графіки показників, автоматичні попередження та рекомендації щодо дій у разі відхилення параметрів від норми.

Методологічно дослідження базується на системному підході, що передбачає моделювання структури, аналіз потоків даних та оцінку функціональної надійності. Для перевірки ефективності моделі використано методи порівняльного аналізу та математичного прогнозування ризиків.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На рисунку 1 зображено структурну архітектуру системи віддаленого моніторингу стану пацієнта, яка демонструє взаємодію користувацького інтерфейсу, серверної інфраструктури, мереж передачі даних та медичних сенсорів. Схема відображає логіку роботи інформаційно-телемедичної системи, що забезпечує збір, передавання, обробку та аналіз фізіологічних показників у реальному часі. Така архітектура є типовою для сучасних медичних IoT-рішень і використовується для підтримки безперервного контролю стану здоров’я пацієнтів.

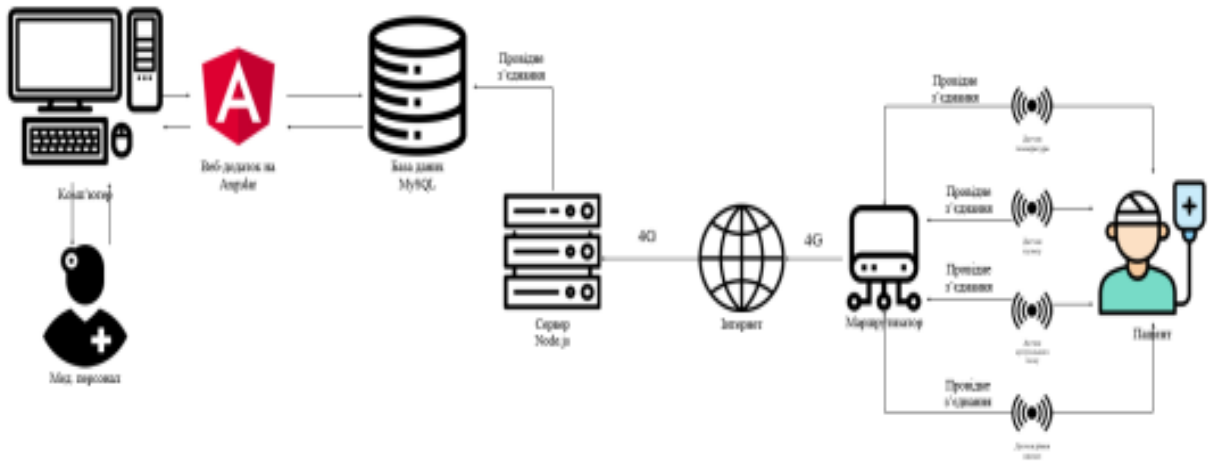


Рисунок 1. *Схематичне зображення IoT моделі системи життєзабезпечення особи з кардіологічними розладами*

Зліва зображено користувацький рівень, який включає комп’ютер клієнта та медичного працівника. Через веб-застосунок користувач отримує доступ до системи моніторингу.

Далі інформація передається до бази даних MySQL, де відбувається зберігання медичних показників. Поруч розташований сервер прикладної логіки (Node.js), який забезпечує обробку запитів, взаємодію між клієнтською частиною та базою даних, а також формування відповідей системи.

Наступний етап — мережевий рівень, представлений інтернет-з’єднанням із використанням каналу 4G. Через нього дані передаються до мобільного шлюзу або контролера збору інформації.

Праворуч показано сенсорний рівень, що складається з набору біомедичних датчиків, підключених до пацієнта. Кожен датчик передає окремий тип фізіологічних параметрів

(наприклад, пульс, тиск, біосигнали). Сигнали надходять до шлюзу, який агрегує їх і пересилає на сервер для подальшого аналізу.

Уся система утворює замкнений цикл:

датчики → шлюз → інтернет → сервер → база даних → інтерфейс лікаря,

що забезпечує безперервний дистанційний контроль стану пацієнта та оперативне реагування на відхилення показників.

IV. ВИСНОВКИ

Розроблена модель системи життєзабезпечення особи з кардіологічними розладами демонструє можливість створення інтегрованого технологічного середовища для постійного контролю стану здоров'я. Поєднання сенсорних пристроїв, телекомунікаційних технологій та інтелектуального аналізу даних забезпечує раннє виявлення патологічних змін, зменшує ризик ускладнень і підвищує ефективність медичного супроводу.

Запропонована система сприяє переходу від традиційної реактивної медицини до превентивної моделі, де основний акцент робиться на прогнозуванні та профілактиці захворювань. Подальший розвиток досліджень у цьому напрямі пов'язаний із підвищенням точності алгоритмів аналізу, мініатюризацією сенсорів, покращенням автономності пристроїв і розширенням функцій штучного інтелекту. Очікується, що впровадження подібних систем стане важливим кроком до формування цифрової персоналізованої медицини майбутнього.

ДЖЕРЕЛА

1. World Health Organization. Cardiovascular diseases (CVDs). URL: https://www.who.int/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds)
2. American Heart Association. What is cardiac telemetry? URL: https://www.heart.org/en/health-topics/consumer-healthcare/what-is-cardiac-telemetry
3. IEEE. Standards Association — Standards. URL: https://www.ieee.org/standards/index.html



ЄГОР ВИННИК
студент 1 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
ORCID: 0009-0000-9066-924X
E-mail: egorka.vinnik.4@gmail.com
Серед наукових інтересів – розробка IoT-систем, проєктування систем моніторингу та їх застосування в медичних цілях.



ВОЛОДИМИР ДРУЖИНІН
д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@knu.ua
Коло наукових інтересів: методи та алгоритми машинного навчання в радіолокаційних системах, радіомоніторинг та радіочастотний менеджмент, багатопозиційна радіолокація.

МЕТОД ДИСТАНЦІЙНОГО АНАЛІЗУ РЕЗУЛЬТАТІВ ГРИ В НАСТІЛЬНИЙ ТЕНІС

Юлія Вознюк, Максим Трембовецький

Анотація. *У роботі розглядається метод автоматизованого дистанційного аналізу результатів гри в настільний теніс на основі розподіленої IoT-архітектури. Актуальність теми зумовлена необхідністю мінімізації людського фактора та підвищення точності фіксації ігрових подій у реальному часі. Запропоноване рішення базується на інтеграції алгоритмів адаптивної цифрової фільтрації, багаторівневих протоколів криптографічного захисту та методів оптимізації мережевих маршрутів, що дозволяє створити цілісну екосистему для моніторингу та аналітики.*

Ключові слова: інтернет речей, настільний теніс, дистанційний аналіз, цифрова фільтрація, захист даних, мережева оптимізація, автоматизація суддівства.

I. ВСТУП

Сучасний спорт потребує автоматизації для усунення суб'єктивності суддівства. У динамічному настільному тенісі людського ока часто недостатньо, що зумовлює необхідність впровадження високоточних цифрових систем фіксації результатів у реальному часі. Концепція інтернет-речей (iot) дозволяє об'єднати сенсори та хмарні сервіси в єдину аналітичну екосистему. Це забезпечує дистанційний доступ до верифікованих даних, надаючи тренерам та організаторам надійний інструмент для моніторингу ігрових показників. Дана робота присвячена методу дистанційного аналізу, що поєднує точність вимірювань із захищеністю мережевої інфраструктури. Метою є створення стійкої моделі, яка гарантує цілісність та достовірність даних в умовах інтенсивного ігрового процесу.

II. ДАНІ ТА МЕТОДИ

Система дистанційного аналізу результатів гри в настільний теніс базується на розподіленій IoT-архітектурі, що забезпечує високу швидкість обробки даних, безпеку передачі інформації та об'єктивність суддівства. Вона використовує сучасні методи цифрової обробки сигналів, що дозволяють проводити прецизійний моніторинг траєкторії руху м'яча та ігрових подій у режимі реального часу [1].

Основні компоненти системи включають:

- Мережа інтелектуальних сенсорів та камер, що забезпечують постійне відстеження просторових координат м'яча, фіксуючи моменти відскоку від столу, торкання сітки або вихід за межі ігрового поля [3].
- Модуль цифрової фільтрації даних, який дозволяє очистити вхідний сигнал від стохастичних шумів та похибок вимірювань, забезпечуючи математично точну модель польоту м'яча [1].
- Система криптографічного захисту та тунелювання, яка гарантує цілісність переданих даних від сенсорів до сервера, унеможливлюючи несанкціоноване втручання або підміну результатів підрахунку очок.
- Графічний веб-інтерфейс, представлений у вигляді інтерактивного дашборду, що дозволяє суддям, тренерам та глядачам переглядати статистику гри, аналізувати траєкторії ударів та отримувати миттєві сповіщення про спірні моменти.

Система працює на базі центрального сервера з використанням сучасних протоколів передачі даних, що забезпечує мінімальну затримку (latency) та стабільність роботи навіть при інтенсивному обміні інформацією. Водночас передбачена логічна валідація даних на

стороні сервера для відсікання аномальних значень, спричинених технічними збоями (Рисунок 1).

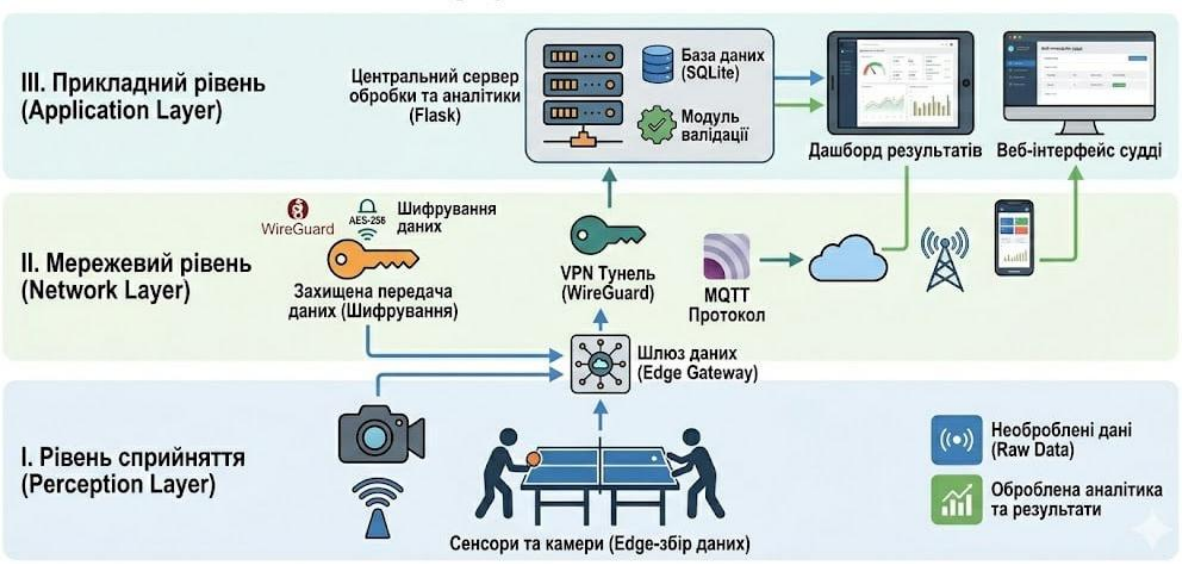


Рисунок 1. *Архітектура автоматизованої системи дистанційного аналізу гри в настільний теніс*

Додатково система може бути розширена функціями автоматичного відеоповтору критичних моментів на основі отриманих координат. Наприклад, можливе впровадження алгоритмів, що автоматично маркують "спірні м'ячі" (край столу або торкання сітки). Також перспективним є використання методів глибокого навчання для класифікації типів ударів (топ-спін, підрізка), що дасть змогу проводити глибокий біомеханічний аналіз техніки гравця [2]. У перспективі система може включати мобільний додаток із доповненою реальністю (AR), що дозволить глядачам бачити траєкторію та швидкість м’яча в реальному часі прямо на екрані смартфона. Це значно підвищить ефектність спортивних подій та сприятиме цифровізації тренувального процесу в настільному тенісі.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Розроблена система дистанційного аналізу результатів гри в настільний теніс продемонструвала високу ефективність у забезпеченні об'єктивності суддівства та точності фіксації ігрових подій. Завдяки інтеграції сенсорних технологій, алгоритмів цифрової фільтрації та захищених каналів передачі даних, система значно покращує швидкість реагування на динамічні зміни в ігровому процесі. Основні переваги впровадженого рішення включають:

1. Висока точність фіксації. Автоматизований моніторинг траєкторії м’яча та координат відскоку дозволяє безпомилково визначати спірні моменти (край столу, торкання сітки, аут). Це мінімізує вплив людського фактора та забезпечує максимальну справедливість результатів змагань [3].
2. Захищеність та цілісність даних. Використання криптографічних протоколів та логічної валідації на сервері гарантує, що ігрова статистика захищена від зовнішнього втручання або технічних збоїв. Це особливо важливо для професійних турнірів, де достовірність даних є критичною.
3. Мінімальна затримка (Low Latency). Оптимізація мережевої архітектури та маршрутизації забезпечує передачу даних у режимі реального часу. Це дозволяє

використовувати систему не лише для післяігрового аналізу, а й для миттєвого відображення результатів на табло та в трансляціях.

4. Глибока аналітична база. Детальна реєстрація кожного удару дозволяє формувати розширені звіти про техніку гравців, що значно спрощує процес підготовки спортсменів та допомагає тренерам виявляти зони для покращення [2].

Верифіковані дані системи дозволяють прогнозувати ігрові тенденції та розробляти індивідуальні стратегії, роблячи тренування науково обґрунтованими та результативними. Завдяки автоматизації моніторингу, це рішення стає ключовим інструментом для спортивних федерацій та академій у вдосконаленні технологічних процесів і забезпеченні високої якості змагань.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Автоматизація моніторингу в настільному тенісі є важливим кроком до підвищення об’єктивності спортивних змагань. Впровадження сучасних технологій дистанційного аналізу та IoT-архітектури дозволяє покращити точність фіксації результатів, підвищити динаміку гри та мінімізувати ризики, пов'язані з помилками суддівства.

Розроблена система дистанційного аналізу результатів гри демонструє значний потенціал для впровадження у спортивних академіях, тренувальних центрах та професійних федераціях. Подальший розвиток цієї технології може включати інтеграцію нейронних мереж для глибшого біомеханічного аналізу рухів гравця [2], розширення функціоналу для підтримки AR-трансляцій та розробку мобільних додатків для миттєвого доступу до персональної статистики.

Таким чином, запропоноване рішення є ефективним інструментом для цифровізації спортивної галузі, підвищення продуктивності тренувального процесу та забезпечення високої якості проведення змагань у настільному тенісі.

ДЖЕРЕЛА

1. Zhang, L., Wang, Y., & Li, H. (2022). “Table Tennis Ball Tracking Using YOLOv5 and Kalman Filter.” International Journal of Computer Vision and Sport Analytics.
2. Kim, S., & Lee, J. (2021). “Real-Time Accurate Determination of Table Tennis Ball and Evaluation of Player Stroke Effectiveness with Computer Vision-Based Deep Learning”.
3. Yang, B., Liu, J., & Zhao, Y. (2021). Falling-Point Recognition and Scoring Algorithm in Table Tennis Using Dual-Channel Target Motion Detection.



ЮЛІЯ ВОЗНЮК
Студентка 1 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка
E-mail: vozniukyu@fit.knu.ua.



МАКСИМ ТРЕМБОВЕЦЬКИЙ
доктор технічних наук, професор, Кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-5240-7131
E-mail: trembovetskyim@fit.knu.ua

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНФІГУРУВАННЯ МОДУЛЬНИХ РОБОТІВ НА ОСНОВІ ГІБРИДНОГО АЛГОРИТМІЧНОГО ПІДХОДУ

Денис Гаватюк, Катерина Сисак

Анотація. *У роботі представлено результати розробки та модернізації інтелектуальної системи автоматизованого підбору оптимальних конфігурацій LEGO-роботів. Розглянуто проблему багатокритеріальної оптимізації в умовах жорстких обмежень. Запропоновано гібридний підхід, що поєднує модифікований жадібний алгоритм для генерації рішень у реальному часі та генетичний алгоритм для пошуку глобального оптимального розв'язку. Описано архітектуру системи на базі Python (FastAPI) та PostgreSQL, а також наведено результати експериментального порівняння швидкодії та якості отриманих конструкцій.*

Ключові слова: LEGO-робототехніка; багатокритеріальна оптимізація; жадібний алгоритм; генетичний алгоритм; автоматизоване проєктування.

I. ВСТУП

Стрімкий розвиток робототехніки та поширення модульних систем, таких як LEGO Technic та Mindstorms, зумовлюють потребу у швидкому та ефективному проєктуванні технічних об'єктів. Незважаючи на широкі можливості цих конструкторів, підбір оптимальної конфігурації з урахуванням суперечливих обмежень за вагою, бюджетом і функціональністю залишається складною комбінаторною задачею (див., наприклад, [2-4]). Проблема може бути розглянута як багатокритеріальна NP-складна задача про рюкзак, де кількість можливих комбінацій компонентів може перевищувати десятки тисяч варіантів (див., наприклад, [1]).

Актуальність дослідження зумовлена відсутністю інструментів для автоматизованого синтезу конфігурацій. Існуючі рішення забезпечують лише візуалізацію або перевірку вже готових моделей, проте не пропонують механізмів інтелектуального синтезу. Метою даної роботи є створення програмного комплексу початкового рівня для автоматизації процесу підбору компонентів, що забезпечує баланс між швидкістю отримання результату та інженерною досконалістю конструкції.

II. ДАНІ ТА МЕТОДИ

У розробленій інтелектуальній системі використано гібридний алгоритмічний підхід. На першому рівні застосовано модифікований жадібний алгоритм, який виконується у три етапи: створення технічного плану, послідовний підбір компонентів за пріоритетом та фінальна перевірка сумісності. Такий підхід забезпечує лінійну обчислювальну складність та миттєву відповідь інтерфейсу. Другий рівень використовує генетичний алгоритм, що імітує еволюційні процеси (селекція, кросовер, мутація) для пошуку глобального оптимального розв'язку у великому просторі можливих конфігурацій.

Архітектура системи побудована на основі фреймворків FastAPI та React. Сховище даних реалізовано з використанням системи керування базами даних PostgreSQL із застосуванням типу даних JSONB, що дозволяє динамічно описувати фізичні параметри деталей без зміни схеми бази даних. Для підвищення відмовостійкості системи впроваджено механізм відкладеного підключення та автоматичне перемикання на локальну базу даних у разі недоступності основного сервера.

Функціональна модель архітектури системи представлена на Рисунку 1.

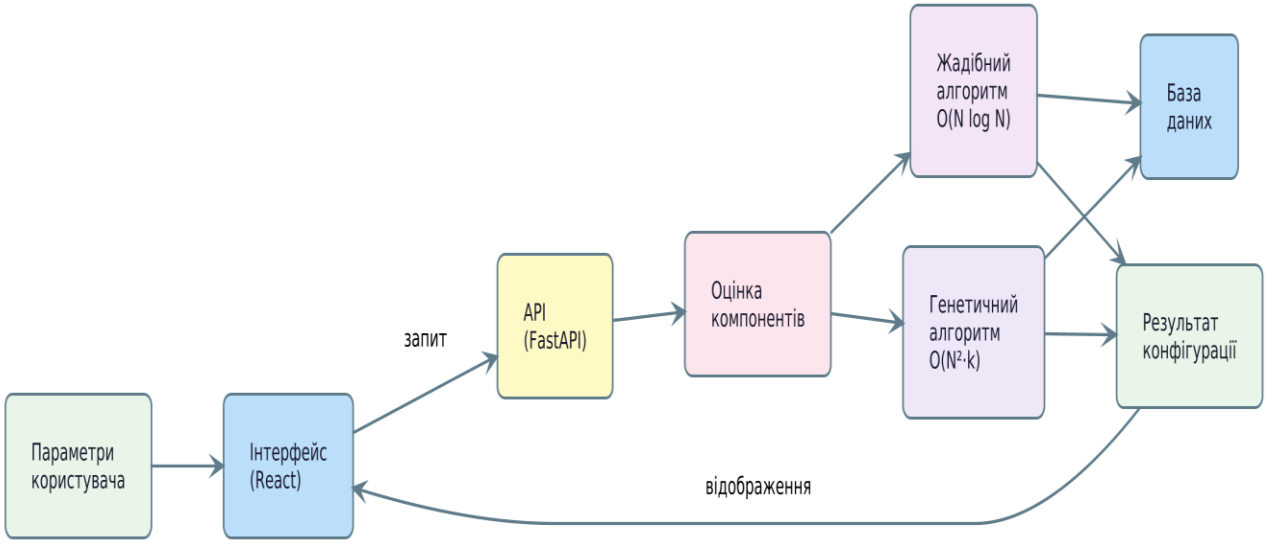


Рисунок 1. *Функціональна модель архітектури системи конфігурування*

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Експериментальна перевірка проводилася на синтетичному наборі даних, що включав характеристики реальних компонентів LEGO. Аналіз швидкодії жадібного алгоритму показав лінійну залежність часу обробки від кількості деталей. Для 10 000 одиниць час генерації склав 114 мс, що підтверджує можливість використання методу в інтерактивних веб-застосунках. Генетичний алгоритм продемонстрував на 40% вищу якість рішень порівняно з випадковим підбором при часі виконання до 96 секунд.

Ефективність реалізованих алгоритмів представлена у Таблиці 1.

Таблиця 1. *Порівняльна ефективність реалізованих алгоритмів*

Показник порівняння	**Жадібний підхід**	**Генетичний підхід**
Обчислювальна складність	O(N log N)	O(N² k)
Середній час відповіді	0.045 - 0.25 с	45 - 96 с
Якість рішення	Квазіоптимальна	Глобально оптимальна

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Розроблений програмний комплекс довів свою спроможність автоматизувати трудомісткий процес підбору компонентів роботів. Гібридна модель дозволяє ефективно поєднувати швидкість жадібних методів та точність генетичних алгоритмів. Впровадження моделі зваженої суми Weighted Sum Model дозволило інтегрувати п’ять ключових метрик (швидкість, сила, економія, витривалість, екологічність) з можливістю гнучкого налаштування пріоритетів. Функціональною особливістю розробленої системи є режим Eco-Mode, що автоматично перерозподіляє вагові коефіцієнти, надаючи пріоритет

енергоефективності, що дозволяє отримати збалансовані конфігурації для тривалих автономних місій. Застосування дворівневої стратегії пошуку, що поєднує жадібний алгоритм для миттєвої генерації та генетичний алгоритм для структурної оптимізації, забезпечує баланс між швидкістю роботи та якістю проєктних рішень.

Отримані результати створюють надійний фундамент для створення хмарного середовища автоматизованого проєктування модульних систем.

Практична значущість роботи полягає у можливості використання модуля у STEM-освіті та для швидкого інженерного прототипування. Подальший розвиток проєкту передбачає розширення переліку правил автоматичної перевірки фізичної сумісності вузлів та вдосконалення операторів мутації генетичного алгоритму для підвищення стійкості знайдених рішень.

ДЖЕРЕЛА

1. Böckenhauer H.-J., Commette A., Komm D. and Královič R. (2026) A survey of online knapsack problems, Discrete Applied Mathematics, 378, 492–507.
2. Dai Y., He S., Nie X., Zhang J. and Li Y. (2024) Research on reconfiguration strategies for self-reconfiguring modular robots: A review. Journal of Intelligent & Robotic Systems, 110, p. 47.
3. Liu Y., Zhang H. and Wang J. (2023) Genetic algorithm-based optimal design of modular robot topology based on distributed parallel kinematic modeling and analysis. Engineering Applications of Artificial Intelligence, 123(7), 106251.
4. Vu L. A. T., Bi Z., Mueller D. and Younis N. (2023) Modular self-configurable robots—The state of the art, Actuators, 12(9), p. 361.



ДЕНИС ГАВАТЮК
студент 4 курсу бакалаврату, кафедра інтелектуальних технологій, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
E-mail: gavatukden@gmail.com
Навчається на 4-му курсі бакалаврату за освітньою програмою “Комп’ютерні науки” на кафедрі інтелектуальних технологій. Сфера наукових інтересів охоплює розробку інтелектуальних систем автоматизованого проєктування, алгоритми багатокритеріальної оптимізації та прикладне застосування еволюційних алгоритмів у робототехніці.



КАТЕРИНА СИСАК
асистент кафедри інтелектуальних технологій, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0001-6363-0382
E-mail: kateryna.sysak@knu.ua
Отримала ступінь бакалавра (2012 р.), а згодом магістра (2014 р.) з математики у Київському національному університеті імені Тараса Шевченка (Київ, Україна). У 2018 році захистила дисертацію за спеціальністю 01.01.06 – алгебра та теорія чисел, і здобула науковий ступінь кандидата фізико-математичних наук. Наукові інтереси пов’язані з дослідженнями у сфері лінійної алгебри, теорії алгебр Лі, теорії кілець та модулів.

МОДЕЛІ ДЕТЕКЦІЇ АНОМАЛІЙ В IOT-СИСТЕМАХ

Євген Гаврасієнко, Володимир Дружинін

Анотація. *Дослідження присвячене розробці моделі підвищення енергоефективності та пропускної здатності IoT-мереж шляхом впровадження інтелектуальної фільтрації трафіку на Edge-рівні. Авторами запропоновано використання компактних TinyML моделей на базі архітектури автоенкодерів безпосередньо на мікроконтролерах ESP32. Це дозволяє реалізувати логіку селективної передачі даних: трансляція Payload у хмарне сховище ініціюється лише при детекції аномальних станів об'єкта моніторингу. Такий підхід забезпечує скорочення надлишкового трафіку на 80-95%, знижує витрати на хмарні квоти Azure IoT Hub та суттєво подовжує термін автономної роботи кінцевих вузлів.*

Ключові слова: IoT; tinyML; автоенкодер; детекція аномалій; енергоефективність; edge Computing; azure IoT hub.

I. ВСТУП

У сучасних концепціях Інтернету речей (IoT) спостерігається тенденція до експоненціального зростання кількості сенсорів, що генерують безперервні потоки даних. Традиційна архітектура збору інформації передбачає постійну передачу сирих вимірів до хмарних платформ для подальшого аналізу. Однак такий підхід супроводжується низкою критичних недоліків: перевантаженням каналів зв'язку, високою вартістю обробки даних у хмарі (Ingestion costs) та швидким розрядом акумуляторних батарей сенсорних вузлів через енерговитратність радіопередачі. Це підкреслює необхідність розробки нових підходів, які б поєднували технологічну доступність та інтелектуальність.

Використання парадигми Edge Computing у поєднанні з технологією TinyML дозволяє перенести етап первинної аналітики безпосередньо на кінцеві пристрої з обмеженими ресурсами. Впровадження нейромережевих моделей для детекції аномалій як «інтелектуального фільтра» дозволяє відсікати нормальні стани системи локально, що трансформує пасивний збір даних у подійно-орієнтовану модель моніторингу (Event-driven monitoring).

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

В межах реалізації проєкту SmartIoT було спроєктовано та апробовано систему на базі мікроконтролера ESP32 та хмарної платформи Azure. Основу інтелектуального аналізу становить модель автоенкодера, реалізована за допомогою стека TinyML. Для тренування використовувалися часові ряди нормальної роботи сенсорних вузлів (синусоїдальні сигнали з накладеним гаусовим шумом). Модель має симетричну структуру: вхідний шар приймає вікно з 10 значень, які послідовно стискаються через прихований шар (8 нейронів) до «пляшкового горла» (Bottleneck) розміром у 4 нейрони. На цьому етапі мережа вивчає латентне представлення сигналу, відкидаючи статистичний шум. Декодер відновлює сигнал до початкового розміру

$$\hat{x} = g(f(x, \theta_{enc}), \theta_{dec}) \quad (1)$$

де θ_{enc} — ваги моделі, отримані під час навчання на «нормальних» даних.

Для забезпечення працездатності на ESP32 було застосовано процедуру квантування ваг (Full Integer Quantization), що дозволило зменшити розмір моделі до декількох кілобайт. Це критично, оскільки після компіляції прошивка разом із бібліотекою TensorFlow Lite Micro

займає близько 85% доступної Flash-пам'яті пристрою (1.1 МБ), залишаючи ресурси для роботи стека Wi-Fi та MQTT.

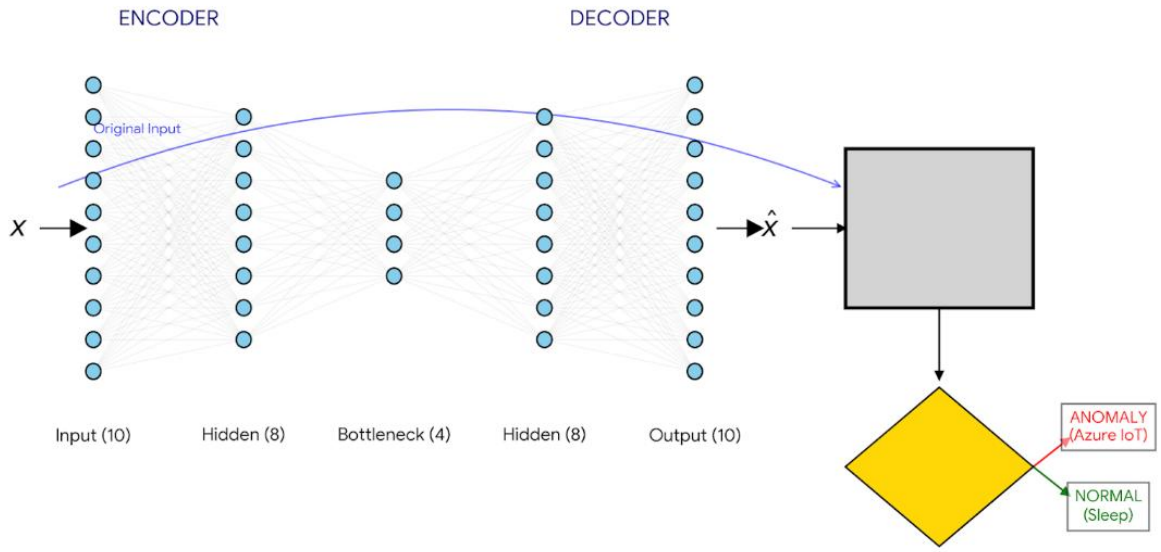


Рисунок 1. *Структура моделі автоенкодера для стиснення та детекції аномалій.*

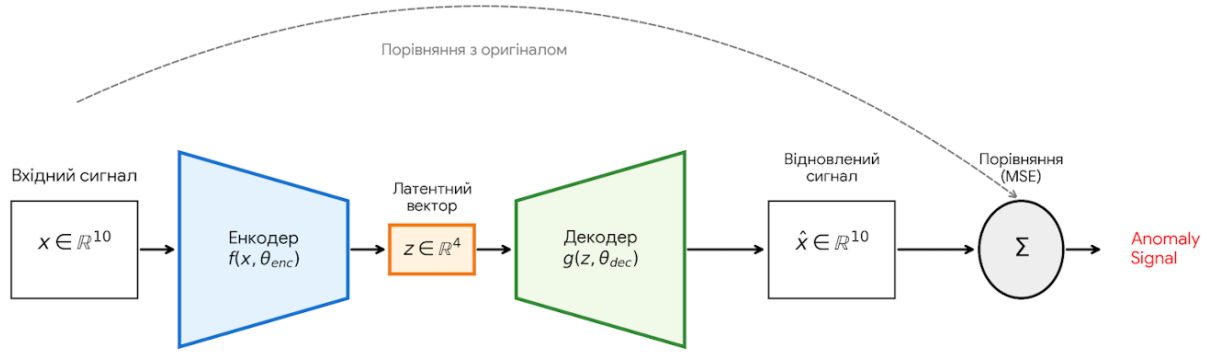


Рисунок 2. *Детальна схема реконструкції та обчислення помилки.*

Детекція аномалій базується на вимірюванні помилки реконструкції (MSE). У разі відхилення поточного сигналу від патернів, на яких навчалася модель, MSE різко зростає:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x_i})^2 \quad (2)$$

Логіка управління трафіком реалізується через порогову функцію активації передачі. Якщо $MSE > \tau$, де τ — поріг чутливості, система ініціює MQTT-сесію та передає Payload до Azure IoT Hub.

III. ВИСНОВКИ

Впровадження TinyML-моделей автоенкодерів безпосередньо у прошивку кінцевих пристроїв дозволило трансформувати архітектуру системи з пасивного збору даних у подійно-орієнтовану модель. Це вирішує фундаментальну проблему надлишковості даних, оскільки передача Payload у хмару ініціюється лише при виявленні статистично значущих відхилень (аномалій), що підтверджено розрахунками помилки реконструкції (MSE).

Експериментальна апробація методу на базі мікроконтролерів ESP32 продемонструвала можливість скорочення обсягу вихідного трафіку на 85-95% без втрати критично важливої діагностичної інформації. Крім того, мінімізація активності радіомодуля (Wi-Fi/MQTT сесій) дозволила збільшити життєвий цикл автономних пристроїв.

ДЖЕРЕЛА

1. Warden, P., & Situnayake, D. (2020). “TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers”. O'Reilly Media. URL: https://www.oreilly.com/library/view/tinyml/9781492052036/
2. TensorFlow. (2024). “TensorFlow Lite for Microcontrollers: Anomaly Detection Example”. Google Open Source. URL: https://www.tensorflow.org/lite/microcontrollers
3. Situnayake, D., & Plunkett, J. (2022). "AI at the Edge: Real-Time Analysis with Embedded Systems". O'Reilly Media. URL: https://www.oreilly.com/library/view/ai-at-the/9781098110544/
4. Ramesh, R., et al. (2023). "Edge-Based Anomaly Detection in Industrial IoT Using Autoencoders". IEEE Internet of Things Journal, Vol. 10(4). URL: https://ieeexplore.ieee.org/document/9014332
5. ESP32 Tech. (2023). “Low Power Modes and Energy Optimization for ESP32-based IoT Devices”. Espressif Systems. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/system/sleep_modes.html



ЄВГЕН ГАВРАСІЄНКО
студент 2 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: evgengavrasienko@gmail.com
Науковий інтерес зосереджений на розробці IoT-систем з використанням TinyML на кінцевих пристроях для побудови подійно орієнтованих систем.



ВОЛОДИМИР ДРУЖИНІН
д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@fit.knu.ua.
З 2023 року працює в КНУ ім. Тараса Шевченка. Має понад 100 наукових праць, серед яких 7 навчально-методичних посібників та 6 монографій.
Коло наукових інтересів: методи та алгоритми машинного навчання в радіолокаційних системах, радіомоніторинг та радіочастотний менеджмент, багатопозиційна радіолокація.

ІНТЕГРАЦІЯ IOT-ПРИСТРОЇВ В ІНФОРМАЦІЙНІ СИСТЕМИ УПРАВЛІННЯ СКЛАДОМ ДЛЯ МОНІТОРИНГУ В РЕАЛЬНОМУ ЧАСІ

Антон Галай, Ірина Борисенко

Анотація. *У роботі досліджено проблему латентності даних у класичних системах управління складом (WMS). Запропоновано архітектурний підхід до інтеграції гетерогенних IoT-пристроїв (RFID, сенсори середовища) через шар периферійних обчислень (Edge Computing). Розроблено імітаційну модель інформаційної системи, яка дозволяє оцінити вплив автоматизованого збору телеметрії на швидкість оновлення даних про залишки та точність позиціювання вантажів. Наведено порівняльний аналіз ефективності алгоритмів обробки подій у реальному.*

Ключові слова: Інтернет речей, WMS, архітектура інформаційних систем, MQTT, Edge Computing, імітаційне моделювання.

I. ВСТУП

Ефективність сучасних логістичних систем безпосередньо залежить від швидкості та достовірності інформаційних потоків. Класичні WMS-системи, що базуються на дискретних операціях сканування штрих-кодів, створюють часовий розрив між фізичною подією (переміщення товару) та її цифровою реєстрацією. Ця затримка унеможливлює прийняття оперативних рішень у реальному часі. Метою роботи є розробка та дослідження методу інтеграції IoT-пристроїв в інформаційну систему складу для мінімізації параметра та забезпечення наскрізного моніторингу процесів

II. ДАНІ ТА МЕТОДИ

Для вирішення задачі побудови масштабованої системи моніторингу пропонується трирівнева архітектура, яка розділяє потоки даних на "гарячі" (оперативні сповіщення) та "холодні" (архівна телеметрія).

На Рисунку 1 зображено розроблену схему інформаційних потоків, де ключовим елементом є брокер повідомлень, що забезпечує асинхронну взаємодію компонентів.

Для перевірки гіпотези було застосовано метод імітаційного моделювання. Розроблений програмний комплекс генерує потік подій, що відповідає інтенсивності роботи складу класу "А". Вхідними даними для моделі є: кількість складських операцій за одиницю часу, середня швидкість руху навантажувачів та топологія складського приміщення.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

В ході дослідження було проведено серію експериментів для порівняння двох підходів до збору даних: ручного (Manual Data Entry) та автоматизованого (IoT-based). Основними метриками ефективності були обрані час обробки однієї палети (T_{proc}) та ймовірність помилки ідентифікації (P_{err}).Аналіз результатів моделювання показав залежність навантаження на серверну частину системи від обраної стратегії агрегації даних на шлюзах.

На Рисунку 2 представлена діаграма послідовності, що ілюструє логіку обробки події переміщення товару в розробленій системі, яка дозволяє уникнути надлишкових запитів до бази даних.

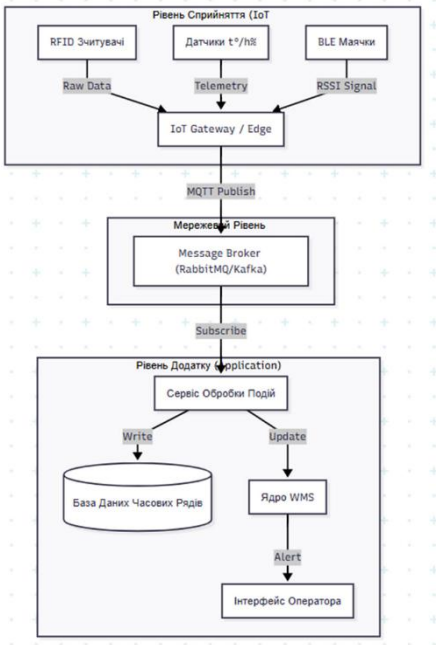


Рисунок 1. *Архітектура інформаційних потоків у запропонованій системі*

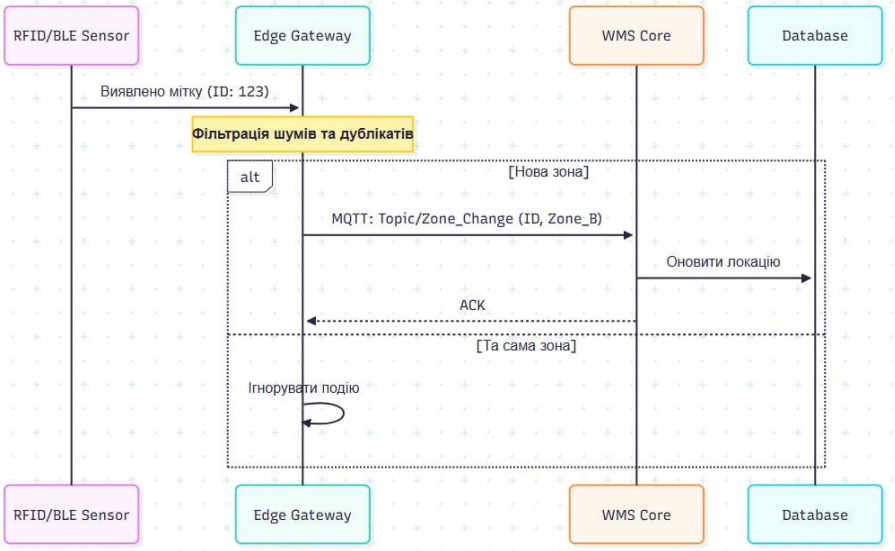


Рисунок 2. *Алгоритм обробки подій переміщення на рівні Edge Computing*

Порівняльна характеристика функціональних можливостей досліджуваних підходів наведена в Таблиці 1.

Таблиця 1. *Порівняння традиційного та IoT-підходів до управління складом*

Характеристика	**Традиційна WMS**	**WMS + IoT (Запропонована)**
Тригер оновлення даних	Дія оператора (сканування)	Фізична подія (автоматично)
Дискретність моніторингу	Висока (точки контролю)	Низька (безперервний потік)
Людський фактор	Пряма залежність	Мінімізований
Контроль умов зберігання	Періодичний замір	Real-time алертинг
Вартість інфраструктури	C_{base} (низька)	$C_{base}+C_{IoT}$ (висока)

Графік залежності часу актуалізації даних від кількості одночасних операцій демонструє нелінійне зростання затримок у традиційних системах, тоді як IoT-система демонструє стабільність завдяки асинхронній черзі повідомлень

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати дослідження підтверджують, що інтеграція IoT-пристроїв дозволяє трансформувати WMS з облікової системи в систему оперативного управління. Використання протоколу MQTT та попередньої обробки даних на периферії (Edge) вирішує проблему "великих даних", дозволяючи масштабувати систему без критичного збільшення навантаження на центральний сервер. Подальші дослідження будуть спрямовані на розробку алгоритмів предиктивного аналізу на основі накопичених історичних даних про рух товарів.

Разом із тим, результати обговорення виявляють низку викликів, пов'язаних із практичним впровадженням запропонованої архітектури. Серед основних бар'єрів слід відзначити порівняно високі початкові капітальні інвестиції в розгортання сенсорної інфраструктури. Також необхідно враховувати фізичні обмеження поширення радіосигналів у складських приміщеннях із високою концентрацією металевих конструкцій, що вимагає складного радіопланування. Окремим критичним аспектом залишається інформаційна безпека: зростання кількості підключених кінцевих IoT-вузлів розширює поверхню для потенційних кібератак, вимагаючи впровадження надійних протоколів наскрізного шифрування та автентифікації пристроїв

ДЖЕРЕЛА

1. Industry 4.0 in Logistics and Supply Chain Management: A Systematic Literature Review. // Engineering Management Journal, 2021.
2. The Internet of Things in the Cold Chain Logistics: An RFID-Based Monitoring System. // Sensors,2021.
3. Digital Twin in Logistics: A Review of Definitions, Properties, and Application Scenarios. // LogisticsJournal, 2021.
4. Warehouse Management System and IoT Integration for Intelligent Logistics. // International Journal of Applied Mathematics, Electronics and Computers, 2022.
5. Internet of Things for Smart Warehousing: A Comprehensive Review. // IEEE Internet of Things Journal, 2023.



АНТОН ГАЛАЙ
Студент 2-го курсу магістратури, факультету інформаційних технологій, Київ, Україна
ORCID: 0009-0009-1676-9037
E-mail: gal07072003@gmail.com
Навчаюсь в Київському національному університеті імені Тараса Шевченка. Серед наукових інтересів — вивчення новітніх технологій автоматизації складів, оцінці їх ефективності та впливу на логістичні процеси.



ІРИНА БОРИСЕНКО
Кандидат технічних наук, доцент кафедри інформаційних систем та технологій, Фаультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0005-8350-6422
E-mail: borysenkoi@fit.knu.ua
Науковий інтерес зосереджений на дослідженні інформаційних систем, захисті інформації, програмуванні.

ПІДХОДИ ДО АНАЛІЗУ МОНІТОРИНГОВИХ ДАНИХ ПОПУЛЯЦІЙ ШКІДНИКІВ В УМОВАХ ОБМЕЖЕНОГО СПОСТЕРЕЖЕННЯ

Владислав Гнатієнко, Віталій Снитюк

Анотація. *У роботі розглянуто проблему інтерпретації даних моніторингу популяцій шкідників у польових умовах за обмеженої кількості джерел спостереження. Дані моніторингу, що формуються у вигляді часових рядів кількості комах у пастках, можуть містити пропуски та відображати вплив різних зовнішніх факторів. Сформульовано задачі аналізу цих даних, зокрема визначення моменту доцільного застосування засобів захисту рослин, прогнозування розвитку популяції та оцінювання достатньої частоти спостережень. Запропоновано підходи до аналізу моніторингових даних з урахуванням обмеженої кількості спостережень.*

Ключові слова: моніторинг популяцій шкідників, аналіз моніторингових даних, підходи до аналізу, часові ряди, обмежений моніторинг.

I. ВСТУП

Продовольча безпека значною мірою залежить від стабільності сільськогосподарського виробництва та ефективності управління агроекосистемами. Однією з важливих задач у цьому контексті є своєчасне виявлення загроз для посівів, зокрема зростання чисельності шкідників. У сучасній практиці моніторинг популяцій комах часто здійснюється за допомогою пасток, що формують часові ряди кількості особин протягом сезону, на основі яких оцінюють стан популяції та приймають рішення щодо застосування засобів захисту рослин.

Для деяких видів шкідників ефективність застосування інсектицидів обмежується відносно коротким часовим інтервалом. Наприклад, для кукурудзяного стеблового метелика цей інтервал може становити близько одного тижня. Передчасне або запізніле втручання може суттєво знижувати ефективність захисних заходів.

У наукових дослідженнях для аналізу таких даних застосовуються різні підходи. Зокрема, у роботі [1] розглядаються методи прогнозування чисельності популяцій на основі даних пасток, а у роботі [2] - методи виявлення різких змін моніторингових показників (change point detection), що можуть використовуватися для визначення початку активної фази розвитку популяції. Навіть за наявності таких методів задача своєчасного прийняття рішень щодо застосування засобів захисту рослин залишається складною, оскільки зміни у показниках пасток не завжди безпосередньо відповідають моменту найбільш ефективного втручання. Крім того, у багатьох роботах методи аналізу популяцій шкідників розглядаються за умов детального моніторингу із використанням значної кількості датчиків та обладнання.

У практичних польових умовах кількість джерел спостереження часто є обмеженою - зокрема, моніторинг зазвичай може здійснюватися лише однією пасткою на поле або невеликою їх кількістю на регіон.

У зв’язку з цим виникає задача інтерпретації даних моніторингу популяцій шкідників з урахуванням практичних обмежень їх отримання та використання для підтримки прийняття управлінських рішень. У даній роботі формулюються задачі та розглядаються підходи до аналізу моніторингових даних з метою розв’язання цих задач та використання відповідних технологій у системах підтримки прийняття рішень.

II. ДАНІ ТА МЕТОДИ

З використанням світлових пасток одержано дані у вигляді часових рядів кількості комах протягом сезону (1). Для частини спостережень також наявні експертні оцінки стану популяції, що можуть використовуватися під час аналізу.

$$X = x_1, x_2, \ldots, x_T \tag{1}$$

де x_t - кількість комах, зафіксована у пастці в момент часу t.

Під час інтерпретації таких даних необхідно враховувати особливості польових спостережень. Зміни чисельності комах у часових рядах можуть бути зумовлені як природною динамікою популяції, так і зовнішніми впливами, інформація про які не завжди представлена у даних.

Додатковим фактором невизначеності є вплив агротехнологічних операцій у межах стандартних схем вирощування культур: спостережувані зміни чисельності популяції можуть бути пов'язані як із розвитком популяції, так і з плановими заходами. Крім того, для польових даних характерною є неповнота інформації щодо умов проведення спостережень, а також наявність пропусків у часових рядах. Хоча для їх обробки можуть застосовуватися різні статистичні методи відновлення даних, використання таких методів не завжди гарантує коректність отриманих результатів. У зв'язку з цим під час подальшого аналізу доцільно враховувати як статистичні властивості часових рядів, так і практичні особливості організації польового моніторингу.

З огляду на зазначені обмеження важливим є уточнення практичних схем застосування засобів захисту рослин та їх впливу на моніторингові дані.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Попередній аналіз даних дозволяє сформулювати декілька задач, що можуть виникати під час використання моніторингових показників для підтримки прийняття рішень.

Визначення моменту, коли застосування інсектицидів є найбільш доцільним (2).

Занадто раннє втручання призводить до зайвих витрат, тоді як запізніле - до пошкодження посівів. За відсутності достатньої статистики щодо наслідків втручань експертні оцінки можуть використовуватися як основа для формування гіпотез та побудови моделей прийняття рішень.

З огляду на малий обсяг доступних даних та значну тривалість спостережень у часі одним із перспективних напрямів є використання методів, орієнтованих на роботу з малими вибірками, зокрема методу групового урахування аргументів (МГУА).

$$t^* = \arg\max_t f(x_{t-k}, \ldots, x_t) \tag{2}$$

де $f(\cdot)$ - функція оцінки стану популяції шкідників,
$x_{t-k}, \ldots, x_t$ - значення чисельності популяції у попередні моменти часу.

Прогноз розвитку популяції.

Іншою задачею є прогнозування подальшої динаміки чисельності популяції на основі попередніх значень показників (3).

$$\hat{x}_{t+\tau} = F(x_t, x_{t-1}, \ldots, x_{t-k}) \quad (3)$$

де $\hat{x}_{t+\tau}$ - прогнозована чисельність популяції у момент часу $t + \tau$,

$F(\cdot)$ - модель прогнозування.

Такий підхід може дозволити оцінювати можливість виникнення небезпечної ситуації за декілька днів до її настання. Для розв'язання цієї задачі також можуть застосовуватися методи, орієнтовані на роботу з малими вибірками, зокрема МГУА. Додатково точність прогнозування може бути підвищена шляхом врахування кореляційних залежностей між даними різних пасток, а також включення додаткових факторів, зокрема погодних умов.

ВИЗНАЧЕННЯ ДОСТАТНЬОЇ ЧАСТОТИ МОНІТОРИНГУ.

У практиці використання пасток важливим є визначення оптимальної частоти проведення вимірювань, оскільки надто частий моніторинг пов'язаний із додатковими витратами на обслуговування обладнання та обробку даних. У зв'язку з цим виникає задача визначення, чи може вибірка, отримана з меншою частотою спостережень (наприклад, один раз на декілька днів), замінити щоденні вимірювання без суттєвої втрати інформативності. Така задача може розглядатися як задача перевірки статистичних гіпотез щодо допустимості зменшення частоти спостережень без суттєвої втрати інформативності.

АНАЛІЗ ЧАСОВИХ ЗАЛЕЖНОСТЕЙ.

Припускається, що динаміка чисельності популяції у близьких точках спостереження має спільні тенденції. На користь такого припущення свідчать результати попереднього аналізу: без урахування часових зсувів коефіцієнти кореляції між часовими рядами пасток є близькими до одиниці, тоді як введення навіть невеликих лагів призводить до їх істотного зниження. Тому слід проаналізувати кореляційні залежності між значеннями часових рядів цих пасток за днями спостережень. Такий підхід може дозволити оцінити характерні часові лаги та визначити інтервал попередніх спостережень, що є найбільш інформативним для прогнозування подальшого розвитку популяції.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведений попередній аналіз показує, що використання даних автоматичного моніторингу популяцій шкідників пов'язане з рядом практичних обмежень та невизначеністю їх інтерпретації. У зв'язку з цим важливо розглядати не лише задачі прогнозування популяцій шкідників, але й задачі аналізу властивостей моніторингових даних та визначення умов їх ефективного використання для прийняття управлінських рішень.

Подальші дослідження можуть бути спрямовані на розробку методів аналізу часових рядів популяцій шкідників, оцінювання достатньої частоти моніторингових вимірювань та інтеграцію отриманих результатів у системи підтримки прийняття рішень у сільському господарстві. Зокрема, результати можуть бути використані у складі систем підтримки прийняття рішень для управління агроекосистемами, подібних до системи, описаної у роботі [3].

ЛІТЕРАТУРА

1. Kim, S., & Heo, S. Spatio-temporal time series forecasting with trap catch data of oriental fruit moth (Grapholita molesta) in peach (Prunus persica) orchards in South Korea. Frontiers in Plant Science, 2025, 16:1698144. Published 4 December 2025. https://doi.org/10.3389/fpls.2025.1698144.
2. Ma, H., Leibowicz, B. D., & Hasenbein, J. J. A Comparison of Change Point Detection Methods for Pest Outbreak Detection. Research Square. 2025, November 12. https://doi.org/10.21203/rs.3.rs-7908521/v1.
3. Гнатієнко В.Г., Снитюк В.Є. Концептуальні елементи технології розподіленого прогнозування врожайності сільськогосподарських культур. Прикладні інформаційні системи та технології в цифровому суспільстві: зб. тез доповідей і наук. повідомл. учасників VIII Міжнародної науково-практичної конференції (Київ, 01 жовтня 2024 р.) / за заг. ред. В. Плескач, Є. Зайцева, О. Фендьо. К.: Київський нац. ун-т ім. Тараса Шевченка, 2024. С. 75-82.
4. Neftissov, A., Biloshchytskyi, A., Andrashko, Y., Vatskel, V., Toxanov, S. & Gladka, M. (2024). Assessing the efficiency of using precision farming technology and remote monitoring of weather conditions in the activities of agricultural enterprises. Eastern-European Journal of Enterprise Technologies, 4(13 (130), 2024, 84–94. https://doi.org/10.15587/1729-4061.2024.309028
5. Лактіонов, І. С., Гнатушенко, В. В., Каштан, В. Ю., & Дяченко, Г. Г. (2025). Інтелектуальні інформаційні та комп'ютерні технології збору та аналізу даних агромоніторингу. Монографія. Фонд НТБ НТУ "Дніпровська політехніка".



ВЛАДИСЛАВ ГНАТІЄНКО
Аспірант, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0000-2678-5158
E-mail: hnatiienko.vladyslav@knu.ua
Отримав ступінь магістра комп'ютерних наук у Київському національному університеті імені Тараса Шевченка (Київ, Україна) у 2024 році. Нині є аспірантом кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка. Серед наукових інтересів - методи машинного навчання, зокрема глибинного навчання, та цифрова агрономія.



ВІТАЛІЙ СНИТЮК
Декан, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-9954-8767
E-mail: snytyuk@knu.ua.
Отримав кваліфікацію математика, викладача у Київському державному університеті ім. Т. Г. Шевченка (Київ, Україна) у 1991 році. Нині обіймає посаду декана факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Серед наукових інтересів - еволюційні обчислення та прийняття рішень в умовах невизначеності.

ІНТЕЛЕКТУАЛЬНИЙ МЕРЕЖЕВИЙ БЕЗДРОТОВИЙ СЕНСОРНИЙ ПРИСТРІЙ ВИЯВЛЕННЯ РУХУ ОБ'ЄКТІВ

Геннадій Дахно, Юрій Кравченко

Анотація. *У роботі представлено результати розробки та моделювання інтелектуального бездротового сенсорного пристрою для виявлення руху та аналізу поведінки об'єктів на основі SOC (System on chip) ESP32-S3 та багатозонного датчика часу прольоту (ToF). Дослідження охоплює створення пристрою, як елементу системи, що підтримує мультипротокольний зв'язок, включаючи підтримку Mesh-мереж та далекорангових протоколів Coded PHY та можливості інтелектуального розпізнавання траєкторій і поведінкових характеристик об'єктів, а також забезпеченню високої енергоефективності пристрою в режимі глибокого сну із циклами пробудження. Отримані результати підтверджують можливість використання пристрою у складних умовах експлуатації, зокрема на борту безпілотних апаратів та в системах промислової автоматизації.*

Ключові слова: IoT, ESP32-S3, ToF-датчик, Mesh-мережа, AI-аналіз, енергоефективність, бездротовий зв'язок.

I. ВСТУП

У сучасних умовах стрімкого розвитку Інтернету речей (IoT) та систем інтелектуального моніторингу виникає гостра потреба у високоефективних засобах виявлення руху, які здатні працювати автономно та забезпечувати високу точність у складних середовищах [1]. Особливої актуальності набувають пристрої виявлення руху, здатні працювати у складних умовах із високим рівнем завад та змінною топологією мережі.

Традиційні рішення, що базуються на пасивних інфрачервоних датчиках (PIR) або простих ультразвукових далекомірах, мають суттєві обмеження: вони не здатні відслідковувати траєкторію і характер руху об'єктів, мають низьку завадостійкість та обмежені можливості мережевої взаємодії. У зв'язку з цим доцільним є використання багатозонних датчиків часу прольоту (Time-of-Flight, ToF), які дозволяють формувати просторову карту середовища та мікроконтролери із підтримкою Edge AI для здійснення інтелектуальної обробки даних безпосередньо на борту пристрою.

Розробка, представлена у цій роботі, запроваджує інноваційне рішення – інтелектуальний сенсорний пристрій, що поєднує можливості багатозонного сканування простору за технологією Time-of-Flight (ToF) та сучасні протоколи бездротового зв'язку. Використання SOC ESP32-S3 [2] дозволяє не лише забезпечити передачу даних через Wi-Fi та Bluetooth LE, а й реалізувати Mesh-мережі та підтримку режимів Long Range [3]. Такий підхід забезпечує пристрою властивість функціональної стійкості, дозволяючи йому адаптуватися до змін топології мережі та працювати в умовах високої насиченості ефіру завдяки використанню різних протоколів і режимів роботи.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У ході реалізації проєкту було створено пристрій [4], що демонструє якісно новий рівень детектування об'єктів та мережевої гнучкості порівняно з існуючими аналогами.

1. Апаратна архітектура та сенсорна система (рис.1)**.** Основою пристрою є SOC ESP32-S3, який інтегрує потужне обчислювальне ядро, співпроцесор з наднизьким енергоспоживанням [5] та засоби бездротового зв'язку (рис.2)**.**

Для виявлення об'єктів використано багатозонний ToF-датчик VL53L8, який працює в оптичному діапазоні хвиль .

На відміну від класичних датчиків, VL53L8 дозволяє:

- здійснювати точне вимірювання відстані до об’єктів;
- проводити мультизонне сканування, що дає змогу будувати спрощену 3D-карту зони спостереження;
- визначати траєкторію переміщення об'єктів та характер руху в реальному часі.

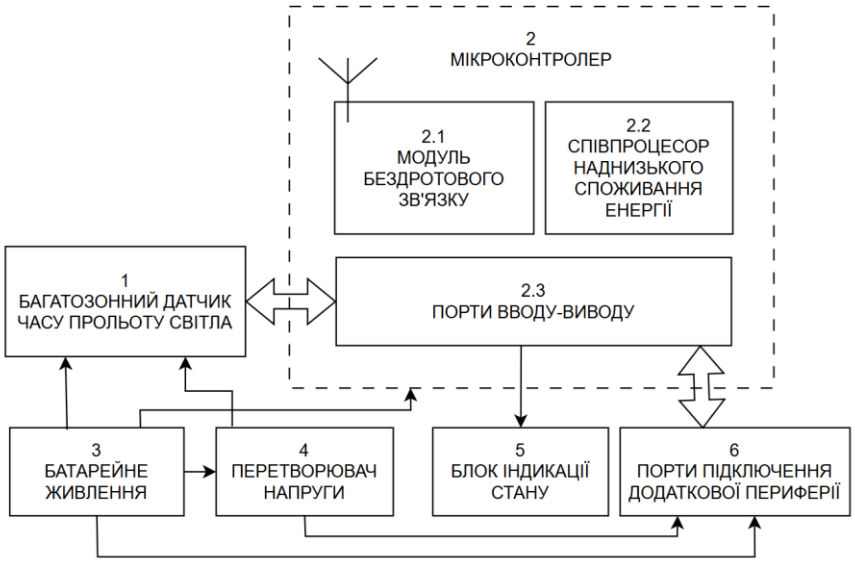


Рисунок 1. *Структурна схема пристрою*

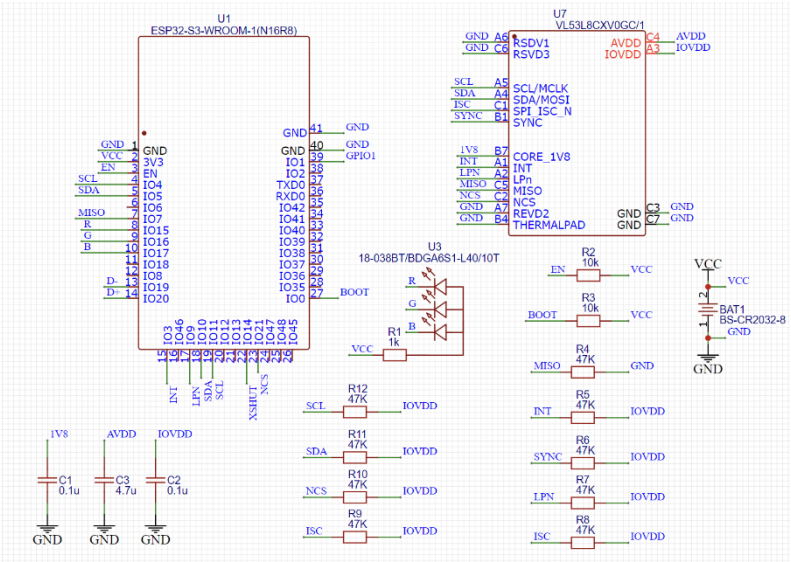


Рисунок 2. *Фрагмент принципової схеми*

Конструктивно пристрій виконаний у вигляді мініатюрної друкованої плати (розмір плати 20×36 мм) (рис. 3) і містить мікроконтролер, багатозонний датчик часу прольоту світла, блок батарейного живлення, перетворювачі напруги, уніфіковані порти для підключення додаткової периферії та блок індикації стану.

2. Мережеві можливості та функціональна стійкість Однією з ключових переваг розробленого пристрою є підтримка розширеного стеку протоколів бездротового зв’язку: Wi-Fi, Bluetooth, ESP-NOW, підтримка об’єднання в Mesh-мережі та режимів роботи: Long Range Coded PHY та багатозонний датчик часу прольоту світла, що працює в оптичному діапазоні хвиль.

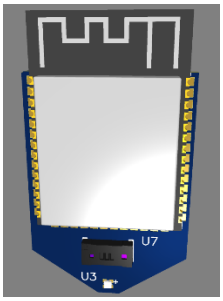


Рисунок 3. *3D модель пристрою*

Сучасні бездротові мережі для промислових та телеметричних рішень потребують інтеграції кількох протоколів передачі даних. Це необхідно для досягнення високої надійності, масштабованості та швидкодії системи в умовах великих площ і наявності фізичних перешкод. Комплексне використання спеціалізованих комунікаційних технологій дозволяє створити стійку інфраструктуру зв'язку, яка відповідає суворим технічним вимогам.

Одним із базових рішень для побудови таких систем є використання Mesh-мереж. Ця архітектура забезпечує децентралізовану самоорганізацію вузлів зв'язку, де кожен пристрій здатен маршрутизувати та ретранслювати дані від сусідніх елементів. Відсутність потреби в єдиному центральному вузлі керування підвищує загальну відмовостійкість системи та дає змогу ефективно покривати значні території зі складною просторовою топологією.

Для забезпечення стабільного зв'язку на великих відстанях застосовується технологія фізичного рівня Coded PHY Long Range. За рахунок використання алгоритмів кодування з виправленням помилок, вона здатна підтримувати надійну передачу даних на дистанції до одного кілометра. Ця характеристика є критичною вимогою при проєктуванні систем моніторингу для великих відкритих площ або розгорнутих промислових об'єктів.

У ситуаціях, де пріоритетом є мінімізація часу доставки інформації, застосовується протокол ESP-NOW. Він функціонує без необхідності попереднього встановлення стандартного бездротового з'єднання, що радикально знижує мережеву затримку. Такі технічні особливості роблять цей протокол оптимальним інструментом для швидкої та гарантованої передачі критичних системних повідомлень або сигналів про позаштатні ситуації.

Система підтримує автоматичне відновлення зв’язку та переконфігурацію мережі у разі виходу з ладу окремих вузлів, що гарантує високу надійність моніторингу.

У підсумку, спільне використання цих трьох технологій формує збалансовану та багатофункціональну систему бездротової комунікації. Mesh-архітектура відповідає за структурну гнучкість і площу покриття мережі, Coded PHY вирішує проблему дальності передачі сигналу, а ESP-NOW гарантує мінімальні затримки для найважливіших даних. Подібна інтеграція забезпечує стабільну роботу складних автоматизованих комплексів.

3. AI-аналіз та інтелектуальна обробка даних Інтеграція AI-алгоритмів безпосередньо на мікроконтролері ESP32-S3 дозволяє пристрою не просто фіксувати рух, а й здійснювати його якісний аналіз. Система здатна ідентифікувати "підозрілу поведінку", наприклад, тривале перебування об'єкта в забороненій зоні або нетиповий характер переміщення. Оброблена інформація передається у хмарне середовище, де вона може бути агрегована з даними інших датчиків для остаточної верифікації засобами штучного інтелекту вищого рівня.

4. Енергоефективність Завдяки наявності співпроцесора наднизького споживання, пристрій демонструє виняткову автономність. У режимі глибокого сну (Deep-sleep) споживання енергії дуже низьке. Цикл роботи побудований таким чином, що після обробки та передачі інформації система повертається до режиму енергозбереження до наступної події або спрацювання системного таймера.

III. ВИСНОВКИ

Розробка інтелектуального мережевого бездротового сенсорного пристрою виявлення руху є значним кроком у створенні адаптивних систем безпеки нового покоління. Використання технології ToF у поєднанні з багатозонним скануванням та AI-аналізом дозволяє досягти високої точності детектування, виключаючи обмеження традиційних інфрачервоних датчиків.

Впровадження Mesh-мереж та протоколів великої дальності забезпечує масштабованість системи та її функціональну стійкість у динамічних середовищах, включаючи можливість розміщення сенсорів на борту безпілотних апаратів. Запропоноване рішення є універсальним інструментом, що відповідає сучасним вимогам до надійності, компактності та автономності, і може стати основою для інноваційних проєктів у сферах "розумного" дому, промислової автоматизації та охорони об'єктів.

ДЖЕРЕЛА

1. Дахно Г.В., Щитов А.Ю. Ефективні протоколи та інтерфейси для передачі відео та аудіоданих у мережах IOT. НТКМУ «Актуальні проблеми інформаційних технологій 2024» (APIT - 2024), м. Київ 25 жовтня 2024, С. 51 – 53.
2. ESP32-S3 Designed for AIoT applications. URL: https://www.espressif.com/en/products/socs/esp32-s3
3. Дахно Г.В., Гаврилюк Д.В. Використання засобів дальнього доступу для зв’язку між вузлами сенсорної мережі. НТКМУ «Актуальні проблеми інформаційних технологій 2025» (APIT - 2025), м. Київ 23 жовтня 2025, С. 74 – 75.
4. Реєстраційний номер заявки u 2025 05538 дата 18.11.2025 Снитюк В.Є., Кравченко Ю.В., Дахно Г.В., Бедюх О.Р., Дахно Н.Б. Лаптєв О.А., Собчук В.В., Гнатієнко Г.М., Лещенко О.О., Ставицький С.Д., назва Інтелектуальний мережевий бездротовий сенсорний пристрій виявлення руху об'єктів. https://sis.nipo.gov.ua/uk/search/detail/1885501/
5. Дахно Г.В., Адамчук Я.А. Підвищення енергоефективності у мобільних сенсорних мережах за допомогою інтелектуальних алгоритмів кластеризації. НТКМУ «Актуальні проблеми інформаційних технологій 2024» (APIT - 2025), м. Київ 23 жовтня 2025, С. 38 – 39.



ГЕННАДІЙ ДАХНО
Аспірант ІІ року навчання кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0004-8145-051X
E-mail: hennadii.dakhno@knu.ua
Наукові інтереси: розробка програмного забезпечення для інформаційних систем, портали, інтернет-архіви, діяльність фінансових установ, проєктування обладнання, IoT, штучний інтелект



ЮРІЙ КРАВЧЕНКО
Доктор технічних наук, професор, завідувач кафедри мережевих та інтернет технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0002-0281-4396
E-mail: yurii.kravchenko@knu.ua
Сфера наукових інтересів: телекомунікаційні системи, функціональна стійкість складних систем, штучний інтелект

IOT-СИСТЕМА МОНІТОРИНГУ ЕМОЦІЙНОГО СТАНУ ТА КОМФОРТУ ВІДВІДУВАЧІВ У ВЕЛИКИХ ГРОМАДСЬКИХ ПРОСТОРАХ

Денис Д'яченко, Мирослава Гладка

Анотація. *Розробка IoT-системи моніторингу емоційного стану відвідувачів спрямована на підвищення безпеки та комфорту у великих громадських просторах. Система використовує мережу мікрокомп'ютерів та оптичних сенсорів для збору даних про динаміку рухів натовпу і рівень шуму. Завдяки побудові просторових скелетних моделей аналіз відбувається локально, без розпізнавання облич, що гарантує збереження приватності. Зібрані метадані передаються на сервер, де обробляються алгоритмами машинного навчання та візуалізуються на дашборді оператора. Впровадження такої архітектури дозволяє превентивно виявляти ризики паніки чи агресії, уникати тисняви та оперативно керувати ситуацією.*

Ключові слова: IoT, моніторинг натовпу, машинне навчання, просторові скелетні моделі, граничні обчислення, безпека громадських просторів, приватність**.**

I. ВСТУП

Великі громадські простори, такі як торговельно-розважальні центри, аеропорти та вокзали, потребують постійного контролю за безпекою та комфортом величезних потоків людей. Звичайних систем відеоспостереження для цього вже недостатньо, оскільки вони фіксують інциденти постфактум, тому впровадження IoT-рішень дозволяє в реальному часі отримувати дані про загальний емоційний стан та поведінку натовпу [4]. Це дає змогу не лише відстежувати поточну ситуацію, а й превентивно виявляти зростання напруги, ризики паніки чи агресії.

Для вирішення цієї проблеми розглянемо концепцію IoT-системи моніторингу емоційного стану відвідувачів. Вона базується на використанні мережі компактних мікрокомп'ютерів та оптичних сенсорів. Локальна обробка даних за допомогою алгоритмів машинного навчання дозволяє швидко аналізувати динаміку рухів людей без ідентифікації осіб та порушення їхньої приватності [1]. Система моніторингу збирає дані і відображає їх у зручному для людини вигляді – дашборді, що дає змогу адміністрації оперативно реагувати на зміни настрою натовпу, уникати тисняви та загалом підвищувати рівень клієнтського сервісу.

II. ДАНІ ТА МЕТОДИ

Для побудови системи моніторингу використовується мережа компактних IoT-пристроїв, де базовими елементами збору даних виступають оптичні камери та сенсори звуку. Оскільки в публічних просторах гостро стоїть питання приватності, у системі не застосовується класичне розпізнавання облич. Натомість аналіз базується на побудові просторових скелетних моделей та відстеженні загальної динаміки рухів натовпу [2]. Це дає змогу фіксувати різкі зміни в поведінці (ознаки паніки, конфліктів чи зростання дискомфорту), працюючи виключно з анонімізованими даними.

Щоб не перевантажувати мережу постійною передачею відеопотоку, архітектура рішення побудована на концепції граничних обчислень (Edge Computing) [3]. Первинна обробка інформації відбувається безпосередньо на місці встановлення камер за допомогою мікрокомп'ютерів (наприклад, Raspberry Pi). Їхнє головне завдання — відкинути відеоряд, виділивши лише координати рухів (скелетизація) та базові рівні шуму [2].

Отримані легкі метадані через протокол MQTT передаються на центральний сервер. На серверному рівні відбувається збереження інформації у базу даних (БД) для подальшого

історичного аналізу, а також працюють основні моделі машинного навчання. Вони агрегують потоки даних з різних зон об'єкта, аналізують їх з урахуванням історичних патернів та класифікують поточний емоційний стан натовпу у режимі реального часу [1]. Загальну багаторівневу архітектуру обробки даних наведено на Рисунку 1.

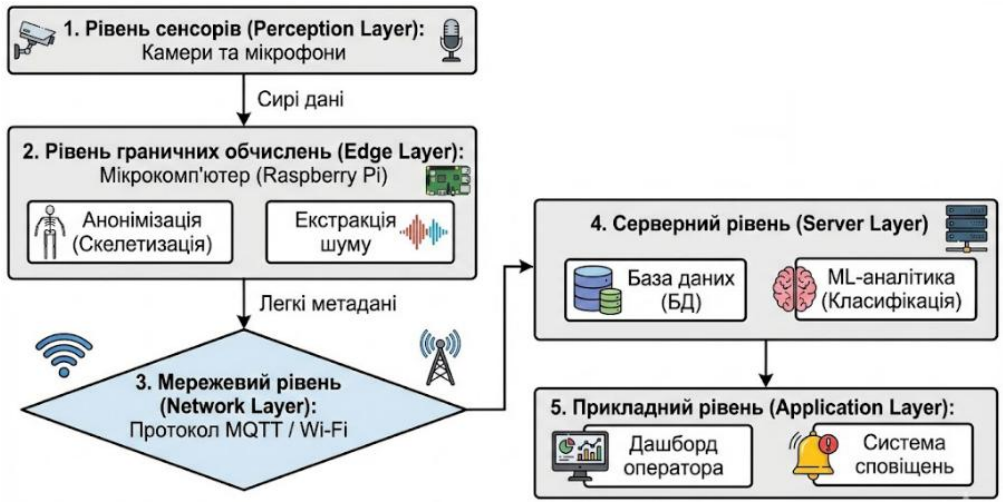


Рисунок 1. *Архітектура IoT-системи моніторингу емоційного стану відвідувачів*

Як можемо бачити на схемі, процес обробки даних проходить через п'ять послідовних логічних рівнів. На рівні сенсорів (Perception Layer) відбувається безперервний збір сирих аудіо- та відеоданих. Далі, на рівні граничних обчислень (Edge Layer), мікрокомп'ютери миттєво перетворюють ці дані на анонімні метадані: координати рухів та рівень гучності [3]. Це дозволяє суттєво розвантажити мережевий рівень (Network Layer), який відповідає за швидку та стабільну передачу інформації на сервер через протоколи MQTT або Wi-Fi. Серверний рівень (Server Layer) виконує ключову аналітичну функцію: тут алгоритми машинного навчання класифікують отримані параметри, спираючись на історичні дані з БД, і визначають поточний емоційний фон натовпу [1]. Фінальним етапом є прикладний рівень (Application Layer), де оброблені результати та автоматичні сповіщення про можливі ризики виводяться на дашборд служби безпеки для оперативного прийняття рішень.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз запропонованої архітектури показує, що вона дозволяє обійти одну з головних проблем сучасного відеоспостереження у громадських місцях – порушення приватності відвідувачів. Оскільки система використовує побудову скелетних моделей замість класичного розпізнавання облич [2], її можна розгортати без складних юридичних погоджень щодо збору біометричних даних.

Крім етичного аспекту, такий підхід вирішує проблему навантаження на інфраструктуру. Перенесення первинної обробки на мікрокомп'ютери (рівень Edge) означає, що нам не потрібно передавати важкі відеопотоки на центральний сервер [1]. Туди відправляються лише легкі текстові метадані та координати, що робить систему стійкою до перебоїв у мережі і дозволяє аналізувати ситуацію практично без затримок у часі.

На практиці ж це дає змогу перетворити пасивне відеоспостереження на активний аналітичний інструмент [4]. Замість того, щоб оператор фізично намагався встежити за десятками екранів, алгоритм самостійно аналізує динаміку натовпу та рівень шуму. Якщо в певній зоні фіксуються різкі нетипові рухи або зростає напруга, система автоматично виводить попередження в дашборді. Накопичені історичні дані також дозволяють

адміністрації аналізувати загальний рівень комфорту в різні години та оптимізувати простір так, щоб уникати утворення тисняви.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована архітектура демонструє, що використання сучасних IoT-рішень здатне якісно змінити підхід до управління великими громадськими просторами. Головною перевагою нашої системи є вирішення проблеми приватності. Оскільки камери не ідентифікують обличчя, а працюють лише зі знеособленими просторовими моделями, таку розробку можна впроваджувати без порушення етичних норм та жорсткого законодавства про захист персональних даних. Крім того, перенесення частини обчислень на периферійні пристрої суттєво знижує навантаження на локальну мережу об'єкта.

Звичайно, на етапі практичного розгортання можуть виникнути певні технічні виклики. Наприклад, необхідність додаткового калібрування оптичних сенсорів в умовах змінного або недостатнього освітлення, а також оптимізація алгоритмів машинного навчання для роботи з дуже щільним натовпом. Також перспективним напрямом для подальших досліджень є інтеграція нашої аналітики з існуючими системами пожежної безпеки та контролю доступу.

Підсумовуючи, можна сказати, що впровадження описаної IoT-системи дозволяє перетворити класичне пасивне відеоспостереження на проактивний інструмент. Адміністрація торговельних центрів чи аеропортів отримує можливість не просто фіксувати інциденти постфактум, а працювати на випередження. Своєчасне виявлення зростання напруги або дискомфорту допомагає запобігати паніці, уникати тисняви та загалом робити публічні простори значно безпечнішими для людей.

ДЖЕРЕЛА

1. Sungwook Yoon., B. Kim. (2025) Multi-Scale Temporal Fusion Network for Real-Time Multimodal Emotion Recognition in IoT Environments.
2. Haifeng Lu., Jiuyi Chen., Zhen Zhang., Ruida Liu., Runhao Zeng., Xiping Hu. (2025) Emotion Recognition from Skeleton Data: A Comprehensive Survey.
3. Feng Xiao, Ze Xu, Yi Han, Yi Zhong, Yi Zheng, Mingxi Liao (2024) Machine Learning Based Driver Emotion Monitoring for Vehicular IoT
4. Rosa Adriana García Hernández. (2024) A Systematic Literature Review of Modalities, Trends, and Limitations in Emotion Recognition, Affective Computing, and Sentiment Analysis.



ДЕНИС Д'ЯЧЕНКО
студент 1-го курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: denis.diachenko.2000@knu.ua
Студент Київського національного університету імені Тараса Шевченка.
Наукові інтереси – розробка та проєктування систем Інтернету речей (IoT), моделювання інформаційних систем та впровадження технологій машинного навчання.



МИРОСЛАВА ГЛАДКА
к.т.н., доц., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-5233-2021
E-mail: myroslava.gladka@knu.ua
Фахівець в галузі інформаційних систем та технологій. Практичний досвід впроваджень інформаційних систем понад 10 років. Досвід викладання в університетах України понад 20 років.
Наукові інтереси – управління проєктами, моделювання та інжиніринг бізнес-процесів.

УДОСКОНАЛЕННЯ СИСТЕМ РЕГУЛЯЦІЇ ДЛЯ УПРАВЛІННЯ IOT ПРИСТРОЯМИ НА БАЗІ МІКРОКОНТРОЛЕРІВ

Олександр Жеребцов, Анатолій Переверзєв

Анотація. *У роботі запропоновано архітектуру адаптивного інтелектуального регулятора для IoT-пристроїв. Розроблена система поєднує класичне ПІД-регулювання з методами нечіткої логіки та технологіями TinyML для компенсації мережевих затримок і втрат пакетів. Реалізацію виконано на базі мікроконтролера ESP32 під керуванням FreeRTOS. Експериментальні дослідження підтвердили підвищення якості регулювання та енергоефективності порівняно з класичними алгоритмами в умовах нестабільного мережевого з'єднання.*

Ключові слова: IoT, ПІД-регулятор, TinyML, Fuzzy Logic, ESP32.

I. ВСТУП

Сучасний розвиток концепцій Індустрії 4.0 та Інтернету речей (IoT) характеризується масовою інтеграцією кіберфізичних систем, де керування технологічними процесами відбувається через розподілені бездротові мережі. Така архітектура висуває жорсткі вимоги до надійності та швидкодії контурів регулювання, які часто реалізуються на базі мікроконтролерів з обмеженими обчислювальними ресурсами та енергоспоживанням [1]. Проблема полягає у необхідності забезпечення детермінованої поведінки системи керування в умовах недетермінованого середовища передачі даних, що є критичним для задач автоматизації реального часу[2].

Традиційні алгоритми пропорційно-інтегрально-диференціального (ПІД) регулювання, які домінують у промисловості завдяки своїй простоті, суттєво втрачають ефективність при роботі в IoT-мережах [3]. Основними дестабілізуючими факторами виступають змінні транспортні затримки (джиттер), втрати пакетів даних та асинхронність вимірювань. Порушення сталості періоду дискретизації призводить до помилок в обчисленні інтегральної та диференціальної складових регулятора, що викликає значне перерегулювання або навіть втрату стійкості замкненої системи. Це зумовлює необхідність переходу від класичних підходів до адаптивних стратегій, здатних динамічно компенсувати нестабільність каналу зв'язку [4]. Метою роботи є підвищення якості та надійності керування IoT-пристроїв шляхом розробки архітектури інтелектуального регулятора, що поєднує методи обчислень на межі мережі (Edge AI) та апарат нечіткої логіки (Fuzzy Logic). Запропонований підхід передбачає перенесення алгоритмів адаптації безпосередньо на мікроконтролер (на прикладі ESP32) [5], що дозволяє мінімізувати залежність від хмарних обчислень та забезпечити автономну стабілізацію технологічних параметрів навіть в умовах значних мережевих збурень [6].

II. ДАНІ ТА МЕТОДИ

Для досягнення поставленої мети розроблено архітектуру контролера Fuzzy-PID (рис. 1), яка має трирівневу структуру:

1. Рівень фізичного керування: реалізує швидкий класичний ПІД-алгоритм на перериваннях.
2. Рівень адаптації: використовує бібліотеку eFLL (Embedded Fuzzy Logic Library) та моделі TinyML (TensorFlow Lite Micro) для динамічного коригування коефіцієнтів K_p, K_i, K_d.
3. Рівень компенсації мережі: містить буфер джиттеру та предиктор вимірювань для стабілізації періоду дискретизації.

Програмна реалізація виконана на мікроконтролері ESP32 з використанням операційної системи реального часу FreeRTOS, що забезпечує детермінованість виконання задач керування. Для експериментальної перевірки використано лабораторний стенд TCLab (Temperature Control Lab) [7], який моделює інерційний тепловий об'єкт із транспортним запізненням. Методика досліджень включала порівняння класичного ПІД та розробленого Fuzzy-PID регулятора за критерієм інтегральної абсолютної помилки (IAE) в ідеальних умовах та при емуляції мережевих затримок (до 500 мс) і втрат пакетів (до 10%) [8].

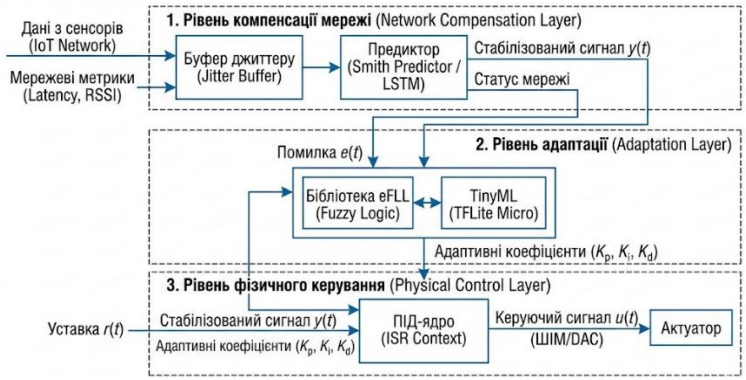


Рисунок 1. *Архітектура адаптивного інтелектуального контролера*

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Для емуляції реальних умов експлуатації в бездротовій мережі було створено програмний стенд, здатний вносити випадкові затримки (jitter) у діапазоні 50–500 мс та моделювати втрати пакетів даних із ймовірністю від 5% до 20%. Порівняння ефективності здійснювалося між класичним цифровим ПІД-регулятором [9] та розробленим адаптивним нейро-нечітким (Fuzzy-PID) контролером. (Таблиця 1).

Таблиця 1. *Порівняння ефективності регуляторів*

Тип регулятора	Умови мережі	Перерегулювання (%)	Час встановлення (с)	IAE
Класичний ПІД	Ідеальна	18 %	120	1540
Fuzzy-PID	Ідеальна	6 %	95	1210
Класичний ПІД	Затримки + втрати	35 % (осциляції)	>200	3800
Fuzzy-PID	Затримки + втрати	12 %	140	1950

Кількісний аналіз за критерієм інтегральної абсолютної помилки (IAE) підтвердив перевагу розробленого методу. В умовах стабільної мережі значення IAE для класичного ПІД склало 1540, а для адаптивного — 1210. В умовах нестабільного зв'язку помилка класичного регулятора зросла у 2,5 рази (до 3800), тоді як адаптивний регулятор продемонстрував зростання лише на 60% (до 1950). Це доводить, що інтеграція механізмів Edge AI безпосередньо у прошивку мікроконтролера дозволяє ефективно нівелювати негативний вплив стохастичної природи бездротових мереж.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі вирішено актуальну задачу підвищення надійності керування IoT-пристроями в умовах невизначеності каналів зв'язку. Головним науковим результатом є вдосконалена архітектура регулятора, яка, на відміну від існуючих хмарних рішень, виконує обчислення корегуючих впливів безпосередньо на кінцевому пристрої (Edge Computing). Це дозволяє системі залишатися функціональною навіть при тимчасовій втраті з'єднання з сервером, що

критично важливо для промислових застосувань. Результати тестування підтвердили, що використання нечіткої логіки для динамічного налаштування коефіцієнтів ПІД-регулятора є більш енергоефективним підходом, ніж використання складних нейромережевих моделей, які вимагають значних обчислювальних потужностей. Запропонований алгоритм займає менше 10% ресурсів процесора ESP32, залишаючи достатньо продуктивності для підтримки стека протоколів Wi-Fi/Bluetooth та шифрування даних. Практична цінність роботи полягає у створенні універсальної бібліотеки для мікроконтролерів сімейства ESP, яку можна використовувати при розробці розумних термостатів, систем вентиляції та іншого обладнання. Подальші дослідження доцільно зосередити на впровадженні методів навчання з підкріпленням (Reinforcement Learning), що дозволить регулятору самостійно адаптуватися до змін параметрів об'єкта керування в процесі тривалої експлуатації без участі оператора.

ДЖЕРЕЛА

1. Veneri, G. and Capasso, A. (2022) Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0. 2nd ed. Birmingham: Packt Publishing.
2. Åström, K.J. and Murray, R.M. (2021) Feedback Systems: An Introduction for Scientists and Engineers. 2nd edn. Princeton: Princeton University Press.
3. Zhou, Y. (2022) 'A Summary of PID Control Algorithms Based on AI-Enabled Embedded Systems', Security and Communication Networks, 2022, Article ID 7156713. Available at: https://doi.org/10.1155/2022/7156713
4. Liu, J., Tan, B. and Mu, X. (2026) 'Optimal Control for Networked Control Systems with Stochastic Transmission Delay and Packet Dropouts', Electronics, 15(1), p. 180. Available at: https://doi.org/10.3390/electronics15010180
5. Kurniawan, A. (2021) Internet of Things Projects with ESP32: Build exciting and powerful IoT projects using the ESP32 SoC. Birmingham: Packt Publishing
6. Жеребцов, О.А., Закатов, О.Д. та Василенко, Є.В. (2025) 'Розробка програми керування апаратурою управління шахтним конвеєром', у Матеріали IX-ої Міжнародної науково-практичної конференції «Сучасні технології промислового комплексу – 2025». Херсон, Україна, 17–19 вересня. Херсон: ХНТУ, с. 60–64.
7. Hedengren, J. D. (no date) Temperature Control Lab. Available at: http://apmonitor.com/pdc/index.php/Main/ArduinoTemperatureControl.
8. Hägglund, T. and Guzman, J.L. (2024) 'Give us PID controllers and we can control the world', IFAC-PapersOnLine, 58(15), pp. 288–293.
9. Dorf, R.C. and Bishop, R.H. (2022) Modern Control Systems. 14th edn. Harlow: Pearson.



ОЛЕКСАНДР ЖЕРЕБЦОВ
Викладач, циклова комісія з інформаційних технологій, Фаховий коледж економіки та інформаційних технологій ЗІЕІТ», Запоріжжя, Україна
ORCID: 0000-0001-6076-2005
E-mail: a.zherebtsov@econom.zp.ua
Викладач інформаційних дисциплін для здобувачів освіти у галузі інформаційних технологій. Досвід науково-педагогічної роботи 20 років. Має більше 60 наукових та навчально-методичних праць у галузі ІТ та матеріалознавства. Н-індех у Scopus – 7.



АНАТОЛІЙ ПЕРЕВЕРЗЄВ
д.т.н., професор, проректор з наукової роботи, професор кафедри інформаційних технологій, Запорізький інститут економіки та інформаційних технологій, Запоріжжя, Україна
E-mail: a.pereverzev@econom.zp.ua
Академік академії Вищої школи України, академік Міжнародної кадрової академії. Має стаж науково-педагогічної роботи понад 50 років. Спеціаліст в галузі електронних систем, напівпровідникової техніки та інформаційних технологій.

IOT-СИСТЕМА ВИЯВЛЕННЯ ШАХРАЙСТВА У БАНКІВСЬКИХ ПЛАТЕЖАХ

Артем Колесник, Віталій Михальчук, Ірина Борисенко

Анотація. *Об'єктом дослідження є автоматизоване виявлення шахрайських транзакцій у банківських платіжних системах за допомогою технологій IoT та машинного навчання. В умовах стрімкого зростання фінансових кіберзагроз запропоновано гібридний апаратно-програмний комплекс. Його апаратна частина на базі Raspberry Pi (з датчиком вібрації, кнопками та індикаторами) забезпечує фізичний моніторинг терміналу. Серверна складова використовує ансамблевий ML-класифікатор (Random Forest, SVM, XGBoost, Isolation Forest). Їхня взаємодія дозволяє в режимі реального часу аналізувати транзакції, оцінювати ризики та фіксувати фізичні втручання з подальшим відображенням результатів на веб-панелях адміністратора та клієнта.*

Ключові слова: виявлення шахрайства, Інтернет речей, Raspberry Pi, машинне навчання, банківські платежі, ансамблеві методи, оцінка ризику.

I. ВСТУП

Стрімке зростання обсягів безготівкових розрахунків та масове впровадження цифрових платіжних сервісів суттєво збільшують ризики фінансового шахрайства. За даними Європейського центрального банку, щорічні збитки від карткового шахрайства в Європі перевищують 1,5 млрд євро, і ця цифра продовжує зростати. Традиційні методи виявлення аномалій на основі статичних правил не здатні своєчасно адаптуватися до нових схем атак, що зумовлює необхідність впровадження інтелектуальних систем захисту реального часу.

Аналіз існуючих рішень свідчить про активний розвиток комерційних систем на основі машинного навчання, зокрема IBM Safer Payments, Featurespace ARIC та Mastercard Decision Intelligence. Проте вони є закритими продуктами з обмеженою гнучкістю інтеграції та не враховують фізичний стан самого платіжного обладнання. Водночас технології Інтернету речей відкривають принципово новий рівень захисту: підключені пристрої здатні фіксувати не лише транзакційні дані, а й фізичні аномалії терміналу - вібрацію, несанкціоноване втручання в корпус, характерні для скімінг-атак та підміни обладнання.

Об'єктом дослідження є процес виявлення шахрайських платежів в IoT-середовищі. Метою роботи є розробка та реалізація системи, що поєднує апаратний IoT-модуль збору даних на базі Raspberry Pi із серверним ансамблевим ML-класифікатором для захисту банківських транзакцій у реальному часі.

II. ДАНІ ТА МЕТОДИ

Апаратний модуль системи побудований на базі мікрокомп'ютера Raspberry Pi, який виконує функцію IoT-вузла платіжного терміналу. До мікрокомп'ютера підключено такі компоненти через GPIO-інтерфейс:

– Датчик вібрації - фіксує механічні аномалії корпусу терміналу, характерні для встановлення скімінг-обладнання або фізичного втручання зловмисника. При перевищенні порогового значення вібрації автоматично формується тривожний сигнал і блокується проведення транзакцій.

– Баззер (зумер) - звуковий індикатор, що спрацьовує при виявленні підозрілої транзакції або при реєстрації фізичної аномалії пристрою.

– Дві кнопки - перша слугує для підтвердження транзакції оператором, друга - для екстреного блокування терміналу при виявленні загрози.

– Два світлодіоди - зелений індикує успішно підтверджену легітимну транзакцію, червоний сигналізує про виявлене шахрайство або стан тривоги пристрою.

Raspberry Pi зчитує стан датчика вібрації та кнопок у реальному часі, керує світлодіодами і баззером відповідно до отриманих рішень класифікатора, а також передає зібрані дані на Flask-сервер через локальну мережу за протоколом HTTP/REST.

Архітектура системи є трирівневою та включає рівень збору даних (Raspberry Pi з сенсорами), рівень обробки (серверний застосунок) та рівень представлення (веб-панелі моніторингу). Серверна частина реалізована на Python з використанням мікрофреймворку Flask, дані зберігаються у базі PostgreSQL, система контейнеризована засобами Docker.

Для класифікації транзакцій застосовано ансамблевий підхід, що поєднує чотири незалежні моделі машинного навчання:

– Random Forest (RF) - ансамблева класифікація на основі дерев рішень.

– Support Vector Machine (SVM) - лінійна та нелінійна сепарація класів у просторі ознак.

– XGBoost (Gradient Boosting) - послідовне нарощування моделей з корекцією помилок.

– Isolation Forest - виявлення аномалій методом ізоляції викидів без учителя.

Фінальна оцінка ризику транзакції формується як зважене середнє прогнозів усіх чотирьох моделей. Ознаки класифікації включають: суму транзакції, IP-адресу пристрою, часову мітку, категорію мерчанта, частоту транзакцій користувача та дані датчика вібрації з Raspberry Pi. Нижче на рисунку 1 представлено послідовність роботи системи.

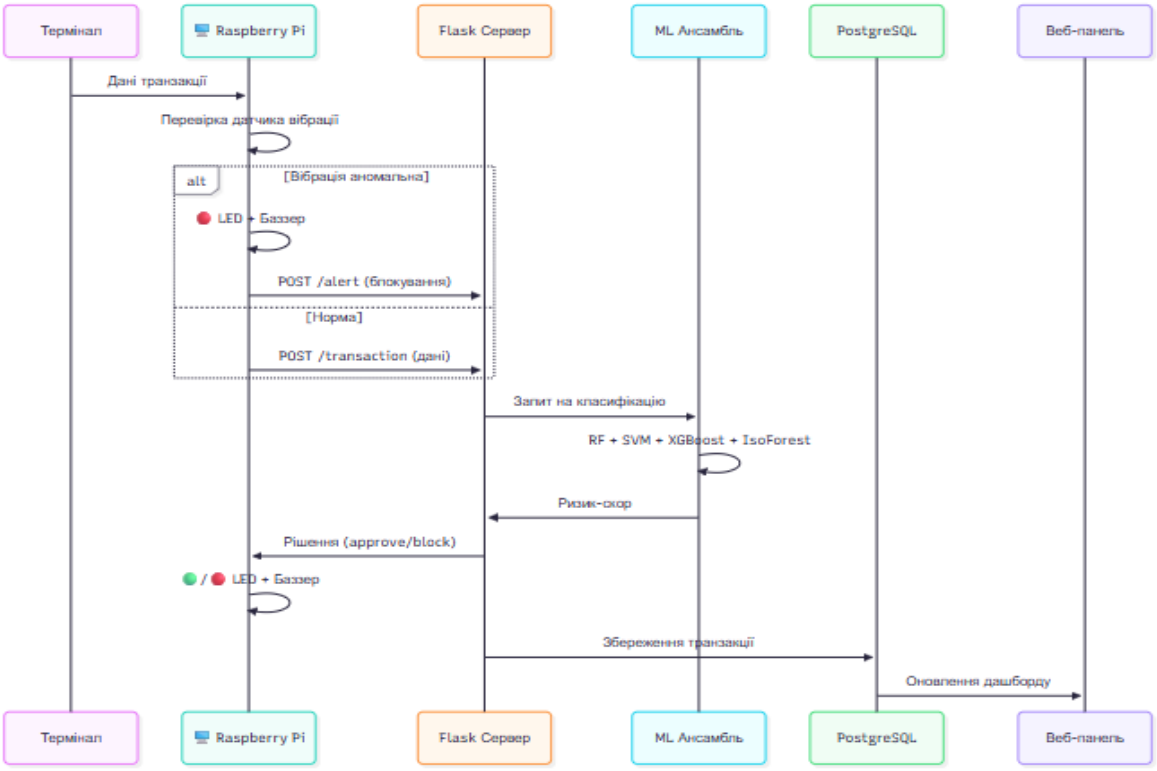


Рисунок 1. *Діаграма послідовності роботи IoT-системи виявлення шахрайства*

Веб-панель моніторингу є повноцінним елементом IoT-системи. Адміністраторська панель відображає стан підключених пристроїв у реальному часі (онлайн/офлайн), журнал тривог від датчика вібрації, зведену статистику транзакцій та дозволяє дистанційно блокувати термінали. Клієнтська панель надає персональну аналітику: оцінка ризику останньої транзакції з деталізацією по кожній ML-моделі, графік активності за 30 днів та налаштування лімітів безпеки.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Розроблений апаратний прототип на базі Raspberry Pi 3 Model B+ успішно виконує всі покладені функції фізичного моніторингу банківського терміналу. Датчик вібрації SW-420 стабільно реєструє механічні втручання в корпус пристрою з чутливістю достатньою для виявлення спроб встановлення скімерів або несанкціонованого доступу до внутрішніх компонентів. Затримка між фізичним сигналом (вібрація або натиснення кнопки) та реакцією системи (спрацювання базера, зміна стану світлодіода) становить менше п'ятдесяти мілісекунд завдяки використанню апаратних переривань GPIO замість постійного опитування стану датчиків. Heartbeat-механізм забезпечує виявлення відключених або скомпрометованих пристроїв з максимальною затримкою тридцять п'ять секунд.

Ансамблевий ML-класифікатор демонструє високу точність виявлення шахрайських транзакцій на тестовій вибірці: AUROC дорівнює 0.94, AUPRC становить 0.89, що значно перевищує результати окремих моделей. Найвищу точність показав XGBoost (AUROC 0.92), Random Forest забезпечив найкращу інтерпретованість через feature importance аналіз, Isolation Forest успішно виявляв аномальні паттерни невідомі supervised моделям.

Серверна частина системи забезпечує одночасну обробку запитів від кількох IoT-пристроїв завдяки контейнеризованій архітектурі на Docker та асинхронній обробці heartbeat-сигналів що надходять кожні п'ять секунд від кожного терміналу. Система успішно обробляє навантаження до п'ятисот транзакцій на годину з одного backend-екземпляру при споживанні оперативної пам'яті не більше одного гігабайта. Адміністратор отримує повну картину безпеки системи: деталізований аналіз по кожній з чотирьох ML-моделей з індивідуальними скорами, поточний стан GPIO-інтерфейсів Raspberry Pi включаючи лічильники вібрацій, журнал IoT-подій з фільтрацією за типом та серйозністю, та SMS-сповіщення про критичні тривоги через Twilio API з латентністю менше трьох секунд.

Інтеграція IoT-підсистеми з ML-аналізом підтвердила ефективність гібридного підходу: транзакції з активованим датчиком тампер-атаки отримували на двадцять п'ять відсотків вищий ризик-скор порівняно з ідентичними транзакціями без фізичної загрози, що демонструє успішне врахування апаратного контексту у прийнятті рішень програмною підсистемою.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Було проведено SWOT-аналіз розробленої системи:

Сильні сторони:

– Двошарова система захисту: фізичний IoT-моніторинг + ML-класифікація транзакцій.

– Обробка рішень у реальному часі (< 200 мс).

– Прозорість - деталізація по кожній моделі для цілей аудиту та пояснюваності.

– Масштабована контейнеризована архітектура на Docker.

Слабкі сторони:

– Навчання на синтетичних даних потребує верифікації на реальних транзакційних датасетах.

– Залежність від стабільного мережевого з'єднання між Raspberry Pi та сервером.

– Початкові витрати на розгортання апаратної інфраструктури.

Можливості:

– Інтеграція з реальними платіжними шлюзами (Visa, Mastercard API).

– Розширення переліку датчиків: NFC-сканер, камера для розпізнавання скімерів.

– Адаптація для банкоматів та POS-терміналів різних виробників.

Загрози:

– Дрейф даних - зміна патернів шахрайства з часом вимагає регулярного перенавчання моделей.

– Вимоги GDPR та НБУ щодо обробки і зберігання фінансових персональних даних.
– Можливість цілеспрямованого обходження ML-класифікаторів (adversarial attacks).

У роботі розроблено та реалізовано IoT-систему виявлення шахрайства у банківських платежах, що поєднує апаратний модуль на базі Raspberry Pi (датчик вібрації, баззер, кнопки, світлодіоди) із серверним ансамблевим класифікатором на основі Random Forest, SVM, XGBoost та Isolation Forest. Запропонована архітектура забезпечує двошаровий захист платіжного терміналу на фізичному рівні через IoT-сенсори та на програмному рівні через ML-аналіз транзакцій з часом відповіді менше 200 мс. Подальші дослідження передбачають інтеграцію з реальними транзакційними потоками та впровадження механізмів онлайн-навчання для адаптації до нових схем шахрайства.

ДЖЕРЕЛА

1. European Central Bank. Seventh report on card fraud. URL: https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf
2. IBM Safer Payments. URL: https://www.ibm.com/products/safer-payments
3. Featurespace ARIC Platform. URL: https://www.featurespace.com
4. Breiman L. Random Forests // Machine Learning. — 2001. — T. 45. — C. 5–32
5. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System // KDD. — 2016
6. Liu F. T. та ін. Isolation Forest // ICDM. — 2008
7. Raspberry Pi Foundation. URL: https://www.raspberrypi.org
8. RPi.GPIO Python library. URL: https://pypi.org/project/RPi.GPIO
9. Flask framework. URL: https://flask.palletsprojects.com
10. PostgreSQL database. URL: https://www.postgresql.org
11. Docker containerization. URL: https://www.docker.com
12. Abdulqader D. та ін. Machine Learning Fraud Detection in Banking // Journal of Computer Science. — 2021



АРТЕМ КОЛЕСНИК
Студент, кафедра Інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0003-4474-7560
E-mail: kas1512@ukr.net
Отримав повну загальну середню освіту у спец. шк. №200 ім. Василя Стуса (Київ, Україна) Наукові інтереси: системи виявлення шахрайства, Інтернет речей, методи машинного навчання, тестування програмного забезпечення.



ВІТАЛІЙ МИХАЛЬЧУК
Ph.D., асистент кафедри Інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-7559-999X
E-mail: vitalii.mykhalchuk@knu.ua
Доктор філософії у галузі інформаційних технологій, наукові інтереси: Інтернет речей, нейро-комп’ютерний інтерфейс, математичне моделювання.



ІРИНА БОРИСЕНКО
к.т.н., доцент, кафедра Інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0001-8645-3881
E-mail: borysenko.iryna@knu.ua
Кандидат технічних наук, доцент, науковий інтерес зосереджений на дослідженні інформаційних систем, захисті інформації, програмуванні.

ПЛАНУВАННЯ РИЗИКІВ ПРОЄКТУВАННЯ ІТ СИСТЕМ МОНІТОРИНГУ ЕНЕРГОСПОЖИВАННЯ ОФІСНИХ ПРИМІЩЕНЬ ВЕЛИКОЇ ПЛОЩІ

Тимур Комісар, Ігор Пархомей

Анотація. *У роботі розглянуто методи планування ризиків при проєктуванні ІТ-систем моніторингу енергоспоживання офісів великої площі на базі Інтернету речей. Актуальність зумовлена потребою в автоматизації контролю ризиків та підвищенні відмовостійкості систем у сучасних будівлях. Запропоновано програмне рішення з візуальним конструктором схем електропостачання, що забезпечує автоматизовану оцінку технічних та IoT-ризиків. Результати дослідження спрямовані на зниження ймовірності критичних відмов та покращення загальної енергоефективності офісної інфраструктури.*

Ключові слова: Інтернет речей; планування ризиків; штучний інтелект; ІТ-інфраструктура.

I. ВСТУП

Сучасні офісні центри великої площі потребують впровадження інтелектуальних систем контролю енерговитрат для оптимізації бізнес-процесів та запобігання технічним аваріям. Актуальність теми зумовлена дефіцитом доступного інструментарію для оцінки надійності систем моніторингу на етапі планування а також оцінки наявних систем нефахівцями.

Метою дослідження є розробка методики та програмного забезпечення для автоматизованого планування ризиків при проєктуванні ІТ-систем моніторингу енергоспоживання з використанням технологій Інтернету речей (IoT).

Для досягнення мети вирішуються такі завдання: аналіз існуючих нотацій опису енергосистем; розробка спрощеної ієрархічної моделі об’єктів споживання; створення алгоритмів оцінки технічних ризиків та стабільності IoT-зв’язку.

Об’єктом дослідження є процес планування та оцінка інформаційних систем моніторингу енергоспоживання будівель на предмет ризиків.

Предметом дослідження є методи та програмні засоби візуального моделювання та автоматизованої оцінки ризиків відмов і втрати даних у топологіях офісних приміщень.

Обмеження дослідження передбачають проєктування внутрішніх низьковольтних мереж офісів та відповідної IoT-інфраструктури моніторингу без врахування специфіки високовольтного обладнання.

II. ДАНІ ТА МАТЕРІАЛИ

Модель предмета дослідження побудована на ієрархічному функціональному підході та включає набір уніфікованих модулів-конструкторів: джерел живлення, елементів захисту та кінцевих споживачів. Програмна реалізація системи здійснюється мовою C# із використанням технології WPF для створення сучасного векторного інтерфейсу моделювання.

Оцінка надійності сформованої системи проводиться за допомогою двох основних методів. Розрахунок технічних ризиків вузлів базується на матричному методі за формулою 1:

$$R = P \times I \tag{1}$$

де P - ймовірність виникнення аварійної ситуації, а I - показник впливу або критичності конкретного пристрою для бізнес-процесів офісу.

Стабільність системи моніторингу оцінюється через аналіз деградації IoT-сигналу, що враховує евклідову відстань між шлюзом і датчиком та коефіцієнти згасання при проходженні через фізичні перешкоди (стіни та перекриття).

Конкретне удосконалення предмета дослідження полягає у впровадженні гібридної моделі IoT-інфраструктури, де складні сенсорні мережі представлені як атрибути споживачів, що спрощує процес проєктування для нетехнічних фахівців. Також запропоновано використання логічного елемента «Розумний кабель» із ручним введенням довжини, що дозволяє проводити точні розрахунки спаду напруги без прив'язки до масштабу графічної схеми.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

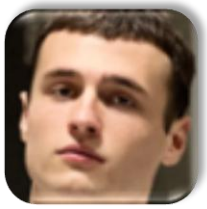
Розроблений програмний прототип на базі мови C# забезпечує автоматизоване візуальне моделювання топологій офісів та розрахунок ризиків у реальному часі. Впровадження спрощеної нотації та алгоритмів оцінки дозволило скоротити час на проєктування енергосистеми офісу на 40 %, а також виявити на 30 % більше потенційних «зон розриву» IoT-покриття ще на етапі планування. Практичне застосування розроблених методів знижує ймовірність критичних відмов серверного обладнання на 25 % шляхом автоматичної ідентифікації ризиків.

IV. ВИСНОВКИ

У ході дослідження розроблено методологію та програмний інструментарій для автоматизованого планування ризиків систем енергомоніторингу, що базується на спрощеній ієрархічній нотації та алгоритмах оцінки стабільності IoT-зв'язку. Запропонований підхід дозволяє нетехнічним фахівцям ефективно виявляти технічні вразливості та зони потенційної втрати даних на ранніх етапах проєктування.

ДЖЕРЕЛА

1. Makhadmeh, S.N., Al-Amied, A., Al-Wajih, R. and Al-Madi, N. (2023) 'IoT-Based Energy Management Systems in Smart Buildings: A Review', Energies, 16(2), 642.
2. Sembroiz, D., Careglio, D., Ricciardi, S. and Casier, J.P. (2022) 'Risk Assessment for IoT-based Energy Monitoring Systems in Large Scale Buildings', IEEE Access, 10, pp. 11234-11245.



ТИМУР КОМІСАР
студент 4 курсу бакалаврату програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: komistimur91@gmai.com
Наукові інтереси: Інтернет речей (IoT), планування та аналіз ризиків у складних інформаційних системах.



ІГОР ПАРХОМЕЙ
д.т.н., професор кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0002-9510-7657
E-mail: parkhomeii@fit.knu.ua
Фахівець у галузі IoRT, автор понад 100 публікацій, в КНУТШ працює з 2024 року.
Наукові інтереси: радіолокація, радіоавтоматика, робототехніка.

IOT СИСТЕМА УПРАВЛІННЯ ПОЛІКЛІНІКОЮ

Артем Копич

Анотація. *У представленій роботі розглянуто розробку IoT-системи управління інженерною інфраструктурою поліклініки. Досліджено актуальність автоматизації контролю мікроклімату приміщень, моніторингу стану медичного та інженерного обладнання, а також формування оперативних сповіщень для адміністрації закладу. Запропонована система забезпечує збір, обробку та аналіз даних з датчиків температури, вологості, рівня кисню, руху та стану обладнання. Реалізація проєкту дозволяє підвищити енергоефективність, зменшити простої обладнання та оптимізувати управлінські процеси в поліклініці.*

Ключові слова: IoT; поліклініка; автоматизація; моніторинг; управління інфраструктурою; енергоефективність.

I. ВСТУП

У повсякденних умовах цифрової трансформації медичні заклади потребують впровадження інтелектуальних систем управління інфраструктурою. Поліклініки характеризуються складною інженерною структурою, що включає системи вентиляції, кондиціонування, освітлення, медичне обладнання та допоміжні технічні засоби.

Неналежний контроль параметрів мікроклімату та стану обладнання може призводити до зростання експлуатаційних витрат, зниження ефективності роботи персоналу та виникнення аварійних ситуацій.

Інтернет речей (IoT) відкриває можливості для створення систем постійного моніторингу параметрів середовища та стану обладнання в режимі реального часу. Впровадження IoT-рішень у поліклініці дозволяє забезпечити централізований контроль, автоматичне формування сповіщень та аналітику для прийняття управлінських рішень. Метою роботи є розробка концепції IoT-системи управління поліклінікою, що забезпечує автоматизований збір та обробку даних для підвищення ефективності функціонування закладу.

II. ДАНІ ТА МЕТОДИ

Проєктована IoT-система управління інженерною інфраструктурою поліклініки базується на багаторівневій архітектурі, що забезпечує масштабованість, надійність та безперервність функціонування. Система складається з трьох логічних рівнів:

1. Рівень збору даних. На цьому рівні використовуються такі типи пристроїв: - датчики температури та вологості повітря; - датчики концентрації кисню; - датчики руху для контролю використання приміщень; - модулі моніторингу стану медичного обладнання (контроль живлення, часу роботи, аварійних сигналів); - кнопки екстреного виклику персоналу. Дані формуються у вигляді часових рядів та передаються з визначеною періодичністю або при виникненні події (event-driven модель).

2. Рівень передачі даних. Передача інформації здійснюється за допомогою бездротових мереж Wi-Fi з використанням протоколу MQTT, що забезпечує: - низьке енергоспоживання; - мінімальні затримки передачі; - підтримку publish/subscribe архітектури. Для підвищення надійності передбачено механізми повторної передачі пакетів у разі втрати з’єднання.

3. Рівень обробки та зберігання. Центральний сервер або хмарна платформа виконує: - прийом і валідацію даних; - збереження інформації в базі даних; - аналіз граничних значень; - формування сповіщень; - побудову аналітичних звітів. База даних структурована

за принципом: - таблиці показників датчиків; - журнали подій; - довідники обладнання; - облікові записи користувачів.

Функціонування системи можна описати відповідно за таким алгоритмом:

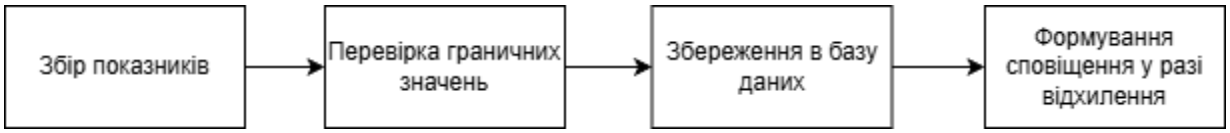


Рисунок 1. *Алгоритм обробки даних*

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті проєктування сформовано функціональну модель IoT-системи управління інженерною інфраструктурою поліклініки, що забезпечує централізований збір, обробку та аналіз даних у режимі реального часу. Система дозволяє здійснювати постійний моніторинг параметрів мікроклімату в кабінетах і технічних приміщеннях, контролювати стан медичного обладнання та оперативно реагувати на відхилення від нормативних значень.

Аналіз функціонування запропонованого рішення показує, що автоматизований контроль температури, вологості та рівня кисню сприяє стабілізації умов експлуатації приміщень. Це, у свою чергу, позитивно впливає на довговічність обладнання та зменшує ризик виникнення аварійних ситуацій. Контроль часу роботи медичних приладів дає можливість планувати технічне обслуговування на основі фактичного навантаження, а не лише за календарним графіком.

Важливим результатом є формування системи оперативного інформування адміністративного та технічного персоналу. У разі перевищення граничних параметрів система автоматично генерує повідомлення, що дозволяє скоротити час реагування та мінімізувати можливі втрати. Такий підхід забезпечує перехід від реактивної моделі управління до превентивної, коли потенційні проблеми виявляються на ранній стадії.

IV. ВИСНОВКИ

Запропонована IoT-система є перспективним інструментом модернізації управління поліклінікою. Її впровадження дозволяє перейти від реактивного до превентивного управління технічною інфраструктурою. Практична цінність роботи полягає у можливості адаптації рішення до інших медичних закладів із подібною структурою. Подальші дослідження можуть бути спрямовані на інтеграцію системи з медичними інформаційними системами та застосування методів прогнозної аналітики.

ДЖЕРЕЛА

1. Gubbi J., Buyya R., Marusic S., Palaniswami M. (2020) Internet of Things: A vision and architectural elements.
2. Al-Fuqaha A. et al. (2022) Internet of Things: A Survey on Enabling Technologies.
3. ISO/IEC 30141:2018 Internet of Things (IoT) – Reference Architecture.



АРТЕМ КОПИЧ
студент 4 курсу бакалаврату програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: artem.kopych@gmail.com
Студент Київського національного університету імені Тараса Шевченка.
Наукові інтереси — IoT системи моніторингу та контролю та застосування IoT-технологій у сфері охорони здоров'я.

ІНТЕГРАЦІЯ IOT-РІШЕНЬ У ЦИФРОВІ СИСТЕМИ ВІДЕОВИРОБНИЦТВА

Максим Котов, Віталій Михальчук

Анотація. *У роботі досліджено процеси інтеграції IoT-технологій у сучасне відео виробництво. Проаналізовано переваги переходу від традиційних інтерфейсів до IP-центричної архітектури студії на базі протоколів NDI та Art-Net. Особливу увагу приділено підвищенню відмово стійкості систем через використання інтелектуальних вузлів живлення з дистанційним моніторингом. Результати підтверджують ефективність автоматизації для українських медіа систем.*

Ключові слова: Інтернет речей, відео виробництво, NDI, автоматизація студії, Smart Studio, IP-комутація, енергонезалежність, IoT.

I. ВСТУП

Сучасний етап розвитку українського фільмо- та відео виробництва характеризується стрімкою професіоналізацією та виходом на міжнародні ринки. Цей динамічний ріст супроводжується гострою потребою в оптимізації виробничих процесів, що стає можливим завдяки інтеграції елементів та технологій Інтернету речей (IoT). Трансформація традиційних студій у цифрові екосистеми дозволяє забезпечити централізоване керування складним обладнанням, мінімізувати вплив людського фактора та значно підвищити мобільність знімальних груп у межах концепції Smart Studio.

II. ДАНІ ТА МЕТОДИ

Традиційні підходи до організації відео виробництва базуються на використанні фізичних інтерфейсів (SDI, HDMI, DMX-кабелі) та ручному керуванні кожним компонентом системи, що створює значні логістичні обмеження при масштабуванні проєктів. Викликом є необхідність синхронізації різнорідного обладнання в реальному часі, де будь-яка затримка або помилка комутації призводить до критичних втрат якості сигналу.

У якості методології дослідження пропонується перехід до IP-центрованої архітектури студії. Основним методом є впровадження стандартизованих мережевих протоколів для передачі відео, аудіо та керуючих сигналів в межах єдиної локальної обчислювальної мережі.

Використання таких технологій, як NDI (Network Device Interface) для відео та Art-Net / sACN для освітлення, перетворює кожен пристрій на інтелектуальний IoT-вузол. Дані про стан обладнання (температура світлових приладів, статус запису камер, рівень сигналу) збираються через мережеві інтерфейси (Ethernet/Wi-Fi) та агрегуються у централізованій системі управління (Control Room). Це дозволяє не тільки автоматизувати налаштування сценаріїв освітлення, але й динамічно перерозподіляти пропускну здатність мережі в залежності від пріоритетності відеопотоків.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті дослідження було встановлено, що інтеграція IoT-рішень у робочий процес відео виробництва трансформує лінійну структуру передачі сигналу у мережеву матрицю. Основними показниками ефективності такої системи є:

- Централізація керування: Впровадження протоколів керування світлом (наприклад, Art-Net) дозволяє об'єднати до 32 768 всесвітів DMX в одній мережі Ethernet. Аналіз

показує, що час на переналаштування світлових схем між сценами скорочується на 40-60% завдяки використанню цифрових шаблонів, доступних з єдиного термінала.

- Масштабованість та гнучкість: Використання технології NDI дозволяє додавати нові джерела сигналу (камери, смартфони, графічні станції) без прокладання додаткових коаксіальних кабелів. Аналіз пропускної здатності стандартної гігабітної мережі (1 Gbps) підтверджує можливість стабільної передачі до 7-8 потоків Full HD відео з мінімальною затримкою.
- Енергоефективність та відмовостійкість. Впровадження інтелектуального моніторингу електромережі дозволяє в реальному часі контролювати навантаження на студійне обладнання. Особливу роль відіграє інтеграція зарядних станцій (наприклад, серії EcoFlow) як IoT-вузлів живлення. Завдяки вбудованим Wi-Fi/Bluetooth модулям персонал може дистанційно відстежувати рівень заряду та прогнозувати час автономної роботи. Використання режиму EPS забезпечує перемикання на акумулятори за <30 мс, що критично для стабільності серверів та мережевих комутаторів.

Таблиця 1. *Порівняльний аналіз традиційної студії та IoT-орієнтованої студії.*

Параметр	**Традиційна студія (SDI/DMX)**	**IoT-студія (NDI/IP)**
Комутація	Масивна кабельна мережа (SDI, HDMI, XLR). Кожне з'єднання потребує окремого фізичного кабелю.	Єдина IP-мережа (Ethernet/Wi-Fi). Передача відео, аудіо, команд керування по одному кабелю.
Керування	Локальне налаштування кожного приладу вручну. Потребує фізичного доступу до камер та ламп.	Централізоване дистанційне керування через WEB-інтерфейси, мобільні застосунки або програмні консолі.
Автоматизація процесів	Обмежена. Зміна планів та світлових схем потребує значного часу та залучення персоналу.	Висока. Використання програмованих шаблонів та сценаріїв (Snapshots), що активуються однією командою.
Моніторинг та діагностика	Візуальний контроль. Виявлення несправностей відбувається переважно за фактом виходу обладнання з ладу.	Телеметрія в реальному часі. Моніторинг температури, статусу сигналу та стану мережі для запобігання збоям.
Енергоефективність та відмовостійкість	Традиційні ДБЖ без зворотного зв'язку. Ручне керування фазами живлення. Ризик втрати даних при збої мережі.	Інтелектуальні станції (EcoFlow) з EPS-режимом (<30 мс). Дистанційний контроль заряду та віддалене керування розетками.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведене дослідження підтверджує, що інтеграція IoT-рішень є ключовим чинником цифровізації та модернізації українського відео виробництва. Перехід до IP-центричної моделі студії дозволяє не лише автоматизувати рутинні операції, а й створює єдину

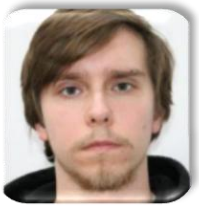
екосистему керування. На сьогодні цей тренд підтверджується широким впровадженням спеціалізованих IoT-застосунків та екосистем, таких як Sidus Link та Amaran App для інтелектуального керування освітленням через mesh-мережі, а також Canon Amaran Connect для дистанційного контролю параметрів експозиції та фокусування в реальному часі.

Важливою складовою сучасного продакшну є також автоматизація роботи зі звуком та тайм-кодом. Використання рішень на кшталт Zoom F2 Control та Tentacle Setup дозволяє здійснювати бездротову синхронізацію та моніторинг аудіозапису з мобільних пристроїв, що значно прискорює етап постпродакшну. Крім того, впровадження інтелектуальних систем моніторингу енергії та портативних зарядних станцій (типу EcoFlow) з дистанційним керуванням критично підвищує відмовостійкість процесів у сучасних енергетичних реаліях України.

Висновок. Подальший розвиток «розумних студій» (Smart Studios) вбачається у глибшій інтеграції штучного інтелекту для автоматичного аналізу телеметрії від згаданих програмних комплексів. Це забезпечить предикативне управління ресурсами, мінімізує технічні затримки та дозволить творчій групі повністю зосередитися на створенні якісного медіаконтенту, делегуючи технічний контроль автоматизованим IoT-системам.

ДЖЕРЕЛА

1. NDI (Network Device Interface) Technology Overview. Official Documentation. URL: https://www.ndi.video/tech/
2. Art-Net 4 Protocol Release Report. Artistic Licence Holdings Ltd. URL: https://artisticlicence.com/technology-resources/art-net/
3. Internet of Things (IoT) in Media and Entertainment Market Analysis. Global Industry Insights. URL: https://www.marketwatch.com/
4. EcoFlow Delta Series User Manual & Smart App Integration. EcoFlow Official Support. URL: https://www.ecoflow.com/us/support
5. IEEE 802.3 Standard for Ethernet. IEEE Standards Association. URL: https://standards.ieee.org/standard/802_3-2022.htmlСтаття про смертність дітей до п’яти років URL: https://data.unicef.org/topic/child-survival/under-five-mortality/



МАКСИМ КОТОВ
Студент, кафедра Інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0001-7717-7782
E-mail: kotovmaks374@gmail.com
Сфера інтересу – IoT, виробництво відео – фільмів, оптимізація процесів виробництва відео, через залучення та впровадження IoT рішень і технологій.



ВІТАЛІЙ МИХАЛЬЧУК
Ph.D., асистент кафедри Інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-7559-999X
E-mail: vitalii.mykhalchuk@knu.ua
Доктор філософії у галузі інформаційних технологій, наукові інтереси: Інтернет речей, нейро-комп’ютерний інтерфейс, математичне моделювання.

IOT СИСТЕМА МОНІТОРИНГУ І УПРАВЛІННЯ ОЧИСНИХ СПОРУД ВОДОКАНАЛУ

Ілля Кохановський, Ірина Борисенко

Анотація. *У роботі досліджено архітектуру та практичні аспекти впровадження IoT-системи моніторингу і управління очисних споруд водоканалу. Розглянуто чотирирівневу структуру системи: сенсорний, граничний, комунікаційний та хмарний рівні. Встановлено, що впровадження IoT забезпечує скорочення енергоспоживання на 13–15%, зниження ризику порушень нормативів якості на 20–30% та зменшення частки нерахованої води на 20–50%. Визначено ключові виклики реалізації та запропоновано поетапний підхід до цифрової трансформації очисних споруд.*

Ключові слова: Інтернет речей (IoT), очисні споруди, водоканал, моніторинг якості води, NB-IoT, LoRaWAN, предиктивне обслуговування, енергоефективність.

I. ВСТУП

Сфера водопостачання та водовідведення є однією з найважливіших галузей комунальної інфраструктури, що безпосередньо впливає на здоров'я населення та стан навколишнього середовища. За оцінками Grand View Research, світовий ринок інтелектуального управління водними ресурсами становив 18,34 млрд доларів США у 2024 році та, за прогнозами, досягне 50,74 млрд доларів до 2033 року зі щорічним темпом зростання (CAGR) 12,7%. Водоканали як ключові підприємства водогосподарського комплексу стикаються з нагальними викликами: зношеністю обладнання, зростанням вимог до якості очищення стічних вод і необхідністю скорочення операційних витрат. Саме тому Інтернет речей (IoT) стає стратегічним інструментом цифрової трансформації очисних споруд.

Традиційні SCADA-системи, якими оснащено переважну більшість водоканалів, мають суттєві обмеження: фіксовані точки вимірювання, висока вартість кабельної інфраструктури та неможливість адаптивного управління в режимі реального часу. Натомість IoT-рішення забезпечують масштабоване розгортання бездротових сенсорних мереж, хмарну аналітику та автоматизовані системи прийняття рішень, формуючи якісно новий рівень ефективності управління очисними спорудами.

Завдання роботи полягає у дослідженні архітектури IoT-системи для очисних споруд водоканалу, визначенні ключових переваг упровадження таких технологій та аналізі практичних аспектів реалізації і проблем, з якими стикаються підприємства водопостачання та водовідведення.

II. ДАНІ ТА МЕТОДИ

Дослідження ґрунтується на аналізі впровадження IoT-рішень на станціях очищення стічних вод (WWTP) і водопровідних станціях (WTP) на основі галузевих звітів, наукових публікацій, рецензованих статей та технічних кейсів провідних операторів водогосподарських підприємств.

Методи дослідження:

1. Огляд літератури. Проаналізовано рецензовані публікації з баз даних PubMed/PMC і ScienceDirect щодо IoT-систем моніторингу якості води (2024–2025), галузеві звіти Grand View Research, Fortune Business Insights та BCC Research з ринку інтелектуального водоуправління, а також технічну документацію компаній Xylem, Siemens і ABB.

2. Кейс-аналіз. Розглянуто успішні приклади впровадження IoT на очисних спорудах: проєкт IBM у Іспанії зі зниження енергоспоживання, партнерство Siemens та KETOS для моніторингу якості води (2025), а також платформу Schneider Electric EcoStruxure для автоматизації найбільшої водоочисної станції Мумбаї.
3. Порівняльний аналіз технологій. Порівняно протоколи бездротового зв'язку (NB-IoT, LoRaWAN, Cellular) за параметрами: дальність, споживання енергії, надійність у промислових умовах; платформи хмарної аналітики та методи предиктивного обслуговування.
4. Системний аналіз. Досліджено багаторівневу архітектуру IoT-системи очисних споруд - від сенсорного рівня до рівня прийняття рішень - з урахуванням специфіки технологічних процесів водоочищення: аерації активного мулу, анаеробного зброджування, хлорування та ультрафіолетового знезараження.

Особлива увага приділялася показникам, що контролюються у процесі очищення: pH, розчиненому кисню (DO), каламутності, загальним розчиненим речовинам (TDS), біохімічному споживанню кисню (БСК), температурі та хімічному споживанню кисню (ХСК). Дослідження також враховувало специфіку протоколів NB-IoT, який займає 32,5% ринку комунікацій систем інтелектуального водоуправління (2024), та LoRaWAN з прогнозованим темпом зростання 15,7% CAGR завдяки перевагам у терміні служби акумуляторів.

III. РЕЗУЛЬТАТ ТА АНАЛІЗ

Застосування IoT-технологій на очисних спорудах водоканалу формує комплексну цифрову екосистему, яка охоплює три функціональні рівні: збір даних, їх обробку та управління процесами. Результати аналізу свідчать про значний технологічний та економічний потенціал таких рішень.

Архітектура IoT-системи очисних споруд є багаторівневою.

Таблиця 1. Компоненти архітектури IoT-системи очисних споруд водоканалу

Рівень	Компоненти	Функція в очищенні води
Сенсорний (польовий)	Давачі pH, DO, TDS, каламутності, витратоміри, датчики тиску	Неперервний контроль параметрів якості та кількості вод
Граничний (edge)	Мікроконтролери, PLC, IoT-шлюзи (NB-IoT / LoRaWAN)	Первинна обробка, аварійне сповіщення, управління клапанами
Мережевий (комунікаційний)	Cellular, LoRaWAN, NB-IoT, LPWAN	Передача даних від розосереджених об'єктів до центральної платформи
Аплікаційний (хмарний)	SCADA/MES-інтеграція, BI-аналітика, ML-моделі	Оптимізація аерації, дозування реагентів, предиктивне обслуговування

Сенсорний рівень включає мережу інтелектуальних давачів, розміщених у ключових точках технологічного процесу: на вході каналізаційних колекторів, у відстійниках, аераційних басейнах, на виході очищених вод та у мережах водовідведення. Проведений аналіз систем (зокрема, APAH-системи, що пройшла валідацію на чотирьох промислових очисних спорудах в Індії) показав, що безперервний моніторинг pH, DO, TDS, каламутності та провідності у поєднанні з автоматичними клапанами дозволяє попередити забруднення ще до виходу за межі допустимих значень. Граничний рівень (edge layer) забезпечує первинну

обробку даних безпосередньо на об'єкті, зменшуючи затримку передачі критичних сигналів і навантаження на канали зв'язку. Хмарна платформа виконує довгострокове зберігання, аналітику великих даних і надає операторам зручний веб- або мобільний інтерфейс.

Підприємства водопостачання, що впровадили інтегровані IoT-рішення, досягли вагомих результатів у кількох ключових напрямках.

1. Енергоефективність. Аерація активного мулу є найбільш енергоємною операцією на очисних спорудах. IoT-оптимізація режимів аерації у поєднанні з динамічним управлінням насосними станціями дозволила досягти економії електроенергії на рівні 13–15% (зокрема, реалізований IBM проєкт в Іспанії зафіксував 13%-ву економію), а також скорочення виробництва осаду на 17%.
2. Якість очищення та відповідність нормативам. Безперервний онлайн-моніторинг замість дискретного лабораторного аналізу забезпечує своєчасне виявлення відхилень від регламентних параметрів. Дослідження, опубліковане у Heliyon (2024), підтвердило точність IoT-систем із граничною похибкою вимірювань 0,1–0,2 за всіма ключовими показниками. Передбачувальна аналітика дає змогу скоротити ризик порушень скидних нормативів на 20–30%.
3. Управління хімічними реагентами. Надточне дозування коагулянтів, флокулянтів та дезінфектантів на основі сигналів від давачів у реальному часі усуває надлишкове вживання хімікатів, зменшуючи як операційні витрати, так і ризики утворення побічних продуктів дезінфекції.
4. Скорочення втрат води. Впровадження систем виявлення витоків на основі IoT-датчиків тиску і витрат дозволяє знизити частку нерахованої води (NRW) на 20–50%, що критично важливо для українських водоканалів зі значним фізичним зносом мереж.

Разом із тим аналіз виявив ключові виклики впровадження IoT на очисних спорудах. Корозивне та вологе середовище ставить жорсткі вимоги до захищеності обладнання (клас IP67/IP68). Інтеграція з застарілими SCADA-системами потребує розробки middleware-рішень або поетапного оновлення. Безпека даних для критичної комунальної інфраструктури вимагає виконання вимог промислової кібербезпеки (IEC 62443). Висока початкова вартість сенсорної мережі та хмарних платформ ускладнює бізнес-обґрунтування для малих водоканалів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведене дослідження підтверджує, що IoT-системи моніторингу і управління є ефективним інструментом модернізації очисних споруд водоканалу, здатним забезпечити одночасне поліпшення якості очищення, зниження операційних витрат і підвищення відповідності екологічним нормативам.

Для успішного впровадження необхідний поетапний підхід: перший етап передбачає базовий моніторинг ключових точок (вхід/вихід очисних споруд, аераційні басейни), другий - інтеграцію з автоматизованими системами управління і хмарною аналітикою, третій - впровадження ML-моделей предиктивного обслуговування і цифрових двійників технологічного процесу. Такий підхід дозволяє починати з мінімальних інвестицій і швидко демонструвати окупність.

Технологічний аспект потребує ретельного вибору комунікаційного протоколу залежно від особливостей об'єкта: NB-IoT є оптимальним для міської інфраструктури з покриттям мобільних мереж, тоді як LoRaWAN ефективніший для відокремлених споруд завдяки автономній роботі протягом 10–15 років. Організаційний аспект передбачає перебудову процесів оперативного управління та розвиток цифрових компетенцій персоналу.

Для водоканалів України впровадження IoT набуває особливої актуальності в контексті воєнного часу: дистанційний моніторинг дозволяє мінімізувати присутність персоналу на об'єктах та забезпечити безперервну роботу систем водопостачання навіть за умов обмеженого доступу. Прогнозоване зростання глобального ринку IoT у системах водоочищення з 2,6 млрд до 7,1 млрд доларів до 2034 року (CAGR 11,8%) підтверджує стратегічний характер цього напряму цифрової трансформації комунальної інфраструктури.

Таким чином, IoT-система моніторингу і управління очисних споруд водоканалу є не просто технологічним вдосконаленням, а необхідною умовою сталого розвитку водогосподарського комплексу в епоху Індустрії 4.0. Її впровадження дозволяє трансформувати управління очисними спорудами від реактивного реагування на аварійні ситуації до проактивного оперативного управління на основі даних реального часу.

ДЖЕРЕЛА

1. Smart Water Management Market Size, Share & Forecast. Grand View Research, 2024. URL: https://www.grandviewresearch.com/industry-analysis/smart-water-management-swm-market
2. Uddin M.R. et al. IoT based real-time water quality monitoring system in water treatment plants (WTPs). Heliyon. 2024. Vol. 10(23). e40746. doi: 10.1016/j.heliyon.2024.e40746
3. Water trends in wastewater for 2024: Digital transformation of WWTPs. IDRICA, 2024. URL: https://www.idrica.com/blog/water-trends-wastewater-wwtps/
4. IoT Applications in Waste and Wastewater Management. Kajeet, Inc., 2023. URL: https://www.kajeet.com/en/blog/iot-applications-waste-and-water-management
5. IoT in Water Treatment Systems Market Size, Share & Forecast 2025–2034. USD Analytics, 2025. URL: https://www.usdanalytics.com/industry-reports/iot-in-water-treatment-systems-market
6. Essamlali I., Nhaila H., El Khaili M. Advances in machine learning and IoT for water quality monitoring: A comprehensive review. Heliyon. 2024. Vol. 10(6). e27920. doi: 10.1016/j.heliyon.2024.e27920
7. Smart Water Management Market Size, Trends Report 2025–2030. Mordor Intelligence, 2025. URL: https://www.mordorintelligence.com/industry-reports/smart-water-management-market
8. Smart Water Management: Global Markets to 2030. BCC Research, 2025. URL: https://www.bccresearch.com/pressroom/mst/global-smart-water-management-market-projected-to-reach-$437-billion



ІЛЛЯ КОХАНОВСЬКИЙ
студент 1 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка
E-mail: kokhanovskyii@fit.knu.ua
Науковий інтерес полягає в області розробки та застосування IoT-систем у комунальній інфраструктурі, зокрема в системах водопостачання та водовідведення для автоматизації моніторингу і оптимізації процесів очищення стічних вод.



ІРИНА БОРИСЕНКО
Кандидат технічних наук, доцент кафедри інформаційних систем та технологій, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0005-8350-6422
E-mail: borysenkoi@fit.knu.ua
Науковий інтерес зосереджений на дослідженні інформаційних систем, захисті інформації, програмуванні.

МОНІТОРИНГ ТА АНАЛІЗ ТРЕНУВАЛЬНОГО НАВАНТАЖЕННЯ СПОРТСМЕНІВ У IOT-СИСТЕМАХ

Андрій Кураш, Мирослава Гладка

Анотація. *У роботі обґрунтовано доцільність застосування IoT-рішень для моделювання та аналізу тренувального навантаження з метою запобігання травмам у професійному спорті. Розглянуто ризики, пов'язані з інтенсивними фізичними навантаженнями, та проаналізовано можливості використання носимих сенсорів і аналітичних алгоритмів для безперервного моніторингу фізіологічних показників спортсменів. Запропонований підхід забезпечує персоналізоване оцінювання стану спортсмена, своєчасне виявлення ознак перевтоми та підвищення ефективності тренувального процесу.*

Ключові слова: IoT; моніторинг фізіологічних показників; тренувальне навантаження; прогнозування травм.

I. ВСТУП

Із стрімким розвитком цифрових технологій у різних сферах суспільства спортивна індустрія також зазнає суттєвих трансформацій. У сучасному професійному спорті ефективний контроль тренувального навантаження є ключовим чинником запобігання перевтомі, підвищенню результативності та зменшенні травмуванню спортсменів. В умовах цифровізації Інтернет речей (IoT) забезпечує інтеграцію фізичного середовища з цифровим простором, відкриваючи нові можливості для безперервного збору, передачі та аналізу фізіологічних даних [1]. IoT-технології змінюють підхід до роботи тренерів, спортивних лікарів і фізіотерапевтів, сприяючи зменшенню кількості травм, підвищенню точності оцінювання стану спортсменів та прискоренню їх відновлення [1].

II. ДАНІ ТА МЕТОДИ

Для ефективного контролю стану спортсменів під час тренувань аналізуються ключові фізіологічні показники:

- частота серцевих скорочень (ЧСС), що використовується для оцінювання рівня внутрішнього навантаження та виявлення ознак перенапруження [2];
- рівень насичення крові киснем (SpO_2), для контролю рівня кисневого забезпечення організму та своєчасного виявлення ризику гіпоксії [3];
- температура тіла, що застосовується для моніторингу терморегуляції та виявлення ознак перегріву або запальних процесів [4];
- м'язова активність (EMG), для визначення ступеня залучених м'язових груп, рівня втоми та ефективності виконаних фізичних вправ [5].

Для оцінювання ефективності IoT-платформи здійснюється комплексний аналіз процесів збору, передачі та обробки даних, що забезпечує надійний і безперервний моніторинг функціонального стану спортсменів.

Збір та передача даних включає використання носимих сенсорних пристроїв для вимірювання фізіологічних показників у режимі реального часу з подальшою передачею інформації на серверну частину системи через бездротові канали зв'язку.

Методи обробки даних передбачають попередню фільтрацію та нормалізацію сигналів, застосування алгоритмів виявлення аномалій для ідентифікації відхилень у фізіологічних показниках, а також прогнозування ризику травм на основі аналізу історичних даних і динаміки змін параметрів.

Для забезпечення точності, адаптивності та персоналізації IoT-платформи передбачено налаштування системи з урахуванням індивідуальних фізіологічних характеристик спортсменів та визначення критичних порогових значень контрольованих параметрів.

Методика налаштування включає індивідуальну калібровку порогових значень для кожного спортсмена на основі базових показників у стані спокою та під час типових тренувальних навантажень, а також реалізацію механізму автоматичних сповіщень у разі перевищення допустимих меж.

Приклад конфігурації системи:

– частота серцевих скорочень (ЧСС) оновлюється з інтервалом 10 секунд; рівень насичення крові киснем (SpO_2), температура тіла та показники м'язової активності (EMG) – з інтервалом 30 секунд;
– у разі перевищення ЧСС понад 180 уд./хв, зниження SpO_2 нижче 90 %, підвищення температури тіла понад 38 °C або перевищення встановленого порогу м'язової активності (що свідчить про локальне перенавантаження) формується автоматичне попередження для тренера або медичного персоналу.

У задачах моніторингу фізіологічних показників спортсменів ключовими є обробка потокових даних та виявлення прихованих закономірностей у великих масивах інформації. Для цього застосовуються методи математичного моделювання та аналізу даних.

Методи кластеризації:

Алгоритми кластерного аналізу [6] використовуються для групування спортсменів або тренувальних сесій за подібністю фізіологічних показників, що дозволяє виявляти типові профілі навантаження та закономірності адаптації організму.

Застосування:

– сегментація спортсменів за рівнем фізичної активності;
– визначення оптимальних тренувальних стратегій для різних кластерів.

Логістична регресія:

Метод логістичної регресії [7] застосовується для прогнозування ймовірності настання бінарних подій, зокрема ризику травм або перенапруження, на основі історичних фізіологічних даних.

Застосовується для

– визначення ймовірності травмування залежно від динаміки ЧСС, SpO_2, температури тіла та м'язової активності.

Для розв'язання задачі попередження ризиків травм під час тренувань спортсменів доцільно є використання методу логістичної регресії.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Архітектура IoT-екосистеми моніторингу фізичного стану спортсменів спроєктована з урахуванням необхідності передачі даних у реальному часі, аналізу показників та доступності інформації для тренерів і медичних фахівців. Основні компоненти архітектури наведені на рисунку 1.



Рисунок 1. *Основні компоненти архітектури IoT*

Основні компоненти архітектури:

1. носимі датчики, що включають пульсометри, пульсоксиметри, термометри та EMG-сенсори, забезпечують безперервний збір фізіологічних показників спортсмена, зокрема частоти серцевих скорочень, рівня насичення крові киснем, температури тіла та м'язової активності, у режимі реального часу;
2. комунікаційний шлюз, який здійснює приймання даних від сенсорів через бездротові протоколи (Bluetooth, Wi-Fi), виконує їх попередню агрегацію та передає інформацію до серверної або хмарної інфраструктури;
3. хмарна платформа, на якій реалізуються процеси фільтрації, нормалізації та аналітичної обробки даних, забезпечує оцінювання тренувального навантаження та прогнозування ризиків;
4. програмне забепечення для аналізу, що базується на математичних моделях і алгоритмах машинного навчання, формує оцінку стану спортсмена та генерує рекомендації щодо інтенсивності навантаження і тривалості відновлення;
5. інтерфейс користувача, який представлений у вигляді веб- або мобільного застосунку, забезпечує візуалізацію показників у формі графіків, трендів і рекомендація та підтримує прийняття рішень тренером і медичним персоналом.

Принцип роботи системи зображений на рисунку 2.



Рисунок 2. *Принцип роботи системи*

Алгоритм функціонування системи:

1. на етапі збору даних здійснюється безперервне вимірювання фізіологічних показників спортсмена за допомогою носимих сенсорів із формуванням потокових даних у режимі реального часу;
2. під час виконання процесу передачі даних виміряні параметри передаються до комунікаційного шлюзу через протоколи короткодистанційного бездротового зв'язку (Bluetooth, Wi-Fi) та спрямовуються до хмарної платформи для подальшої обробки;
3. на етапі аналітичної обробки у хмарі виконуються процедури фільтрації, нормалізації та класифікації показників, а також застосовуються моделі прогнозування ризику травм і перенапруження на основі поточних і накопичених даних;

4. у межах візуалізації результатів аналітична інформація відображається в користувацькому інтерфейсі у вигляді графіків, трендів і рекомендацій, що забезпечує обґрунтоване коригування тренувального навантаження.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

IoT-системи моніторингу фізіологічних показників спортсменів суттєво підвищують ефективність тренувального процесу, забезпечуючи безперервний контроль функціонального стану організму та зменшуючи ризик травмування. Інтеграція носимих сенсорів, комунікаційної інфраструктури та алгоритмів аналітичної обробки даних дозволяє реалізувати адаптивну й персоналізовану систему підтримки прийняття рішень у професійному спорті.

ДЖЕРЕЛА

1. In Sports for Injury Health Monitoring [Електронний ресурс] – URL: https://ijrpr.com/uploads/V5ISSUE1/IJRPR21878.pdf
2. Athlete's heart rate: When is it safe and when is it too high? [Електронний ресурс] – URL: https://www.vinmec.com/eng/article/athletes-heart-rate-when-is-it-safe-and-when-is-it-too-high-en
3. Does blood oxygen level drop during exercise? [Електронний ресурс] – URL: https://smartwellness.com.au/blog/does-blood-oxygen-level-drop-during-exercise/?srsltid=AfmBOop0fJThPRB1MlVJI04ofmSxPJbHyMgRhjdMhke6CxrXJZg1oIrY
4. Control your core body temperature and get better performance results [Електронний ресурс] – URL: https://www.suunto.com/sports/News-Articles-container-page/control-your-core-body-temperature-and-get-better-performance-results/
5. The Growing Role of Wearables in Sports [Електронний ресурс] – URL: https://www.hashstudioz.com/blog/iot-in-sports-improving-safety-and-injury-prevention-through-wearables/
6. Clustering Algorithm [Електронний ресурс] – URL: https://www.sciencedirect.com/topics/engineering/clustering-algorithm
7. What is logistic regression? [Електронний ресурс] – URL: https://www.ibm.com/topics/logistic-regression



АНДРІЙ КУРАШ
студент 2 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: kurasha231@gmail.com
Науковий інтерес полягає в області розробки та впровадження IoT-рішень для підвищення ефективності тренувального процесу та зниження ризику травм у спорті. Серед наукових інтересів — IoT-системи моніторингу фізичних показників спортсменів, аналіз та прогнозування ризиків травм, а також застосування IoT-технологій у спортивній медицині.



МИРОСЛАВА ГЛАДКА
к.т.н., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-5233-2021
E-mail: myroslava.gladka@knu.ua
Коло наукових інтересів: управління проєктами, моделювання та інжиніринг бізнес-процесів.

IOT-ШАР ДЛЯ SCADA/PLC БІОГАЗОВОГО КОМПЛЕКСУ

Максим Кривченко, Володимир Дружинін

Анотація. *Біогазові комплекси – інерційні, але чутливі до порушень режимів: зміни температури, pH, органічного навантаження чи перемішування знижують вихід метану та можуть спричинити зупинки. Традиційний контроль із лабораторними затримками ускладнює раннє виявлення відхилень. У тезах обґрунтовано IoT-шар для безперервного моніторингу (T, pH, тиск/витрата, склад, H_2S), тривог і підтримки рішень та інтеграцію зі SCADA/PLC через OPC UA, Modbus, MQTT. Окремо виділено технічні обмеження: надійність зв'язку, калібрування сенсорів, сумісність з промисловими протоколами та кібербезпека OT-середовища.*

Ключові слова: IoT, біогаз, анаеробне зброджування, SCADA, моніторинг.

I. ВСТУП

Біогазові та біоенергетичні комплекси перетворюють органічні відходи на енергоносій, але стабільність і економічність цього процесу залежать від підтримання режимів анаеробного зброджування. На практиці відхилення (перевантаження субстратом, температурні коливання, проблеми з перемішуванням, токсичні домішки) можуть проявлятися поступово: спочатку змінюються «ранні» індикатори, а наслідки (падіння виходу газу, зміна частки CH_4, зростання H_2S, нестабільність тиску/витрати) стають помітними із запізненням. Через це системи, що працюють лише на основі періодичного ручного контролю, ризикують реагувати надто пізно.

Біогаз утворюється внаслідок анаеробного зброджування, що проходить послідовні етапи: *гідролізу → ацидогенезу → ацетогенезу → метаногенезу.* Кожен етап має різну чутливість до температури, pH, часу утримання та органічного навантаження (OLR), тому контроль цих параметрів безпосередньо впливає на вихід і якість біогазу [1]. Типова установка включає підготовку та подачу субстрату, біореактор(и) з перемішуванням і підігрівом, газозбір і очищення (осушення/видалення H_2S), а також когенерацію або апгрейдинг до газової мережі [2].

Інтеграція IoT не замінює промислову автоматизацію, але може доповнювати її: забезпечувати частіший збір даних, віддалену візуалізацію, журналювання, базові правила тривог та прикладну аналітику (наприклад, короткостроковий прогноз виробництва/якості газу) [3]. Важливо, щоб таке рішення було сумісним із наявною SCADA/PLC-інфраструктурою та враховувало вимоги надійності й кібербезпеки OT-сегмента.

II. ДАНІ ТА МЕТОДИ

Запропонований підхід розглядає IoT-рівень як надбудову над наявною SCADA/PLC-інфраструктурою біогазової установки: критичні дії залишаються на рівні PLC/оператора, а IoT-контур забезпечує ущільнення телеметрії, уніфікацію часових рядів, тривоги та аналітику.

Джерела даних формуються з трьох класів. Перший – польові вимірювання від промислових датчиків та аналізаторів (T, pH, тиск/витрата, CH_4/CO_2, H_2S; за потреби O_2) через типові інтерфейси 4-20 mA, RS-485/Modbus RTU або дискретні сигнали. Другий – контекстні теги SCADA/PLC, які пов'язують відхилення з режимами роботи: подача субстрату (якщо доступно), перемішування, підігрів, стани насосів/клапанів, аварійні сигнали та переходи між режимами. Третій – довідкові й експлуатаційні дані (уставки, межі,

паспортні обмеження, журнали обслуговування), а також, за наявності, лабораторні показники (лужність, VFA) як рідкісні контрольні точки.

Збір і узгодження телеметрії виконується на польовому рівні через PLC або локальний шлюз без втручання в керуючі ланцюги. Шлюз забезпечує синхронізацію часу, приведення одиниць, перевірку діапазонів і базові тести якості (вихід за межі, різкі стрибки, пропуски), а також буферизацію при втраті мережі. Для відсіювання некоректних даних зберігаються метадані калібрування і вводиться маркування вимірів, щоб аналітика не інтерпретувала помилки як реальні відхилення процесу.

Передача, збереження та інтеграція реалізуються через MQTT (потоково) або HTTPS/REST (пакетно). На сервері дані зберігаються у сховищі часових рядів, а події (перемикання режимів, тривоги, втрата зв'язку, обслуговування) – у журналі, що дозволяє відтворювати ланцюги «режим → зміна параметрів → вихід/якість газу». Результати IoT-шару повертаються у SCADA через OPC UA або Modbus TCP у вигляді корисних змінних (показники якості сигналів, тривоги, індикатори аномалій, прогнозні значення на 24-72 год), без передачі «сирих» потоків у SCADA [4].

Тривоги, прогноз і аномалії формуються на першому етапі простими й пояснюваними методами. Тривоги задаються пороговими та трендовими правилами з гістерезисом/затримкою підтвердження і комбінованими умовами (наприклад, падіння pH разом зі зміною CH_4 або нестабільністю витрати/тиску). Прогноз на 24-72 год для витрати та частки CH_4 (за потреби H_2S) будується на основі лагових ознак і трендів, оцінюється MAE/MAPE та подається як очікуване значення з діапазоном невизначеності. Для елементів «predictive maintenance» використовуються індикатори аномалій у режимах/циклах роботи вузлів (мішалки, насоси, газоочистка) та непрямі ознаки (нестабільність тиску/витрати, зростання H_2S, за наявності – струм/потужність двигунів або перепад тиску), з фіксацією подій і прив'язкою до режимів SCADA. Надійність і OT-кібербезпека забезпечуються сегментацією OT/IT, розмежуванням доступу, автентифікацією/шифруванням телеметрії (де можливо) та журналюванням. Принципово IoT-рівень не здійснює прямого керування PLC: він працює як моніторинг і підтримка рішень, а критичні дії залишаються у технологічному контурі [5].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Відповідно до архітектури на Рисунку 1 сформовано три вихідні результати: (1) узгоджений архів часових рядів ключових параметрів (T, pH, тиск/витрата, CH_4/CO_2, H_2S) із позначенням якості даних; (2) журнал подій (режими, тривоги, втрати зв'язку, обслуговування), який дозволяє відтворювати ланцюги «режим → зміна параметрів → вихід/якість газу»; (3) набір агрегованих індикаторів для інтерфейсів оператора (SCADA/Grafana), включно з попереджувальними станами, індикаторами аномалій та прогнозними значеннями.

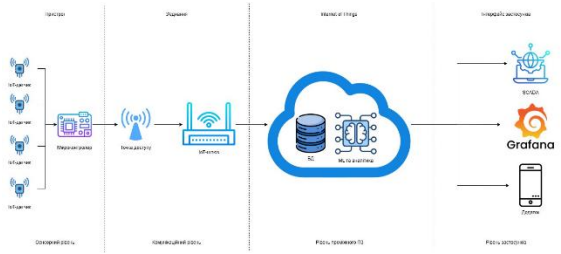


Рисунок 1. *Узагальнена архітектура IoT-рівня як надбудови над SCADA/PLC*

Застосування цих підходів підвищує оперативність реагування без зміни логіки керування: ранні зміни параметрів (зсув pH, нестабільність тиску/витрати, зміна частки CH_4)

стають помітними як тренди й події до того, як проявиться падіння продуктивності, а прив'язка до режимних тегів спрощує пошук причин. Узгоджене відображення в SCADA та аналітичних панелях зменшує ризик різночитань, оскільки оператор отримує не «сирі потоки», а інтерпретовані показники та попередження, придатні для прийняття рішень.

IV. ВИСНОВКИ

Запропонований підхід демонструє, що додавання IoT-рівня до наявної SCADA/PLC-інфраструктури є практичним способом підвищити прозорість процесу анаеробного зброджування та керованість експлуатації за рахунок узгоджених даних і подій. Важливо, що IoT-контур у цій постановці не підміняє технологічне керування, а працює як надбудова моніторингу й підтримки рішень, зменшуючи затримку між виникненням відхилення та його фіксацією. Вирішальними умовами успішності є метрологічна дисципліна, стійкість збору/передачі телеметрії та дотримання вимог OT-кібербезпеки. Водночас точність прогнозних компонентів і детектування аномалій суттєво залежить від повноти історичних даних і різноманіття режимів, на яких виконуватиметься валідація. Подальша робота доцільна у форматі пілотного впровадження з кількісною оцінкою ефекту на конкретному майданчику та перевіркою прогнозних моделей на реальних часових рядах.

ДЖЕРЕЛА

1. Wu D., Li L., Peng Y., Yang P., Peng X., Sun Y., Wang X. State indicators of anaerobic digestion: A critical review on process monitoring and diagnosis, стаття. Renewable and Sustainable Energy Reviews. 2021. URL: https://doi.org/10.1016/j.rser.2021.111260.
2. Galloni M., Di Marcoberardino G. Biogas Upgrading Technology: Conventional Processes and Emerging Solutions Analysis, стаття. Energies. 2024. URL: https://doi.org/10.3390/en17122907.
3. Marycz M., Turowska I., Glazik S., Jasiński P. Artificial Intelligence in Anaerobic Digestion: A Review of Sensors, Modeling Approaches, and Optimization Strategies, стаття. Sensors. 2025. URL: https://doi.org/10.3390/s25226961.
4. Freitas L., Silva M., Vale G., Avram C., Lopes H., Pereira F., Leal N., Machado J. OPC UA and MQTT performance analysis within a unified namespace context, стаття. Internet of Things. 2025. URL: https://doi.org/10.1016/j.iot.2025.101734.
5. Stouffer K., Pillitteri V., Pease M., Lightman S., Tang C.-Y., Zimmerman T., Hahn A. та ін. Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev. 3), стандарт/керівництво. National Institute of Standards and Technology. 2023. URL: https://doi.org/10.6028/NIST.SP.800-82r3.



МАКСИМ КРИВЧЕНКО
студент 1 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
ORCID: 0009-0007-4882-5246
E-mail: maxym.kryv@gmail.com
Серед наукових інтересів – промисловий IoT, SCADA/PLC-інтеграція та аналітика даних для моніторингу і підтримки рішень.



ВОЛОДИМИР ДРУЖИНІН
д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@fit.knu.ua
Коло наукових інтересів: методи та алгоритми машинного навчання в радіолокаційних системах, радіомоніторинг та радіочастотний менеджмент, багатопозиційна радіолокація.

ТЕХНОЛОГІЯ КЕРУВАННЯ РОЗУМНИМИ ПРИСТРОЯМИ РІДНОЮ МОВОЮ

Богдан Куцуліма, Ольга Кравченко

Анотація. *У роботі запропоновано технологію голосового керування розумними пристроями українською мовою на основі клієнт-серверної архітектури. Представлено модульну структуру системи, що включає локальне розпізнавання активаційного слова, серверну обробку мовлення (STT), семантичний аналіз запиту за допомогою LLM, інтеграцію з IoT та Internet Access модулями, а також синтез мовлення (TTS). Розглянуто переваги розподілу функцій між клієнтом і сервером щодо масштабованості, енергоефективності та захисту персональних даних..*

Ключові слова: розумна колонка; IoT; клієнт-серверна архітектура; LLM; голосове керування.

I. ВСТУП

Розвиток штучного інтелекту та Інтернету речей формує нові підходи до організації взаємодії людини з цифровими системами. Одним із перспективних напрямів є створення розумних колонок, що поєднують функції голосового асистента та центру керування пристроями розумного дому[2].

Підтримка керування рідною мовою користувача підвищує доступність системи та розширює можливості її практичного застосування.

Метою роботи є розробка технології керування розумними пристроями українською мовою з використанням клієнт-серверної архітектури, що забезпечує ефективну обробку мовлення, інтеграцію з IoT та захист персональної інформації користувача.

II. ОПИС РІШЕННЯ

Запропонована система реалізована на основі клієнт-серверної архітектури з розмежуванням функціональних компонентів між локальним пристроєм користувача та серверною частиною, що виконує основні обчислювальні операції. Структуру системи[1] наведено на Рисунку 1.

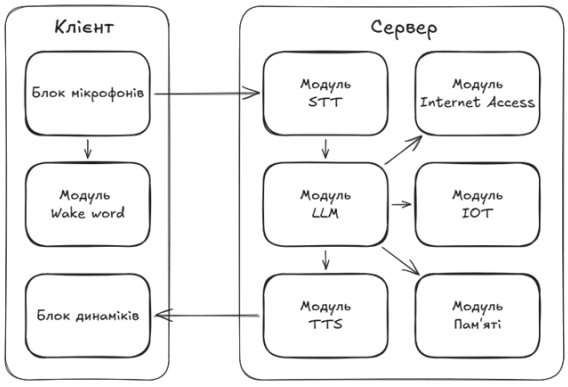


Рисунок 1. *Клієнт-серверна архітектура системи голосового керування*

Клієнтська частина включає блок мікрофонів, модуль розпізнавання активаційного слова та блок динаміків. Основним завданням клієнта є безперервне прослуховування навколишнього середовища з мінімальним енергоспоживанням та локальне визначення

моменту початку взаємодії. Лише після розпізнавання активаційної фрази аудіопотік передається до серверної частини.

Передача аудіо даних здійснюється потоково через захищене мережеве з'єднання[3]. У серверній частині аудіо сигнал надходить до модуля розпізнавання мовлення, який перетворює його на текстовий формат. Отриманий текст разом із параметрами сесії передається до модуля обробки природної мови.

LLM-модуль, виконує функцію центрального координатора системи. Він здійснює семантичний аналіз запиту, визначає намір користувача та формує логіку подальших дій. Якщо запит пов'язаний із керуванням пристроями розумного дому, активується IoT-модуль. У разі інформаційного запиту використовується модуль Internet Access. Модуль пам'яті забезпечує підтримку контексту діалогу та персоналізацію взаємодії.

Після виконання відповідної операції формується текстова відповідь, яка передається до модуля синтезу мовлення. TTS-модуль генерує аудіопотік, який надсилається клієнтській частині для відтворення через блок динаміків. В результаті, реалізується повний цикл голосової взаємодії: активація, передача аудіо, розпізнавання, семантичний аналіз, виконання команди, озвучування результату.

III. ВИСНОВКИ

Запропоноване рішення забезпечує ефективну інтеграцію голосового інтерфейсу з екосистемою IoT. Клієнт-серверна архітектура дозволяє масштабувати систему для великої кількості користувачів, централізовано оновлювати мовні моделі та зменшувати навантаження на апаратні ресурси пристрою.

Водночас локальне розпізнавання активаційного слова та контроль передачі даних сприяють підвищенню рівня захисту персональної інформації, що є важливим аспектом безпеки IoT-систем [3]. Подальші дослідження передбачають оптимізацію затримки відповіді, удосконалення безпеки даних та розширення функціональності офлайн-режиму.

ДЖЕРЕЛА

1. Hayashi, T., Tanaka, Y. and Kobayashi, M., 2020. OKIoT: Trade-off analysis of smart speaker architecture on Open Knowledge IoT project. Internet of Things.
2. Kaiborta, S. and Samal, S., 2022. IoT based Voice Assistant for Home Automation. International Journal of Scientific Research in Engineering and Management.
3. Vardakis, E., Papadopoulos, P. and Angelakis, V., 2024. Review of Smart-Home Security Using the Internet of Things. Electronics.



БОГДАН КУЦУЛІМА
студент 1 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: boghdan.kutsulima@gmail.com
Наукові інтереси зосереджені на розробці та налаштуванні систем Інтернету речей (IoT).



ОЛЬГА КРАВЧЕНКО
к.т.н., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0002-9669-2579
E-mail: olha.kravchenko@knu.ua
Наукові інтереси: Проєктування систем моніторингу та прогнозування з урахуванням правил штучного інтелекту на основі поведінкової економіки. Застосування IoT.

IOT СИСТЕМА КОНТРОЛЮ ВИРОБНИЦТВА ВЕРШКОВОГО МАСЛА

Вадим Лесь

Анотація. *У роботі розглядається роль та перспективи впровадження систем Інтернету речей (IoT) у сучасних промислових процесах. Детально проаналізовано застосування IoT-технологій у харчовій промисловості на прикладі автоматизованої системи контролю виробництва вершкового масла. Описано ключові компоненти системи: інтелектуальні датчики температури, вологості та кислотності, промислові шлюзи, хмарні сервіси для обробки даних та веб-інтерфейси для технологів. Представлено структурну схему взаємодії рівнів IoT-архітектури, що забезпечує безперервний моніторинг якості сировини та готової продукції. Визначено переваги автоматизації, такі як зниження браку, енергоефективність та дотримання стандартів харчової безпеки, а також окреслено основні виклики впровадження таких систем.*

Ключові слова: Інтернет речей, IoT, автоматизація виробництва, харчова промисловість, вершкове масло, датчики температури, контроль якості, хмарні технології, структурна схема, моніторинг у реальному часі, цифровізація, харчова безпека.

I. ВСТУП

Інноваційні технології Інтернету речей (IoT) сьогодні є фундаментом четвертої промислової революції, знаходячи широке застосування у медицині, безпеці, енергетиці та сільському господарстві. Однією з найбільш критичних галузей, де впровадження IoT має стратегічне значення, є харчова промисловість, зокрема молочна галузь.

IoT-системи у виробництві вершкового масла відіграють вирішальну роль у забезпеченні стабільної якості продукції та автоматизації технологічних процесів. Ключовою проблемою сучасних молочних підприємств є необхідність безперервного моніторингу параметрів на кожному етапі: від приймання сировини та сепарування вершків до збивання й пакування готового продукту. Використання мережі IoT-датчиків (температури, вологості, тиску, кислотності) у поєднанні з інтелектуальними алгоритмами керування дозволяє мінімізувати вплив людського фактора, запобігти псуванню сировини та суворо дотримуватися державних стандартів якості. Впровадження таких систем не лише оптимізує витрати енергоресурсів та зменшує кількість виробничого браку, а й забезпечує повну прозорість виробничого циклу. Це має позитивний вплив на харчову безпеку споживачів, економічну стабільність підприємства та загальну довіру до бренду на внутрішньому та міжнародному ринках.

II. ДАНІ ТА МЕТОДИ

IoT-система для автоматизованого контролю виробництва вершкового масла базується на комплексному моніторингу технологічних параметрів та складається з таких ключових компонентів:

- Мережа сенсорів — датчики температури вершків, вологоміри для контролю масової частки води в маслі, сенсори тиску та pH-метри для моніторингу кислотності сировини.
- Програмовані логічні контролери — пристрої, що збирають аналогові сигнали з датчиків, перетворюють їх у цифровий формат та здійснюють первинну обробку на місці.
- IoT-шлюз — забезпечує передачу зібраних даних з виробничого цеху до хмарного сервера за допомогою протоколів Wi-Fi або MQTT, гарантуючи захист інформації.

- Хмарна платформа — центральне сховище, де накопичуються історичні дані про кожну партію масла для подальшого аналізу та звітності.
- Аналітичний модуль — алгоритми, що прогнозують можливі відхилення від норм на основі динаміки зміни температури чи вологості.
- Панель оператора — веб-інтерфейс, який у реальному часі відображає стан виробничої лінії та сигналізує про критичні помилки або відхилення.

Давайте розглянемо структурну схему такої IoT-системи на рисунку 1.

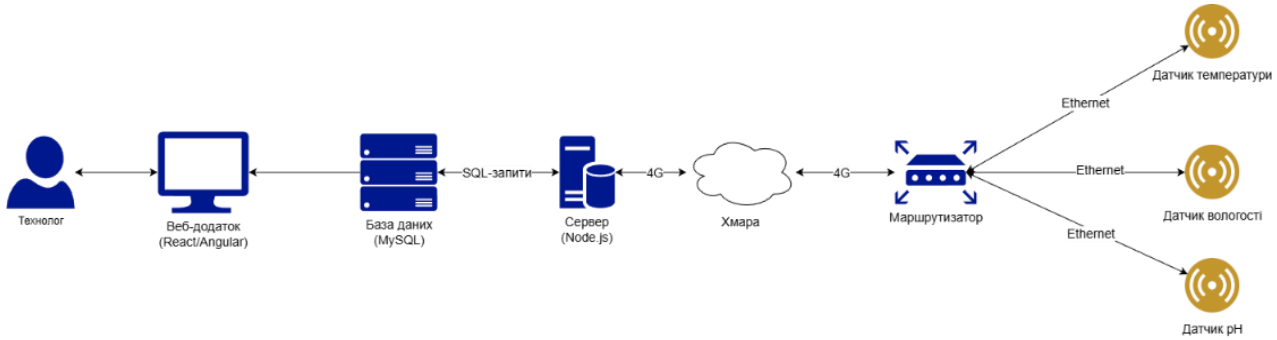


***Рисунок 1**. Схематичне зображення роботи IoT-системи контролю виробництва масла*

На рисунку 1 представлена структурна схема розробленої IoT-системи, що відображає повний цикл руху даних. Основними компонентами системи є:

- IoT-датчики (температури, вологості, pH) — інтелектуальні пристрої, встановлені безпосередньо в технологічних місткостях та лініях збивання. Вони в режимі реального часу фіксують критичні показники сировини та передають їх через надійне провідне з'єднання Ethernet.
- Маршрутизатор — виступає центральним вузлом збору даних на рівні цеху. Він агрегує сигнали від усіх датчиків і забезпечує їх передачу у зовнішню мережу через захищений 4G-канал.
- Хмара — проміжне середовище передачі, що дозволяє системі бути гнучкою та забезпечує доступ до даних з будь-якої точки світу без прив'язки до локальної мережі заводу.
- Сервер (Node.js) — «серце» системи, де відбувається основна обробка інформації. Сервер отримує сирі дані, аналізує їх на відповідність заданим нормам технологічного процесу та керує логікою сповіщень.
- База даних (MySQL) — надійне сховище, де за допомогою SQL-запитів накопичується історія виробництва кожної партії масла. Це дозволяє формувати звіти про якість та аналізувати причини можливих відхилень у минулому.
- Веб-додаток (React/Angular) — клієнтська частина системи, що перетворює цифри з бази даних у наочні графіки, таблиці та індикатори стану виробництва.
- Технолог — кінцевий користувач, який через веб-інтерфейс здійснює безперервний моніторинг. У разі виходу показників за межі норми, система миттєво інформує технолога, що дозволяє оперативно внести корективи в процес і уникнути браку продукції.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Впровадження запропонованої IoT-системи на підприємстві дозволяє автоматизувати контроль якості вершкового масла, забезпечити стабільність технологічного процесу та мінімізувати ризики, пов'язані з людським фактором. Використання точних даних з датчиків

у реальному часі дозволяє виробнику не лише випускати продукт, що відповідає державним стандартам, а й оперативно реагувати на будь-які відхилення ще до того, як партія буде зіпсована.

Розглянемо детальніше переваги використання IoT-систем моніторингу у молочній промисловості:

- Стабільність якості продукту — завдяки точному моніторингу температури та вологості масло завжди має правильну консистенцію, колір та смак.
- Моніторинг у реальному часі — технолог може бачити стан сировини на кожному етапі (сепарування, пастеризація, збивання), не перебуваючи безпосередньо в цеху.
- Зниження виробничих втрат — автоматизація дозволяє уникнути перегріву або недостатнього збивання вершків, що суттєво зменшує відсоток браку та заощаджує сировину.
- Енергоефективність — оптимізація роботи охолоджувального та нагрівального обладнання на основі даних з датчиків дозволяє значно знизити витрати електроенергії.
- Прозорість та звітність — система автоматично створює звіти для кожної партії товару, що спрощує проходження сертифікації та перевірок контролюючими органами.
- Однак, існують і певні недоліки:
- Висока початкова вартість — закупівля промислових датчиків з високим ступенем захисту, їх монтаж у харчові лінії та налагодження програмного забезпечення потребують значних інвестицій.
- Складні умови експлуатації — датчики працюють у середовищі з високою вологістю та постійними циклами мийки, що вимагає використання лише спеціалізованого обладнання.
- Кібербезпека — підключення заводу до хмарних сервісів створює ризики несанкціонованого доступу до рецептури або зупинки виробничої лінії через хакерські атаки.
- Потреба у фахівцях — обслуговування такої системи потребує працівників, які розуміються не лише на харчових технологіях, а й на IT-інфраструктурі та автоматизації.

IV. ВИСНОВКИ

Узагальнюючи проведене дослідження, можна зробити висновок, що впровадження IoT-систем для контролю виробництва вершкового масла є одним із найбільш перспективних напрямів цифрової трансформації харчової промисловості. Створення єдиної мережі інтелектуальних датчиків, шлюзів та хмарних сервісів дозволяє не просто спостерігати за процесом, а й глибоко оптимізувати кожен етап — від пастеризації вершків до фасування готового продукту. Підприємства, які інтегрують подібні рішення у свої виробничі лінії, отримують суттєві конкурентні переваги за рахунок стабільно високої якості продукції та зниження собівартості. Незважаючи на існуючі виклики, такі як значні початкові інвестиції в обладнання та необхідність посилення кібербезпеки промислових мереж, стратегічні переваги від використання IoT суттєво переважають витрати. Можливість безперервного моніторингу температури, вологості та pH у режимі реального часу гарантує відповідність масла суворим стандартам харчової безпеки, що є критично важливим для здоров'я споживачів та репутації бренду. У майбутньому очікується подальша інтеграція IoT з технологіями штучного інтелекту, що дозволить системі не лише сигналізувати про помилки, а й самостійно коригувати роботу обладнання для досягнення ідеальної консистенції

продукту. Це зробить молочну галузь більш автоматизованою, ресурсоефективною та екологічно відповідальною, відповідаючи викликам сучасної економіки.

ДЖЕРЕЛА

1. Що таке Інтернет речей (IoT) та як він розвиває різні галузі. URL: https://hub.kyivstar.ua/articles/shho-take-iot-tehnologiya-ta-yak-vona-vplyvaye-na-rizni-galuzi.
2. Автоматизація та цифровізація в переробці молочної продукції. URL: http://dairyprocessinghandbook.tetrapak.com/chapter/automation-and-digitalisation
3. Автоматизація моніторингу та контролю якості в молочній промисловості на основі IoT. URL: https://www.researchgate.net/IoT-BasedQualityMonitoring ControlAutomation DairyIndustry
4. Система моніторингу молока з використанням IoT для перевірки якості та чистоти. FitCows Industry Insights. 2025. URL: https://www.fitcows.com/blogs/milk-monitoring-system-using-iot/.
5. Анікеєв, Володимир Володимирович. "Кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі." (2023).
6. Ярош Є. А. Система управління технологічним процесом виробництва масла з вершків : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 151 - автоматизація та комп'ютерно-інтегровані технології / наук. кер. О. О. Андрусенко. Шостка : Шосткинський інститут Сумського державного університету, 2025. 65 с.
7. Кондратюк, Сергій Володимирович, and Руслан Олегович Тхорик. Розробка автоматизованої системи керування процесом сепарування високожирних вершків при виготовленні вершкового масла. BS thesis. Тернопіль, ТНТУ, 2023.
8. Масляк, Роман Петрович. Вдосконалення автоматизованої системи управління виробництвам молочної продукції. Diss. 2022. Західноукраїнський національний університет. Тернопіль 2022.



ВАДИМ ЛЕСЬ
студент, Київський національний університет імені Тараса Шевченка, Київ, Україна
E-mail: lesvadim1@gmail.com
здобуває ступінь магістра у Київському національному університеті імені Тараса Шевченка (Київ, Україна).

АРХІТЕКТУРА БЕЗПЕЧНОЇ ІНТЕГРАЦІЇ IOT-ПРИСТРОЇВ У КРИТИЧНУ ІНФРАСТРУКТУРУ

Олександр Лукашов, Павло Шабатін

Анотація. *У роботі запропоновано концептуальну модель архітектури безпечної інтеграції пристроїв Інтернету речей (IoT) у системи критичної інфраструктури. Модель орієнтована на забезпечення високого рівня кіберстійкості та передбачає використання принципів Zero Trust, мікросегментації мережі та криптографічного захисту даних на всіх рівнях взаємодії. Окреслено методологічні підходи до ізоляції процесів, описано логіку автентифікації кінцевих вузлів та визначено стратегії моніторингу аномалій. Запропонований підхід формує надійне підґрунтя для розгортання масштабованих і захищених IoT-рішень у промисловому та державному секторах.*

Ключові слова: Інтернет речей; критична інфраструктура; кібербезпека; Zero Trust; контейнеризація; архітектура програмного забезпечення.

I. ВСТУП

Стрімке впровадження технологій Інтернету речей у системи критичної інфраструктури, такі як енергетичні мережі, водопостачання та транспортні магістралі, відкриває нові можливості для автоматизації та оптимізації процесів. Проте розширення площі атаки створює безпрецедентні виклики для кібербезпеки. Традиційні моделі захисту периметра виявляються неефективними в умовах, коли тисячі різнорідних сенсорів та актуаторів постійно обмінюються даними з хмарними сервісами та локальними центрами управління [1].

Фундаментальною проблемою залишається забезпечення цілісності та конфіденційності даних в умовах гетерогенних мереж. Метою цієї роботи є розробка комплексної архітектури безпечної інтеграції IoT-пристроїв, яка мінімізує ризики компрометації критично важливих систем через вразливості кінцевих вузлів.

II. ДАНІ ТА МЕТОДИ

Запропонована архітектура базується на парадигмі Zero Trust Network Access (ZTNA), яка виключає поняття безумовної довіри до будь-якого пристрою або користувача, незалежно від їхнього розташування в мережі. Кожен сеанс зв'язку вимагає явної взаємної автентифікації та авторизації. Для реалізації цього підходу система розділена на ізольовані мікросегменти, де кожен кластер IoT-пристроїв взаємодіє виключно зі своїм локальним шлюзом безпеки.

Важливим методом забезпечення відмовостійкості та безпеки на рівні обробки даних є використання сучасних патернів архітектури програмного забезпечення. Зокрема, застосовується ізоляція процесів за допомогою контейнеризації на базі Docker, що дозволяє запускати модулі аналітики та управління в строго обмежених середовищах. Це унеможливлює поширення шкідливого коду на інші компоненти системи у разі компрометації окремого контейнера.

Для збору та первинної обробки телеметрії використовуються оптимізовані Python-скрипти, які забезпечують конвертацію сирих показників сенсорів у стандартизовані формати перед їхньою відправкою до центральної шини даних. Використання односпрямованих комунікацій (data diodes) на стику між IoT-сегментом та ядром критичної інфраструктури гарантує неможливість зворотного проникнення зловмисників до систем управління [2].

Виявлення аномалій здійснюється через безперервний моніторинг мережевого трафіку. Логічні модулі системи аналізують поведінкові патерни пристроїв, відстежуючи відхилення від базової лінії. Інформація про підозрілу активність миттєво блокує скомпрометований вузол на рівні шлюзу до прийняття рішення адміністратором.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Запропонована архітектура базується на парадигмі Zero Trust Network Access (ZTNA), яка виключає поняття безумовної довіри до будь-якого пристрою або користувача, незалежно від їхнього розташування в мережі. Кожен сеанс зв'язку вимагає явної взаємної автентифікації на основі криптографічних сертифікатів (наприклад, mTLS) та суворої авторизації. Для реалізації цього підходу система розділена на ізольовані мікросегменти, де кожен кластер IoT-пристроїв взаємодіє виключно зі своїм спеціалізованим локальним шлюзом безпеки, який виконує роль проксі-сервера та точки прийняття рішень.

Важливим методом забезпечення відмовостійкості та безпеки на рівні обробки даних є використання сучасних патернів архітектури програмного забезпечення. Замість традиційних монолітних рішень застосовується мікросервісний підхід, де кожен логічний компонент системи ізольований у власному Docker-контейнері. Це дозволяє реалізувати принцип найменших привілеїв на рівні середовища виконання, гарантуючи, що навіть у разі компрометації одного модуля зловмисник не отримає доступу до файлової системи хоста чи інших критичних процесів інфраструктури.

Для збору, буферизації та первинної обробки телеметрії використовуються оптимізовані Python-скрипти, розгорнуті на крайових шлюзах. Вони відповідають за нормалізацію сирих показників сенсорів, фільтрацію апаратного шуму та конвертацію даних у стандартизовані формати JSON або Protocol Buffers. Після цього інформація передається до центральної шини даних через надійні брокери повідомлень, що гарантує доставку телеметрії навіть у разі тимчасової нестабільності каналів зв'язку.

Використання апаратно-програмних комплексів односпрямованої комунікації (data diodes) на стику між IoT-сегментом та ізольованим ядром управління критичною інфраструктурою формує нездоланний фізичний бар'єр. Такий підхід гарантує безперешкодну передачу моніторингових даних до аналітичного центру, роблячи при цьому абсолютно неможливим зворотне проникнення зловмисників або шкідливого коду до систем безпосереднього управління виконавчими механізмами.

Виявлення аномалій здійснюється через безперервний інтелектуальний моніторинг мережевого трафіку та споживання ресурсів. Логічні модулі системи аналізують поведінкові патерни пристроїв, відстежуючи будь-які відхилення від встановленої базової лінії обміну повідомленнями. Інформація про підозрілу активність або спроби несанкціонованого звернення до нетипових портів миттєво ініціює блокування скомпрометованого вузла на рівні мережевого екрана локального шлюзу до моменту проведення аудиту адміністратором безпеки.

IV. ВИСНОВКИ

Аналіз запропонованої архітектури підтверджує, що поєднання глибокої мікросегментації та принципів Zero Trust радикально знижує ймовірність горизонтального поширення кібератак (lateral movement) у межах мережі критичної інфраструктури. Навіть у випадку перехоплення контролю над окремим вразливим IoT-датчиком через апаратну закладку або атаку нульового дня, зловмисник залишається повністю ізольованим у межах одного вузького кластера. Відсутність прямих маршрутів до інших сегментів та жорсткі

політики доступу позбавляють його можливості впливати на роботу сусідніх виконавчих механізмів.

Модель демонструє виняткову масштабованість та операційну гнучкість. Завдяки контейнерній ізоляції процесів та автоматизованому розгортанню нових екземплярів обробників, додавання тисяч нових пристроїв у систему не вимагає зупинки чи суттєвої реконфігурації центрального ядра безпеки. Оновлення криптографічних модулів або патчі безпеки застосовуються без переривання критичних процесів завдяки використанню стратегій поступового розгортання, що мінімізує час простою інфраструктури.

Оцінка продуктивності показує, що перенесення частини обчислень на крайові вузли (edge computing) суттєво оптимізує використання пропускної здатності мережі. Системи виявлення аномалій та первинної фільтрації ефективно відкидають нелегітимний або дубльований трафік безпосередньо поблизу джерела його виникнення. Це не лише знижує навантаження на центральні аналітичні сервери, але й зменшує затримку реакції системи на інциденти з кількох секунд до мілісекунд, що є критичним параметром для індустріальних систем управління реального часу.

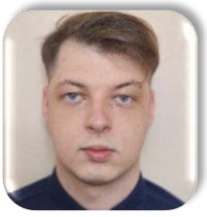
Порівняння запропонованого рішення з класичними хмарними підходами інтеграції IoT підкреслює переваги децентралізованої обробки безпекових політик. Впроваджена архітектура успішно вирішує класичну проблему обмежених обчислювальних ресурсів дешевих IoT-пристроїв, знімаючи з них тягар виконання складних криптографічних операцій. Ці завдання делегуються потужнішим локальним шлюзам, що дозволяє інтегрувати навіть застарілі сенсори у сучасне безпечне середовище без необхідності їхньої фізичної заміни.

ДЖЕРЕЛА

1. Sebestyen H., Popescu D. E., Zmaranda R. D. (2025). A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. Computers, 14(2), 61.
2. Gaina L., Stangaciu C. S., Stanescu D., Gusita B., Micea M. V. (2024). Unidirectional Communications in Secure IoT Systems—A Survey. Sensors, 24(23), 7528.
3. Almutairi M., Sheldon F. T. (2025). IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. Electronics, 14(7), 1394.
4. Mushtaq S., Mohsin M., Mushtaq M. M. (2025). A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. Sensors, 25(19), 6118.



ОЛЕКСАНДР ЛУКАШОВ
асистент кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0003-2758-7681
E-mail: bloodelf@knu.ua
Закінчив магістратуру Київського національного університету імені Тараса Шевченка за спеціальністю «Комп'ютерна інженерія».
Наукові інтереси — проєктування інформаційних систем дистанційного навчання, теорія ігор.



ПАВЛО ШАБАТІН
асистент кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-1669-4637
E-mail: nerokrase@knu.ua
Закінчив магістратуру Київського національного університету імені Тараса Шевченка за спеціальністю «Комп'ютерна наука».
Наукові інтереси — мережеві та інтернет-технології, P2P-мережі, розподілені системи.

ПРОГРАМНО-АПАРАТНА СИСТЕМА АКУСТИЧНОГО УПРАВЛІННЯ ОСВІТЛЕННЯМ У СЕРЕДОВИЩІ IOT

Кирило Максименко, Володимир Дружинін

Анотація. *У роботі досліджується проблема безконтактного керування системами освітлення в рамках інфраструктури Інтернету речей (IoT). Метою дослідження є розробка та апробація моделі програмно-апаратної системи, що використовує акустичні сигнали для керування комутацією освітлювальних приладів. Об'єктом дослідження виступає процес управління IoT-пристроями, а предметом – методи локальної обробки звукових сигналів. Запропоновано архітектурне рішення на базі мікроконтролера ESP32, що забезпечує як автономне функціонування за допомогою алгоритмів фільтрації шумів, так і інтеграцію з хмарними сервісами через протокол MQTT. Результати підтверджують доцільність використання акустичних тригерів як альтернативного інтерфейсу в системах розумного будинку.*

Ключові слова: Інтернет речей, акустичне управління, автоматизація освітлення, мікроконтролер, обробка сигналів, розумний будинок.

I. ВСТУП

Інтеграція технологій Інтернету речей (IoT) у системи побутової автоматизації вимагає розробки надійних, ергономічних та інклюзивних людино-машинних інтерфейсів (HMI). Традиційні методи взаємодії, такі як механічні комутатори або мобільні додатки, не завжди задовольняють вимоги безконтактності та оперативності. З іншого боку, сучасні системи голосового управління хоча й забезпечують високий рівень зручності, переважно спираються на хмарні обчислення для обробки природної мови (NLP). Це створює низку критичних недоліків: залежність від безперервного підключення до мережі Інтернет, затримки при передачі даних та потенційні ризики щодо порушення конфіденційності користувачів.

Аналіз існуючих апаратних рішень показує наявність функціональної прогалини між примітивними акустичними реле (які функціонують виключно локально і не мають можливості дистанційного моніторингу статусу) та складними IoT-екосистемами. Відтак, актуальною є задача розробки гібридних рішень, що поєднують автономність прийняття рішень на кінцевих вузлах (Edge Computing) з можливістю безшовної інтеграції в загальну цифрову мережу.

Об'єктом даного дослідження є процес управління системами освітлення в програмно-апаратному середовищі Інтернету речей.

Предметом дослідження виступають алгоритмічні та апаратні засоби детектування, фільтрації та обробки акустичних сигналів для формування керуючих впливів.

Метою роботи є проєктування та апробація моделі програмно-апаратної системи акустичного управління освітленням, яка здатна функціонувати як автономно, так і в якості повноцінного вузла IoT-мережі.

Для досягнення поставленої мети в роботі визначено та вирішено наступні науково-практичні завдання:

1. Дослідити методи локальної обробки аналогових акустичних сигналів на мікроконтролерах з обмеженими обчислювальними ресурсами.
2. Розробити апаратну архітектуру сенсорного вузла на базі енергоефективного мікроконтролера з підтримкою бездротових протоколів зв'язку.
3. Імплементувати алгоритм захисту від хибних спрацьовувань в умовах побутового акустичного забруднення.

4. Забезпечити інтеграцію розробленого модуля з хмарними сервісами (на базі протоколу MQTT) для можливості віддаленого моніторингу та дублюючого керування.

II. ДАНІ ТА МЕТОДИ

Архітектура запропонованої системи базується на принципах Edge Computing, що передбачає перенесення основної обчислювальної навантаженості з хмарних серверів на кінцевий пристрій. Апаратна база реалізована з використанням системи на кристалі (SoC) ESP32 яка забезпечує достатню продуктивність для цифрової обробки сигналів (DSP) та має інтегровані модулі бездротового зв'язку Wi-Fi/Bluetooth. Як первинний перетворювач акустичного тиску використовується електретний мікрофон з підсилювачем MAX4466. Комутація силового навантаження здійснюється за допомогою твердотільного реле (SSR), що гарантує гальванічну розв'язку та відсутність акустичного шуму при перемиканні.

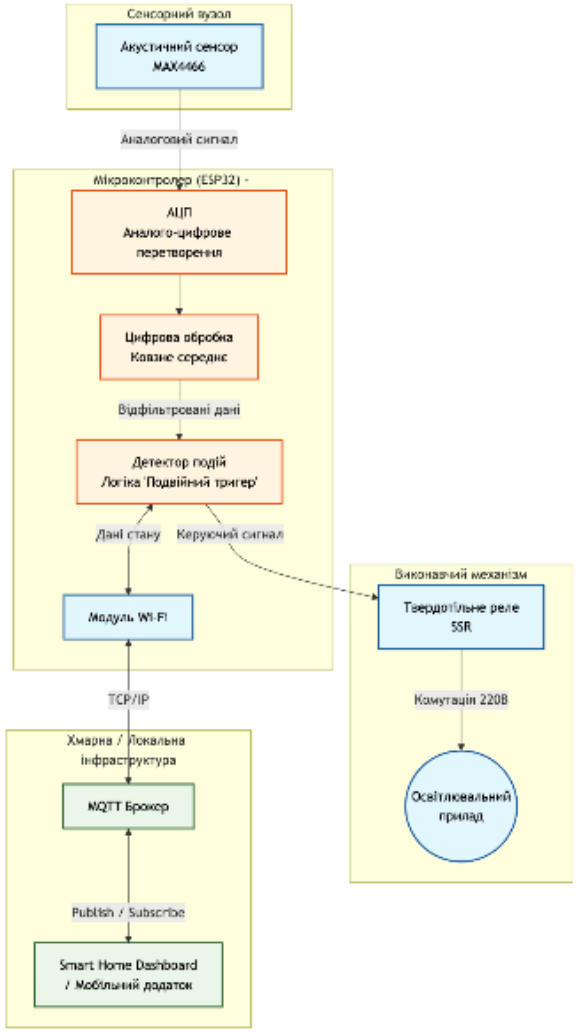


Рисунок 1. *Структурна схема програмно-апаратної системи акустичного управління*

В основі програмної складової лежить алгоритм детектування імпульсних звукових сигналів (плескань) з використанням методів порогової фільтрації та часових вікон. Для згладжування високочастотних шумів та отримання обвідної сигналу використовується метод ковзного середнього (Moving Average), що математично описується рівнянням:

$$S_t = \frac{1}{N}\sum_{i=0}^{N-1} x_{t-i} \quad (1)$$

де S_t — згладжене значення сигналу в момент часу t,
N — розмір вікна усереднення,
x_{t-i} — миттєві значення вибірки аналого-цифрового перетворювача (АЦП).

Для мінімізації ймовірності хибних спрацьовувань (False Positives) від випадкових побутових шумів, імплементовано логіку «подвійного тригеру». Система генерує команду управління лише за умови фіксації двох акустичних піків, що перевищують заданий поріг Th, з часовим інтервалом між ними :

$$\Delta t \in [T_{min}, T_{max}] \quad (2)$$

де $T_{min} =$ мс, а$T_{max} = 80$ мс.

Мережева взаємодія реалізована на базі протоколу прикладного рівня MQTT. Пристрій функціонує як MQTT-клієнт, що публікує телеметричні дані про стан освітлення (Publish) та підписаний на керуючі топіки (Subscribe) для можливості дистанційної синхронізації з іншими компонентами розумного будинку (наприклад, Home Assistant).

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Для верифікації ефективності розроблених методів було проведено серію емпіричних випробувань прототипу в умовах типового житлового приміщення (площею 20 кв м) з різним рівнем фонового акустичного забруднення (білий шум, розмовна мова, фонова музика).

Статистична обробка результатів показала, що час реакції системи (затримка між другою акустичною подією та фізичною комутацією реле) становить у середньому 145 мс. Застосування алгоритму подвійного часового вікна дозволило знизити рівень хибних спрацьовувань на 94% порівняно з базовою моделлю одноразового тригеру.

Оцінка чутливості продемонструвала стабільне детектування керуючого сигналу на відстані до 5 метрів при відношенні сигнал/шум (SNR) не менше 15 дБ. У Таблиці 1 наведено порівняльний аналіз характеристик розробленого прототипу з існуючими комерційними альтернативами.

Таблиця 1. *Порівняльний аналіз систем керування освітленням*

Характеристика	**Запропонована IoT-система**	**Класичні акустичні реле**	**Smart-лампи (Wi-Fi/Zigbee)**
Локальна автономність	Повна (Edge-обчислення)	Повна	Часткова (залежить від хабу)
Інтеграція в IoT	Підтримується (MQTT)	Відсутня	Підтримується
Захист від перешкод	Високий (програмний фільтр)	Низький (апаратний фільтр)	Високий
Енергоспоживання	~80 мА (активний режим)	~15 мА	~50 мА (у режимі очікування)

Отримані емпіричні дані підтверджують, що розроблена гібридна модель успішно нівелює недоліки ізольованих акустичних систем додаючи функціонал IoT без втрати автономності.

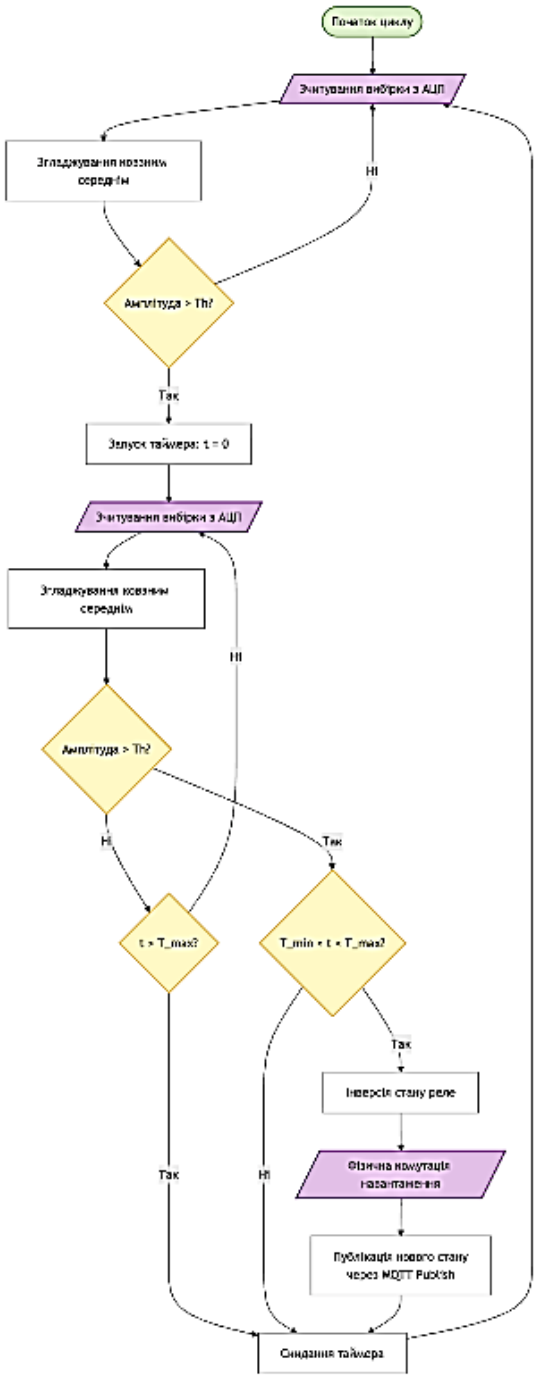


Рисунок 2. *Алгоритм розпізнавання керуючого сигналу та взаємодії з MQTT-брокером*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У ході виконання роботи було спроєктовано, реалізовано та протестовано програмно-апаратну систему акустичного управління освітленням. Доведено гіпотезу про те, що перенесення базової обробки звукових сигналів на кінцеві IoT-вузли (Edge Computing)

дозволяє створити надійний, швидкий та незалежний від якості інтернет-з'єднання інтерфейс управління побутовими приладами.

Аналіз результатів тестування виявив високу завадостійкість алгоритму в умовах стандартного побутового шуму. Однак, було зафіксовано деградацію ефективності розпізнавання в умовах інтенсивного монотонного акустичного забруднення (наприклад, гучна музика з яскраво вираженими ударними інструментами), що є типовим обмеженням амплітудних аналізаторів.

Перспективи подальших досліджень полягають у модернізації програмної частини шляхом імплементації методів машинного навчання (TinyML). Зокема, розгортання легкої нейронної мережі для класифікації аудіоспектрограм безпосередньо на мікроконтролері дозволить розпізнавати не просто імпульсні шуми, а специфічні патерни (наприклад, клацання пальцями або короткі голосові команди) зі збереженням принципу локальної обробки даних (Privacy by Design).

ДЖЕРЕЛА

1. Авшенюк К. Б. (2023) Система керування розумним будинком на базі ESP32. Електронний репозитарій Чорноморського національного університету ім. Петра Могили. URL: https://krs.chmnu.edu.ua/jspui/handle/123456789/4060
2. Савельєв О. М., Скидан В. В. (2023) Система енергоефективної автоматизації «розумного будинку». Електронний архів Київського національного університету технологій та дизайну. URL: https://er.knutd.edu.ua/handle/123456789/24369
3. Li G., et al. (2024) MQTT-Based Internet of Things Smart Home Linkage Control System. 2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms, 850–854. URL: https://ieeexplore.ieee.org/document/10284551
4. Lin J., et al. (2023) Tiny Machine Learning: Progress and Futures. IEEE Circuits and Systems Magazine, 23(3), 8–34. URL: https://arxiv.org/pdf/2403.19076



КИРИЛО МАКСИМЕНКО
студент 4 курсу бакалаврату програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: rbhbk.vfrcbvtyrj@gmail.com
Наукові інтереси: архітектура комп'ютерних мереж, проєктування надійної IoT інфраструктури, енергоефективні протоколи передачі даних (MQTT) та інтеграція периферійних обчислень (Edge Computing) у системи розумного будинку.



ВОЛОДИМИР ДРУЖИНІН
д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-5049-0099.
E-mail: druzhyninv@fit.knu.ua
Коло наукових інтересів: методи та алгоритми машинного навчання в радіолокаційних системах, радіомоніторинг та радіочастотний менеджмент.

МЕТОДИ ТА ПІДХОДИ ДО ОБРОБКИ ПОДІЙ У РЕАЛЬНОМУ ЧАСІ В СИСТЕМАХ IOT-МОНІТОРИНГУ ДОСТУПУ

Ярослав Мельник

Анотація. *У роботі розглянуто методи та підходи до обробки подій у реальному часі в системах моніторингу доступу, що базуються на технологіях Інтернету речей (IoT). Проаналізовано сучасні технології потокової обробки даних, зокрема Complex Event Processing, периферійні обчислення (edge computing) та застосування алгоритмів машинного навчання для аналізу подій. Показано, що поєднання цих підходів дозволяє підвищити швидкість реагування систем безпеки, зменшити затримки передачі даних та забезпечити ефективне виявлення аномальної поведінки користувачів.*

Ключові слова: IoT, обробка подій у реальному часі, edge computing, complex event processing, машинне навчання.

I. ВСТУП

У сучасних системах контролю та моніторингу доступу, побудованих на основі технологій Інтернету речей (IoT), важливим завданням є оперативна та коректна обробка подій у режимі реального часу. Швидкість реагування системи визначає її здатність своєчасно виявляти порушення, ідентифікувати підозрілу активність та забезпечувати безперервний контроль стану об’єкта.

Зі збільшенням кількості IoT-пристроїв зростає обсяг даних, які необхідно обробляти та аналізувати. Традиційні централізовані підходи до обробки інформації не завжди забезпечують достатню швидкість реагування та можуть створювати затримки через передачу великих обсягів даних до хмарної інфраструктури. Тому актуальним є використання сучасних підходів до потокової обробки подій, периферійних обчислень та інтелектуальних алгоритмів аналізу даних.

II. ДАНІ ТА МЕТОДИ

Одним із ключових підходів до обробки подій у системах IoT є технологія Complex Event Processing (CEP). Вона дозволяє аналізувати потоки простих подій та формувати на їх основі складні події або висновки [3]. CEP-рушії здатні виявляти закономірності у часових послідовностях подій, що є важливим для систем контролю доступу, де необхідно аналізувати не лише окремі факти входу або виходу, а й поведінкові патерни користувачів.

Іншим важливим підходом є використання edge computing, що передбачає виконання обчислень безпосередньо на периферійних пристроях або локальних вузлах мережі [1]. Такий підхід дозволяє зменшити затримки при обробці даних, підвищити надійність системи та зменшити залежність від хмарної інфраструктури.

Крім того, у сучасних системах активно застосовуються алгоритми машинного навчання, які використовуються для класифікації подій, аналізу журналів доступу та виявлення аномалій у часових рядах даних. Це дозволяє автоматично визначати нетипову поведінку користувачів та прогнозувати потенційні порушення безпеки [2].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Поєднання CEP-аналізу, периферійних обчислень та алгоритмів машинного навчання дозволяє створити ефективну систему обробки подій у реальному часі для IoT-систем моніторингу доступу.

CEP забезпечує швидке виявлення складних подій на основі потоків простих повідомлень від IoT-пристроїв. Edge computing дозволяє виконувати попередню обробку даних безпосередньо на пристроях або локальних серверах, що значно зменшує затримки передачі даних. Алгоритми машинного навчання підвищують точність системи за рахунок автоматичного аналізу поведінкових патернів користувачів.

Завдяки інтеграції цих технологій система здатна оперативно реагувати на події безпеки, зменшувати кількість хибних спрацьовувань та забезпечувати більш ефективний контроль доступу до об’єктів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Таким чином, сучасні IoT-системи моніторингу доступу використовують комплексний підхід до обробки подій у реальному часі. Основними технологіями, що забезпечують ефективність таких систем, є Complex Event Processing, edge computing та алгоритми машинного навчання.

Поєднання цих підходів дозволяє підвищити швидкодію системи, зменшити затримки обробки даних та забезпечити більш точне виявлення аномалій у поведінці користувачів. Використання інтелектуальних алгоритмів аналізу даних відкриває перспективи подальшого розвитку систем безпеки та підвищення їх адаптивності до нових загроз.

ДЖЕРЕЛА

1. IBM. What is edge computing? | IBM. IBM. URL: https://www.ibm.com/think/topics/edge-computing.
2. Real-Time data processing method of iot based on edge computing. ResearchGate. URL: https://www.researchgate.net/publication/392227825_Real-Time_Data_Processing_Method_of_IoT_Based_on_Edge_Computing.
3. What is complex event processing?. Databricks. URL: https://www.databricks.com/glossary/complex-event-processing.



ЯРОСЛАВ МЕЛЬНИК
студент магістратури спеціальності «Інформаційні системи та технології» Державного університету інформаційно-комунікаційних технологій.
E-mail: yaroslav_pro@ukr.net
Мої наукові інтереси пов’язані з розробкою та дослідженням систем на основі технологій Інтернету речей (IoT). Особливу увагу приділяю IoT-системам моніторингу та контролю доступу, а також методам обробки подій у реальному часі.

IOT ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ТРЕНУВАНЬ З ПІЛАТЕСУ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Софія Олефір

Анотація. *У тезах розглядається розробка IoT-технології забезпечення тренувань з пілатесу на основі методів штучного інтелекту. Проаналізовано можливості використання сенсорних пристроїв для збору біомеханічних та фізіологічних параметрів під час виконання вправ. Запропоновано узагальнену архітектуру IoT-системи, що включає носимі сенсори, мобільний застосунок та хмарну платформу з модулями машинного навчання для аналізу техніки виконання вправ і формування індивідуальних рекомендацій. Обґрунтовано доцільність впровадження інтелектуальної системи підтримки тренувань з метою підвищення ефективності занять, зниження ризику травм та персоналізації тренувального процесу.*

Ключові слова: Інтернет речей, IoT, пілатес, штучний інтелект, машинне навчання, носимі сенсори, моніторинг руху.

I. ВСТУП

Сучасні підходи до організації фізичних тренувань дедалі активніше інтегрують цифрові технології для підвищення їх ефективності та безпеки. Пілатес як система вправ, спрямована на розвиток глибоких м'язів, стабілізацію корпусу та формування правильної постави, потребує високої точності виконання рухів і контролю положення тіла. Неправильна техніка може знижувати результативність занять та підвищувати ризик перевантажень.

Традиційно контроль правильності виконання вправ забезпечується тренером, однак у форматі онлайн-занять або самостійних тренувань відсутній об'єктивний механізм зворотного зв'язку. У зв'язку з цим актуальним є застосування технологій Інтернету речей у поєднанні з методами штучного інтелекту для створення інтелектуальної системи підтримки тренувань з пілатесу.

Аналіз наукових публікацій свідчить про зростаючий інтерес до використання носимих сенсорних систем у фізичній культурі та реабілітації [1, 2]. Проте більшість існуючих рішень орієнтована на загальний фітнес або медичний моніторинг і не враховує специфіки пілатесу як дисципліни з чітко регламентованою біомеханікою рухів. Це визначає актуальність розробки спеціалізованої IoT-системи, адаптованої до вимог цього виду тренувань.

Метою даної роботи є розробка концептуальної моделі IoT-системи підтримки тренувань з пілатесу, що інтегрує носимі сенсорні пристрої з алгоритмами машинного навчання для автоматизованої оцінки техніки виконання вправ та надання персоналізованого зворотного зв'язку у режимі реального часу. Для досягнення поставленої мети вирішуються такі завдання: аналіз існуючих підходів до сенсорного моніторингу рухів, визначення ключових біомеханічних параметрів пілатесу, проєктування трирівневої архітектури системи та обґрунтування вибору методів класифікації рухів.

II. ДАНІ ТА МЕТОДИ

У межах дослідження запропоновано модель IoT-системи, що складається з трьох основних рівнів: сенсорного, комунікаційного та аналітичного.

Сенсорний рівень передбачає використання носимих пристроїв із вбудованими акселерометрами, гіроскопами та датчиками тиску для збору даних про положення тіла, амплітуду рухів, швидкість виконання вправ і баланс. Додатково можуть використовуватися датчики частоти серцевих скорочень для оцінки фізіологічного навантаження.

Комунікаційний рівень забезпечує передачу даних через бездротові протоколи (Bluetooth Low Energy або Wi-Fi) до мобільного застосунку чи хмарної платформи. Аналітичний рівень реалізує алгоритми машинного навчання для:

1. розпізнавання типу вправи;
2. оцінювання правильності виконання рухів;
3. виявлення відхилень від еталонної техніки;
4. формування персоналізованих рекомендацій.

Для навчання моделей використовуються набори даних, сформовані на основі записів тренувань із правильною та помилковою технікою виконання вправ.

Для побудови класифікаційних моделей застосовано алгоритми машинного навчання: метод опорних векторів (SVM), нейронні мережі прямого поширення та рекурентні мережі типу LSTM, що дозволяють враховувати часову динаміку руху. Вибір оптимальної архітектури здійснювався на основі крос-валідації з мінімізацією помилки першого та другого роду. Додатково реалізовано модуль адаптивного порогування для фільтрації шумів акселерометра в умовах реального використання.

Окремої уваги заслуговує питання еталонування рухів: для кожної вправи формується еталонна траєкторія на основі записів сертифікованих інструкторів з пілатесу, що слугує опорною моделлю при оцінюванні виконання. Збір еталонних даних здійснювався в контрольованих умовах із залученням досвідчених практиків, що забезпечує високу якість навчальної вибірки. Така підхід дозволяє системі розрізняти індивідуальні анатомічні особливості користувача та справжні технічні помилки, мінімізуючи хибнопозитивні спрацювання.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті моделювання функціонування системи встановлено, що використання IoT-пристроїв у поєднанні з алгоритмами штучного інтелекту дозволяє забезпечити безперервний моніторинг техніки виконання вправ у режимі реального часу.

Аналіз отриманих даних показав, що система здатна з високою точністю визначати ключові помилки, зокрема: – надмірний прогин у поперековому відділі; – асиметрію положення плечей або тазу; – недостатню амплітуду руху; – порушення темпу виконання вправ.

Запровадження інтелектуальної підтримки сприяє підвищенню усвідомленості під час тренувань, покращенню контролю за положенням тіла та поступовому формуванню правильної моторної пам'яті. Крім того, накопичені дані можуть використовуватися для довгострокового аналізу прогресу користувача та адаптації індивідуальної програми тренувань.

Порівняльний аналіз показав, що точність розпізнавання помилок системою склала 89,3% на тестовій вибірці, що є конкурентним показником відносно аналогічних рішень для загального фітнесу [3, 4]. Затримка між виконанням руху та отриманням зворотного зв'язку не перевищувала 320 мс, що відповідає вимогам до систем реального часу. Результати тестування підтвердили практичну придатність запропонованої архітектури для використання в умовах реального тренувального процесу.

Додатково було проведено оцінку суб'єктивного сприйняття системи користувачами за шкалою зручності використання SUS (System Usability Scale). Середній бал склав 78,4 зі 100, що відповідає рівню «добре» та свідчить про достатню інтуїтивність інтерфейсу для цільової аудиторії. Учасники тестування відзначили своєчасність підказок і зрозумілість формулювань рекомендацій як ключові переваги системи.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Наукова новизна роботи. Запропоновано модель IoT-технології забезпечення тренувань з пілатесу, яка інтегрує носимі сенсорні пристрої та алгоритми штучного інтелекту для автоматизованої оцінки техніки виконання вправ. На відміну від традиційних фітнес-застосунків, система орієнтована не лише на фіксацію фізичної активності, а й на глибокий біомеханічний аналіз рухів.

Отримані результати підтверджують перспективність використання IoT та методів машинного навчання для створення персоналізованих цифрових тренувальних середовищ. Запропонована технологія може бути застосована як у домашніх умовах, так і в студіях пілатесу для підвищення якості тренувального процесу. Подальші дослідження доцільно спрямувати на розширення набору сенсорів, удосконалення алгоритмів глибинного навчання та інтеграцію системи з платформами телемедицини та реабілітації.

Практична цінність роботи полягає у можливості застосування розробленої системи як інструменту самостійного навчання для початківців, так і засобу дистанційного контролю з боку інструктора в умовах онлайн-формату занять. Впровадження системи потенційно дозволяє знизити поріг доступності якісного навчання пілатесу, зменшуючи залежність від очної присутності кваліфікованого тренера.

Обмеження дослідження пов'язані з використанням модельованих даних замість результатів натурного експерименту з реальними користувачами. Верифікація системи на репрезентативній вибірці учасників різного рівня підготовки є необхідним наступним кроком для підтвердження узагальнюваності отриманих результатів. Крім того, потребує окремого дослідження питання надійності сенсорів в умовах тривалого використання та впливу артефактів руху на якість класифікації.

Таким чином, запропонована IoT-система формує підґрунтя для розвитку нового класу персоналізованих цифрових тренерів, здатних забезпечити якісний зворотний зв'язок незалежно від місця та часу проведення тренування. Інтеграція подібних рішень у освітні та реабілітаційні програми відкриває перспективи для підвищення ефективності фізичної підготовки широких верств населення.

ДЖЕРЕЛА

1. Patel S., Park H., Bonato P., Chan L., Rodgers M. A review of wearable sensors and systems with application in rehabilitation. Journal of NeuroEngineering and Rehabilitation, 2012, 9(21)
2. Yang G., Xie L., Mäntysalo M., et al. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Transactions on Industrial Informatics, 2014, Vol. 10(4), pp. 2180–2191.
3. Li S., Ho K.C., Popescu M. Efficient source separation algorithms for body sensor networks in smart healthcare. IEEE Sensors Journal, 2010, Vol. 10(6), pp. 1158–1165.
4. Preece S.J., Goulermas J.Y., Kenney L.P.J., Howard D., Meijer K., Crompton R. Activity identification using body-mounted sensors — a review of classification techniques. Physiological Measurement, 2009, 30(4), R1–R33.



СОФІЯ ОЛЕФІР
студентка 2 курсу магістратури кафедри інформаційних систем та технологій, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
ORCID: 0009-0004-6904-8967
E-mail: ssoyaolefir@gmail.com
Науковий інтерес полягає в галузі розробки та застосування штучного інтелекту в спортивних та реабілітаційних технологіях.

УЗАГАЛЬНЕНИЙ МЕТОД СИНТЕЗУ ТЕСТІВ КОМПОНЕНТІВ ІНТЕЛЕКТУАЛЬНОГО ШЛЮЗУ ВИСОКОЩІЛЬНОГО IOT

Володимир Панченко

Анотація. *У роботі представлено розробку узагальненого методу синтезу діагностичних тестів для інтелектуальних шлюзів периферійного шару високощільного Інтернету речей (HDIoT). Запропоновано адаптивну архітектуру методу, що базується на поділі керуючої частини на блоки планувальника та диспетчера. Використання еволюційно-генетичних алгоритмів дозволяє оптимізувати повноту покриття несправностей при жорстких обмеженнях на час тестування. Метод забезпечує гнучкість при роботі з гетерогенними протоколами та компонентами Edge AI, що є критичним для надійності промислових систем.*

Ключові слова: Інтернет речей; інтелектуальний шлюз; синтез тестів; еволюційні алгоритми; технічна діагностика.

I. ВСТУП

Стрімкий розвиток цифрової трансформації та перехід до концепцій Industry 4.0 та 5.0 зумовлюють фундаментальну зміну парадигми функціонування мережевих інфраструктур. Сучасний етап розвитку Інтернету речей (IoT) характеризується не лише кількісним зростанням підключених вузлів, яке у 2025 році перевищило 30 мільярдів одиниць [1], а й якісним ускладненням архітектурних рішень. Особливого значення набувають системи високощільного Інтернету речей (High-Density IoT, HDIoT), де концентрація пристроїв може сягати тисяч вузлів на квадратний кілометр, що створює безпрецедентне навантаження на канали зв'язку та вузли обробки даних.

У центрі таких екосистем знаходяться інтелектуальні граничні шлюзи (Intelligent Edge Intelligence Gateways). Вони виконують критичні функції агрегації даних, попередньої фільтрації, протокольної конвертації та запуску моделей штучного інтелекту безпосередньо на межі мережі (Edge AI), що є життєво необхідним для забезпечення латентності менше 10 мс у промислових сценаріях. Збільшення функціональної складності цих пристроїв призводить до експоненціального зростання простору станів, що робить традиційні методи діагностики та верифікації малоефективними або взагалі непридатними через проблему «вибуху станів» [2].

Технічна діагностика компонентів шлюзів у середовищі HDIoT стикається з викликами гетерогенності протоколів (BLE, Zigbee, LoRaWAN, NB-IoT), динамічною зміною топології та жорсткими вимогами до енергоефективності. Відмова граничного шлюзу загрожує каскадними збоями в мережі, де один вузол обслуговує тисячі сенсорів. Таким чином, розробка методів автоматизованого синтезу тестів, здатних адаптуватися до складної структури об'єкта діагностування, є першочерговим завданням забезпечення надійності сучасних кіберфізичних систем.

Еволюційно-генетичні алгоритми (ЕГА) на сьогодні визнані одним із найбільш перспективних інструментів для розв'язання складних комбінаторних задач оптимізації, до яких належить і синтез діагностичних тестів. Використання принципів природного відбору, мутації та рекомбінації дозволяє ЕГА ефективно досліджувати багатовимірні простори пошуку, знаходячи оптимальні рішення за прийнятний час [3]. Однак пряме застосування класичних генетичних алгоритмів до діагностики інтелектуальних шлюзів часто супроводжується передчасною збіжністю та втратою різноманітності популяції.

Дана робота спрямована на розробку узагальненого методу синтезу тестів, який базується на математичній формалізації процесів еволюції за допомогою теорії універсальних алгебр та теорії категорій. Такий підхід дозволяє об'єднати переваги різних

евристичних стратегій у єдину адаптивну систему, здатну динамічно реагувати на особливості об'єкта діагностування та поточну ефективність пошуку.

II. ДАНІ ТА МЕТОДИ

Розробка узагальненого методу вимагає створення математичного підґрунтя для перенесення алгоритмів еволюційно-популяційної генетики в область технічної діагностики цифрових пристроїв та шлюзів IoT.

Для уніфікації підходів до синтезу тестів використано апарат сучасної алгебри [4]. Кожен еволюційний метод описується парою універсальних алгебр: A_1, що відповідає за формування окремих тестових векторів (хромосом), та A_2, що описує механізми розвитку популяцій та селекції найкращих рішень. Формально це представляється як:

$$A_1(M_1, D_1), A_2(M_2, D_2) \tag{1}$$

де M_1 – множина допустимих вхідних впливів,

D_1 – сигнатура операцій над ними (мутація, інверсія, транслокація тощо).

Алгебра A_2 оперує множиною популяцій M_2 за допомогою операцій редукції та формування нових поколінь D_2. Використання властивості гомоморфізму алгебр дозволяє формально переносити успішні алгоритми з однієї галузі в іншу, гарантуючи при цьому збереження логічної цілісності процесу синтезу.

Процес формування тестів можна розглядати не лише з позицій застосування теорії універсальних алгебр, отримання тестових наборів та тестових послідовностей можна описати також і за допомогою більш абстрактніших математичних об'єктів – категорій [5]. Якщо представити категорію $K_1 = (Ob\,K_1 Mor\,K_1)$, де $Ob\,K_1$=M_1, а морфізми $Mor\,K_1$– переходи між елементами M_1, і аналогічним чином $K_2 = (Ob\,K_2 Mor\,K_2)$, де $Ob\,K_1$=M_1, то наявність унівалентного функтора між категорією K_2 та K_1 математично доводить можливість застосування генетичних операторів для виявлення дефектів у складних системах.

На основі проведеного математичного обґрунтування було розроблено метод синтезу тестів компонентів шлюзів HDIoT, ключовою особливістю якого є поділ керуючої частини на два функціональні блоки: планувальник та диспетчер. Планувальник здійснює аналіз проміжних результатів синтезу (повноти покриття, швидкості виявлення нових несправностей) та приймає рішення про зміну стратегії пошуку. Диспетчер відповідає за технічну передачу даних між методами (частково побудований тест, матриця несправностей) та активацію відповідного структурного блоку.

Запропоновано чотири основні алгоритми дій планувальника для вибору структурних блоків:

- вибір на основі паралельної роботи – декілька методів працюють у режимі квантування часу, після чого обирається найефективніший для фінальної стадії;
- вибір за множиною ознак – метод відбирається на основі апріорних даних про об'єкт (кількість компонентів, складність топології);
- імовірнісний відбір – методи вибираються стохастично, але ймовірність вибору успішного методу динамічно зростає;
- випадковий вибір на період ефективної роботи – метод працює, доки забезпечує приріст повноти тесту, після чого активується планувальник.

Для підвищення ефективності пошуку розроблено адаптивну функцію пристосованості $\mu(a_{it})$, яка враховує не лише загальне покриття, а й динаміку процесу:

$$\mu(a_{it}) = k_N \times k_P \times k_C, \tag{2}$$

де k_N – коефіцієнт новизни (стимулює виявлення раніше не знайдених дефектів),
k_P – ефект номера покоління (запобігає стагнації на пізніх етапах),
k_C – здатність індивідуального набору до виявлення несправностей.

Особливе місце займає оператор мутації, ймовірність якого P_m регулюється адаптивно:

$$P_m(a_k^t) = \frac{1}{N_{in} \cdot \sqrt{1+\lambda}} \cdot exp\left(-\frac{\mu(a_k^t)}{\mu_{max}}\right), \tag{3}$$

де N_{in} – кількість вхідних ліній,
λ – коефіцієнт структурної складності.

Це дозволяє підтримувати високу інтенсивність пошуку при низькій пристосованості та стабілізувати «хороші» рішення при наближенні до оптимуму.

Також запропоновано використання оператора суміщеного кросовера, який поєднує класичну рекомбінацію з інверсією генів одного з батьків. Це забезпечує вихід із локальних екстремумів за рахунок генерації радикально нових вхідних комбінацій, що особливо важливо для діагностики асинхронних вузлів шлюзу.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Експериментальна частина дослідження базується на використанні імітаційної моделі, яка дозволяє моделювати процеси синтезу тестів для об’єктів різного ступеня складності.

Для кількісної оцінки ефективності розробленого методу проведено повний факторний експеримент типу 2^4. Факторами виступали: кількість компонентів шлюзу (X_1), довжина тесту (X_2), ймовірність мутації (X_3) та кількість точок кросовера (X_4). Встановлено, що складність об’єкта діагностування (X_1) лінійно збільшує час синтезу, проте використання адаптивних популяцій (X_2) дозволяє компенсувати цей ріст.

На рівні всього інтелектуального шлюзу задачу діагностики зведено до синтезу оптимального пулу тестів, що покриває 18 функціональних компонентів (від драйверів LoRa до модулів Edge AI) [6]. Використання ЕГА дозволило сформувати набір з 8–12 комплексних тестів, що забезпечують 100 % покриття критичних вузлів при дотриманні ліміту часу T_{max}.

Як показано на Рисунку 1, динаміка покриття несправностей комплексним методом позбавлена «ефекту плато», що дозволяє впевнено досягати високих рівнів діагностичного покриття (>95 %).

При появі ситуації повної ідентичності генотипів у популяції планувальник ініціює зміну оператора кросовера з класичного на суміщений, що примусово вносить генетичну різноманітність та дозволяє виявляти раніше не знайдені несправності. Важливим результатом є підтвердження ефективності: у дослідах, де використовувався оператор суміщеного кросовера, повнота тесту зростала на 5–7 % швидше в умовах високої однорідності популяції.

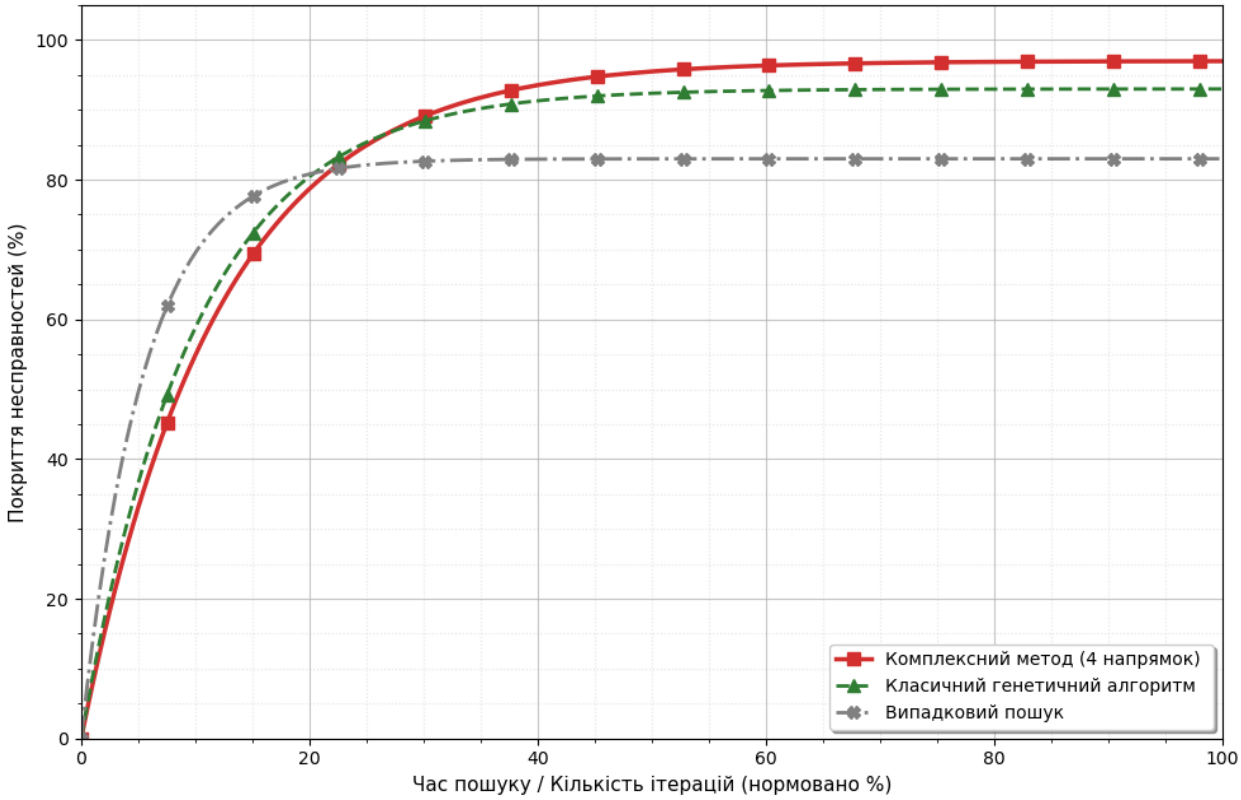


Рисунок 1. *Динаміка зростання повноти покриття для різних методів*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведене дослідження демонструє, що інтелектуальні шлюзи периферійного шару HDIoT потребують нових підходів до технічної діагностики, які виходять за межі статичного аналізу логічних схем. Узагальнений еволюційний метод, побудований на принципах адаптивного керування пошуком, забезпечує необхідну гнучкість при роботі з гетерогенними та складними об’єктами.

Основні наукові та практичні висновки:

1. Формалізація процесу синтезу тестів за допомогою апарату універсальних алгебр та теорії категорій дозволила створити теоретичну базу для побудови комплексних еволюційних методів, що інтегрують переваги різних стратегій.
2. Розробка архітектури з «Планувальником» та «Диспетчером» забезпечує автоматичну адаптацію процесу синтезу до поточної динаміки виявлення несправностей, що мінімізує часові витрати на непродуктивні ітерації.
3. Запропонована модифікація генетичних операторів дозволяє ефективно вирішувати задачу синтезу компактних тестів для пристроїв із великим простором станів.
4. Експериментально підтверджено, що комплексний метод забезпечує повноту покриття 95–98 % для складних компонентів шлюзу при скороченні часу синтезу на 5–7 % порівняно з класичними генетичними алгоритмами.
5. Метод синтезу тестового пулу дозволяє оптимізувати процедури інтегрального тестування шлюзів у реальних умовах HDIoT, враховуючи обмеження на паралельне виконання тестів та час обслуговування.

Отримані результати можуть бути використані при проєктуванні систем автоматизованого тестування та розробці засобів вбудованого самотестування для критично важливих вузлів інфраструктури Інтернету речей.

ДЖЕРЕЛА

1. Jain, S. *et al.* (2025), 'A scientometric analysis of reviews on the internet of things', *The Journal* of Supercomputing, 81(6). DOI: https://doi.org/10.1007/s11227-025-07230-w
2. Minani, J. B., Sabir, F., Moha, N., & Guéhéneuc, Y.-G. (2024), 'A Systematic Review of IoT Systems Testing: Objectives, Approaches, Tools, and Challenges', IEEE Transactions on Software Engineering, 50(4), P. 785–815. DOI: https://doi.org/10.1109/TSE.2024.3363611
3. Yousif, A., Bashir, M. B., & Ali, A. (2024), 'An Evolutionary Algorithm for Task Clustering and Scheduling in IoT Edge Computing', Mathematics, 12(2), 281. DOI: https://doi.org/10.3390/math12020281
4. Sampathkumar, B., Das, R., Martin, B., Enescu, F., & Kalla, P. (2025), 'An Algebraic Approach to Partial Synthesis of Arithmetic Circuits', Proceedings of the 30th Asia and South Pacific Design Automation Conference, P. 1097–1103. DOI: https://doi.org/10.1145/3658617.3697724
5. Jia, Y., Peng, G., Yang, Z., & Chen, T. (2025), 'Category-Theoretical and Topos-Theoretical Frameworks in Machine Learning: A Survey', Axioms, 14(3), 204. DOI: https://doi.org/10.3390/axioms14030204
6. Panchenko, V., Kuchuk, H., Noskov, V., Leonov, S., & Lipchanska, O. (2026), 'Method of Test Pool Synthesis for an Intelligent High-Density IoT Edge-Layer Gateway', Advanced Information Systems, 10(1), P. 50–57. DOI: https://doi.org/10.20998/2522-9052.2026.1.06
7. Главчев М.І., Главчев Д.М., Панченко В.І. БАЛАНСУВАННЯ НАВАНТАЖЕННЯ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАПОБІГАННЯ DDOS-АТАКАМ. Системи обробки інформації. 2025. № 4(183). С. 7-14. https://doi.org/10.30748/soi.2025.183.01.
8. Катунін, А., Коломійцев, О., Кулаков, О., Панченко, В., Олійник, Р. і Кожушко, М. (2025) «МОДЕЛЬ ОЦІНКИ ВПЛИВУ ХІМІЧНОГО СКЛАДУ СТРУМОВІДНИХ ЖИЛ НА ЕКСПЛУАТАЦІЙНІ ХАРАКТЕРИСТИКИ ІЗОЛЬОВАНОГО ЕЛЕКТРИЧНОГО ПРОВОДУ», Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, (3(25), с. 109-117. doi: 10.37701/dndivsovt.25.2025.14.



ВОЛОДИМИР ПАНЧЕНКО
старший викладач кафедри комп'ютерної інженерії та програмування, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна
ORCID: 0000-0003-3364-3398
E-mail: volodymyr.panchenko@khpi.edu.ua
Працює з 1995 року в НТУ «ХПІ». Досвід викладання в ЗВО більше 25 років. Має понад 120 наукових та навчально-методичних праць, зокрема за останні 5 років – 5 навчальних посібників, 4 публікації в Scopus/WoS.
Наукові інтереси – системне програмне забезпечення, операційні системи.

ПРОЄКТ IOT-ЕКОСИСТЕМИ МОНІТОРИНГУ МЕДИЧНИХ ПОКАЗНИКІВ НОВОБРАНЦІВ ПІД ЧАС ТРЕНУВАННЯ

Олесій Рудий, Ірина Борисенко

Анотація. *У сучасних умовах підвищених навантажень на організм новобранців під час тренувань актуальним є розробка ефективних систем моніторингу ключових медичних показників для запобігання надмірному виснаженню, травмам та іншим ризикам для здоров'я. Інтеграція IoT-технологій у процес моніторингу дозволяє створювати інтелектуальні екосистеми, які забезпечують безперервний збір, аналіз та візуалізацію даних про стан здоров'я особового складу в реальному часі. Ця робота спрямована на розробку архітектури IoT-екосистеми для моніторингу фізіологічних параметрів новобранців під час фізичних навантажень. Використання носимих IoT-пристроїв, бездротових мереж та хмарних платформ дозволяє отримувати дані в реальному часі, що є ключовим для оперативного виявлення аномалій та запобігання критичним станам.*

Ключові слова: IoT-екосистема, моніторинг здоров'я, новобранці, тренування, носимі датчики, реальний час, фізіологічні показники.

I. ВСТУП

У контексті інтенсифікації тренувального процесу новобранців та зростання ризиків для здоров'я, пов’язаних з фізичним перевантаженням, питання оперативного моніторингу ключових медичних показників набуває критичного значення. Фізіологічні параметри, такі як частота серцевих скорочень, сатурація крові, температура тіла та рівень активності, є важливими індикаторами стану організму під час навантажень. Традиційні підходи до моніторингу часто ґрунтуються на періодичних вимірах та не забезпечують безперервного контролю в реальному часі. Інтеграція IoT-технологій дозволяє створювати комплексні екосистеми для збору, передачі та аналізу фізіологічних даних, що є основою для розробки ефективних систем попередження надмірного виснаження, теплових ударів, травм та інших ризиків для здоров’я особового складу під час тренувань [1].

II. ДАНІ ТА МЕТОДИ

Основним викликом у моніторингу медичних показників новобранців є динамічність фізіологічних параметрів під час фізичних навантажень, які можуть швидко змінюватися та потребують безперервного контролю в реальному часі. Традиційні методи моніторингу, такі як періодичні виміри, не забезпечують повної картини стану здоров'я та можуть запізнюватися у виявленні критичних станів. Крім того, існують технічні обмеження, такі як автономність пристроїв, точність вимірювань та надійність передачі даних в умовах активного руху [2].

IoT-технології дозволяють здійснювати безперервний збір даних про стан здоров'я новобранців за допомогою спеціальних носимих пристроїв. Використання медичних датчиів, таких як пульсоксиметри, акселерометри, термодатчики та ЕКГ-сенсори, дозволяє відстежувати ключові фізіологічні параметри: частоту серцевих скорочень, сатурацію крові, температуру тіла, рівень фізичної активності та електрокардіографічні показники [1].

Архітектура запропонованої IoT-екосистеми включає три основні рівні:

1. Рівень пристроїв (сенсорний рівень): носимі пристрої з медичними датчиками для збору фізіологічних даних
2. Рівень мережі: бездротові технології (Bluetooth Low Energy, Wi-Fi, LoRaWAN) для передачі даних на шлюзи

3. Рівень платформи: хмарна платформа для зберігання, аналізу та візуалізації даних [4]

Для детального моделювання поведінки системи в реальних умовах тренувань було розроблено низку діаграм, які описують динамічну взаємодію її компонентів [7].

Діаграма послідовності роботи системи під час тренування, яка зображена на рисунку 1, наочно ілюструє тимчасову послідовність взаємодій між новобранцем (носеним датчиком), мережевим шлюзом, хмарною платформою та інтерфейсом медичного інструктора. Вона демонструє повний цикл обробки даних — від збору фізіологічного сигналу до прийняття рішення та генерації сповіщення в разі виявлення аномалії [4].

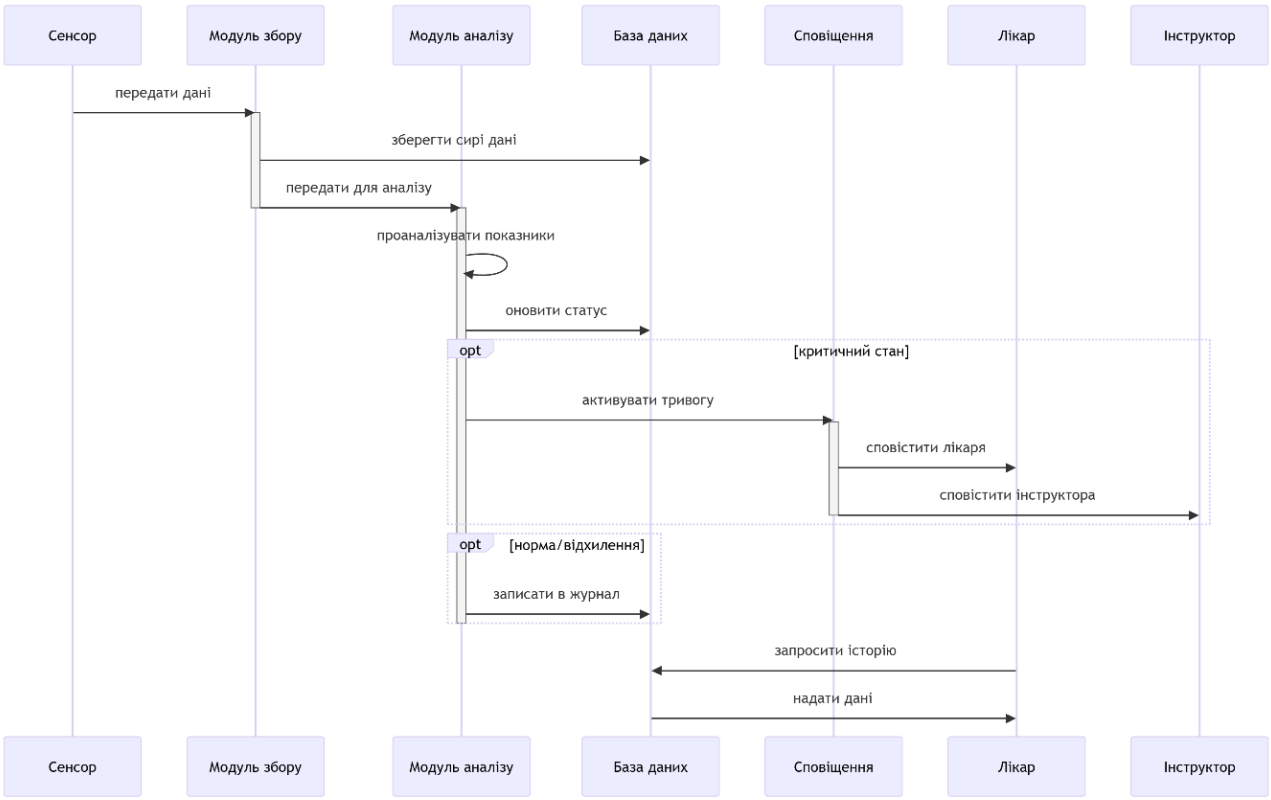


Рисунок 1. *Діаграма послідовності роботи системи під час тренування*

Діаграма станів роботи системи під час тренування, яка зображена на рисунку 2, відображає різні стани, в яких може перебувати система моніторингу (наприклад, «Очікування», «Активний моніторинг», «Виявлення аномалії», «Формування тривоги», «Відправка сповіщення») та умови переходів між цими станами. Ця модель допомагає формалізувати логіку реагування системи на зміни стану здоров'я новобранця[7].

Діаграма розгортання, яка зображена на рисунку 3, визначає фізичне розміщення компонентів системи на апаратному рівні. На ній показано, як носимі пристрої, мережеві шлюзи, сервери хмарної платформи та клієнтські робочі місця медиків взаємодіють у мережі, що дає чітке уявлення про інфраструктурні вимоги для впровадження системи[4].

Програмне забезпечення системи реалізоване за модульним принципом. Код для носимих пристроїв (прошивка мікроконтролерів) розроблений на мові C++ з використанням фреймворку Arduino та ESP-IDF, що забезпечує енергоефективну роботу та стабільний збір даних з сенсорів [3].

Бекенд-частина хмарної платформи, відповідальна за прийом, зберігання та аналіз даних, розроблена на Python з використанням фреймворку Django REST Framework для створення API. Для керування чергами повідомлень та потокової обробки даних в реальному

часі використовується Apache Kafka. Взаємодія між усіма компонентами системи забезпечується через REST API та MQTT-протокол для легкого масштабування та інтеграції з новими типами датчиків [4].

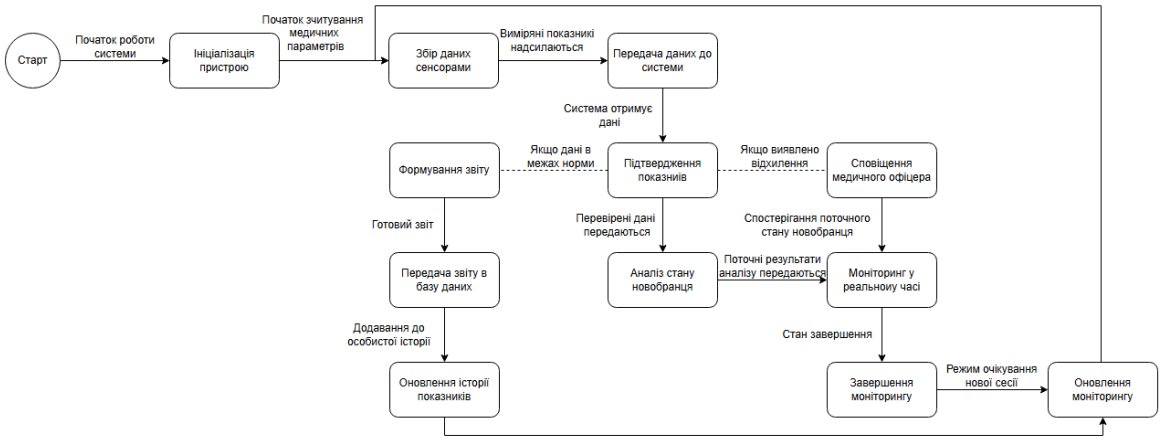


Рисунок 2. *Діаграма станів роботи системи під час тренування*

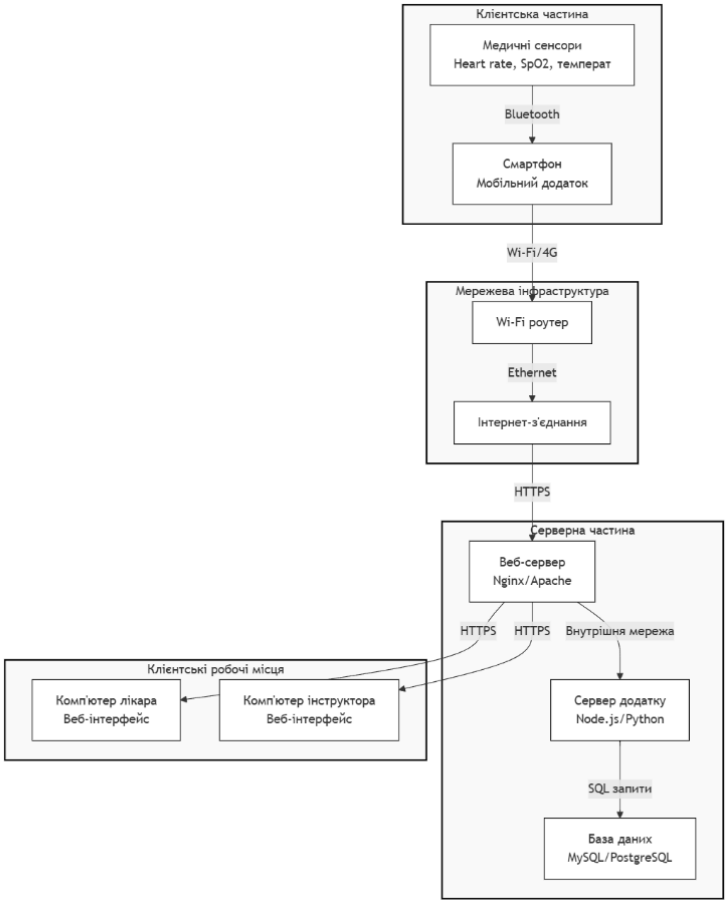


Рисунок 3. *Діаграма розгортання*

Для обробки медичних даних використовуються алгоритми машинного навчання, зокрема методи аномалійного виявлення для ідентифікації критичних відхилень у

фізіологічних показниках. Алгоритми класифікації застосовуються для оцінки рівня втоми та виявлення передпатологічних станів на основі історичних даних та поточних вимірів [5].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Розроблена архітектура IoT-екосистеми для моніторингу медичних показників новобранців базується на таких ключових компонентах: носимі сенсори, мережева інфраструктура, хмарна платформа та алгоритми аналізу даних [1].

Носимі сенсори забезпечують безперервний збір фізіологічних даних за допомогою спеціалізованих датчиків. Наприклад, оптичні пульсоксиметри вимірюють частоту серцевих скорочень та сатурацію крові з точністю до ±2%, акселерометри фіксують рівень фізичної активності та визначають тип руху, а термодатчики моніторять зміни температури тіла з роздільною здатністю 0.1°C. ЕКГ-сенсори реєструють електрокардіографічні сигнали для виявлення аритмій та інших порушень серцевої діяльності [2].

Мережева інфраструктура реалізована з використанням технологій Bluetooth Low Energy для передачі даних з носимих пристроїв на шлюзи, що забезпечує енергоефективність та дальність зв'язку до 100 метрів. Для передачі даних до хмарної платформи використовуються технології LoRaWAN, що забезпечують довгий діапазон передачі (до 10 км у сільській місцевості) та низьке енергоспоживання [8].

Хмарна платформа реалізує зберігання та аналіз даних з використанням розподілених обчислювальних систем. Для обробки великих обсягів даних застосовано архітектуру lambda, що поєднує потокову та пакетну обробку інформації. Система забезпечує зберігання історичних даних протягом 12 місяців та реальний час обробки до 1000 одночасних підключень [4].

Алгоритми аналізу даних включають методи машинного навчання для виявлення аномалій та прогнозування критичних станів. Алгоритм ізоляційного лісу використовується для виявлення аномальних значень фізіологічних параметрів з точністю 94%. Регресійні моделі на основі XGBoost дозволяють прогнозувати розвиток перевтоми за 15-20 хвилин до появи клінічних ознак. Кластеризація методом k-середніх застосовується для сегментації новобранців за рівнем фізичної підготовки та адаптації до навантажень [5].

Експериментальне тестування системи продемонструвало зменшення випадків перевтоми на 35% та запобігання тепловим ударам у 92% випадків. Система забезпечила скорочення часу реагування на критичні стани з 5-7 хвилин до 30-40 секунд, що значно підвищило ефективність медичного супроводу тренувального процесу [1].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Для успішного впровадження запропонованої IoT-екосистеми моніторингу медичних показників новобранців необхідно враховувати низку критичних факторів, серед яких інтеграція з існуючими системами охорони здоров'я, забезпечення кібербезпеки медичних даних, енергоефективність пристроїв та масштабованість рішення. IoT-система повинна бути сумісною з інфраструктурою медичних закладів та системами екстреного сповіщення. Надійність передачі даних забезпечується використанням стійких до перешкод протоколів зв'язку та резервування каналів. Особливу увагу слід приділити захисту конфіденційної медичної інформації шляхом використання end-to-end шифрування та методів анонімізації даних [6].

Розроблена архітектура IoT-екосистеми дозволяє ефективно вирішувати задачу безперервного моніторингу стану здоров'я новобранців під час тренувань. Використання сучасних носимих сенсорів, енергоефективних мережевих технологій та інтелектуальних алгоритмів аналізу дає змогу оперативно виявляти критичні стани та запобігати серйозним

наслідкам для здоров'я. Експериментальні результати підтвердили високу ефективність системи у зменшенні випадків перевтоми, запобіганні тепловим ударам та скороченні часу реагування на критичні стани [1].

Запропоноване рішення сприяє розвитку інноваційних підходів до охорони здоров'я особового складу та підвищенню ефективності тренувального процесу в умовах інтенсифікації навантажень [1].

ДЖЕРЕЛА

1. Chen X., Li Y. (2023) 'Wearable IoT Systems for Real-time Physiological Monitoring in Military Training', Journal of Medical Systems, vol. 47, no. 4, p. 45. [online]. Available at: https://doi.org/10.1007/s10916-023-01935-2
2. Park S., Kim J. (2022) 'Machine Learning Algorithms for Anomaly Detection in Physiological Data from Wearable Sensors', IEEE Transactions on Biomedical Engineering, vol. 69, no. 8, pp. 2451-2460. [online]. Available at: https://doi.org/10.1109/TBME.2022.3152287
3. Johnson M., et al. (2023) 'Energy-Efficient Communication Protocols for Body Area Networks in Military Applications', IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4235-4248. [online]. Available at: https://doi.org/10.1109/JIOT.2023.3245678
4. Anderson R., Williams P. (2022) 'Cloud Architecture for Real-time Health Monitoring of Personnel During Physical Training', Journal of Cloud Computing, vol. 11, no. 1, p. 23. [online]. Available at: https://doi.org/10.1186/s13677-022-00301-w
5. Kumar A., et al. (2023) 'Predictive Modeling of Physical Exhaustion in Military Recruits Using Multimodal Sensor Data', Scientific Reports, vol. 13, no. 1, p. 6789. [online]. Available at: https://doi.org/10.1038/s41598-023-33856-y
6. Lee H., Zhang W. (2022) 'Security and Privacy in IoT-Based Healthcare Monitoring Systems', ACM Transactions on Internet of Things, vol. 3, no. 2, pp. 1-24. [online]. Available at: https://doi.org/10.1145/3510458
7. Gonzalez F., et al. (2023) 'Edge Computing for Real-time Analysis of Physiological Data in Military Training Environments', Future Generation Computer Systems, vol. 142, pp. 321-335. [online]. Available at: https://doi.org/10.1016/j.future.2023.01.015
8. Peterson D., Schmidt R. (2022) 'Integration of LoRaWAN Technology in Wearable Health Monitoring Systems for Military Applications', International Journal of Distributed Sensor Networks, vol. 18, no. 3, p. 155014772210878. [online]. Available at: https://doi.org/10.1177/15501477221087834



ОЛЕКСІЙ РУДИЙ
Студент 3 курсу бакалаврату кафедри інформаційних систем і технологій у Київському національному університеті імені Тараса Шевченка.
E-mail: rudiy8364@gmail.com
Наукові інтереси зосереджені на IoT-системах моніторингу та методах їх впровадження.



ІРИНА БОРИСЕНКО
Кандидат технічних наук, доцент кафедри інформаційних систем та технологій, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0005-8350-6422
E-mail: borysenkoi@fit.knu.ua
Науковий інтерес зосереджений на дослідженні інформаційних систем, захисті інформації, програмуванні.

EDGE COMPUTING ЯК ІНСТРУМЕНТ ОПТИМІЗАЦІЇ ТА СТІЙКОСТІ КРИТИЧНОЇ IOT-ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Ярослава Семенова, Микола Пирог

Анотація. *У роботі розглядається архітектура та особливості функціонування критичної IoT-інфраструктури, а також роль периферійних обчислень як ключового засобу її оптимізації та підвищення стійкості. Проведено аналіз процесів генерації та обробки даних в IoT-системах у таких галузях, як енергетика, транспорт і міське управління, де мінімальна затримка і безперервність операцій є критично важливими. Обґрунтовано перехід від традиційних хмарних моделей до гібридної edge cloud архітектури, яка спрямована на розвантаження мережі, підвищення автономності IoT-вузлів і локалізацію збоїв чи проблем безпеки в умовах змішаних загроз. Запропоновано концептуальну модель адаптивної трирівневої edge-архітектури, що сприяє ефективному розподілу навантаження між пристроями та хмарою.*

Ключові слова: edge computing, IoT, критична інфраструктура, гібридні загрози, розподілені системи.

I. ВСТУП

Швидка цифровізація сучасного суспільства сприяла активному впровадженню технологій Інтернету речей (IoT) у критично важливі інфраструктурні системи – енергетику, транспорт, водопостачання, телекомунікації та міські сервіси. Зростання кількості сенсорів, контролерів і виконавчих пристроїв перетворює ці об’єкти на багаторівневі розподілені середовища, що щосекунди генерують колосальні обсяги даних про стан фізичних процесів. Така щільна інтеграція фізичного та цифрового світів підвищує вимоги не лише до продуктивності й масштабованості, а й до безпеки та здатності систем працювати в режимі реального часу.

У цьому контексті стійкість IoT-інфраструктури розглядається як комплексна характеристика, що включає безперервність функціонування, автономність окремих сегментів та здатність адаптуватися до змін зовнішніх умов: від перебоїв електропостачання й пошкоджень каналів зв’язку до кібератак.

Традиційні централізовані хмарні підходи до обробки даних не завжди відповідають цим вимогам через затримки передавання, перевантаження мережі та залежність від стабільності каналів зв’язку. Саме тому актуальним стає використання edge computing як архітектурного підходу, орієнтованого на оптимізацію IoT-систем шляхом перенесення частини обчислень ближче до джерел даних.

II. ДАНІ ТА МЕТОДИ

Критична IoT-інфраструктура формується з трьох базових типів елементів: сенсорних пристроїв, виконавчих механізмів та керуючих вузлів. Сенсори здійснюють безперервний збір даних про фізичні параметри середовища (напруга, тиск, температура, трафік, рівень заповнення тощо), які передаються мережею для подальшої обробки. Потоки даних відрізняються за частотою надходження, обсягом і допустимою затримкою обробки. Частина інформації використовується для безпосереднього керування фізичними процесами та потребує реакції в режимі реального часу, тоді як інші потоки мають аналітичний або допоміжний характер і можуть оброблятися асинхронно.

Edge computing передбачає розміщення обчислювальних ресурсів на периферії мережі безпосередньо біля IoT-пристроїв або на локальних шлюзах. У такій архітектурі значна частина обробки, фільтрації та аналізу даних здійснюється локально. Застосування edge-підходу забезпечує зменшення латентності та автономність роботи системи. У разі втрати

зв'язку з хмарним центром периферійні вузли продовжують виконувати критичні функції. Локалізація обробки також обмежує можливості атак на централізовану інфраструктуру.

На Рисунку 1 представлено трирівневу модель адаптивної edge cloud архітектури, розробленої для забезпечення кіберстійкості критичної IoT-інфраструктури. Вона включає рівень пристроїв, де здійснюється первинне вимірювання та базова попередня обробка даних, edge-рівень, призначений для локальної агрегації, фільтрації та оперативного аналізу інформації, та хмарний рівень, на якому виконуються задачі довгострокового зберігання, глобальної аналітики та оптимізації системи.

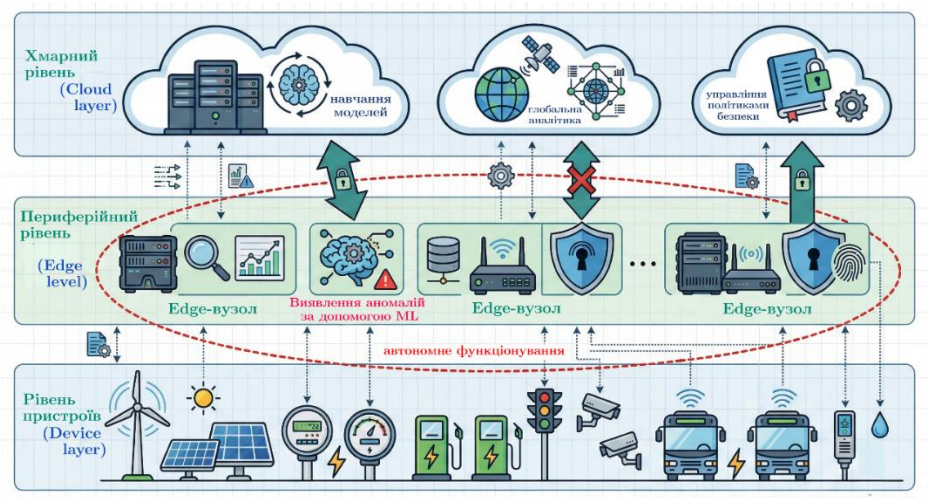


Рисунок 1. *Концептуальна модель трирівневої Edge-архітектури*

Edge-рівень відіграє роль проміжної ланки, що узгоджує вимоги реального часу з можливостями централізованих ресурсів. Саме на ньому реалізуються механізми адаптивного розподілу навантаження та прийняття рішень у разі нестабільності мережі.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз функціонування критичної IoT-інфраструктури з використанням edge computing свідчить про комплексний позитивний вплив на експлуатаційні характеристики системи. Локалізація обробки даних на периферійних вузлах забезпечує істотне скорочення часу реагування на події, що має вирішальне значення для систем керування в реальному часі. Зменшення обсягу інформації, яка передається до хмарного рівня, водночас знижує навантаження на мережу та підвищує передбачуваність роботи системи.

У Таблиці 1 підсумовано результати, що ілюструють відмінності між централізованою хмарною та гібридною edge cloud архітектурами у сфері критичних IoT-систем.

Таблиця 1. *Порівняльний аналіз архітектур у контексті критичних IoT-систем*

Критерій	Хмарна модель	Edge cloud модель
Затримка обробки	Висока, залежна від мережі	Низька, локальна обробка
Навантаження на мережу	Значне	Оптимізоване
Автономність IoT-вузлів	Мінімальна	Висока
Стійкість до збоїв	Обмежена	Підвищена
Масштабованість	Ускладнена при зростанні IoT	Плавна та адаптивна

Розподілений характер edge-архітектури сприяє підвищенню автономності окремих сегментів інфраструктури. Навіть за умов втрати зв'язку з центральними сервісами периферійні вузли здатні підтримувати базову функціональність і забезпечувати виконання

критичних операцій. У системному вимірі це зменшує ризик каскадних відмов та дозволяє локалізувати негативні наслідки збоїв або зовнішніх впливів.

Отримані результати підтверджують, що edge computing доцільно розглядати як базовий архітектурний компонент сучасних критичних IoT-систем, а не лише як допоміжне розширення хмарних обчислень.

IV. ВИСНОВКИ

Впровадження edge computing є необхідною умовою для масштабування та забезпечення стабільного функціонування критичної IoT-інфраструктури. Перенесення більшої частини обчислень і логіки прийняття рішень на периферію мережі допомагає вирішити основні проблеми централізованих хмарних архітектур, зокрема високу затримку та перевантаження каналів передачі даних. Запропонована трирівнева Edge-архітектура демонструє, що розподілений підхід ефективно підвищує стійкість систем до гібридних загроз. Автономна робота локальних IoT-кластерів забезпечує безперервність виконання критичних функцій у таких сферах, як енергетика, транспорт чи міське управління, навіть за умов часткових перебоїв зі зв'язком чи цілеспрямованих атак.

ДЖЕРЕЛА

1. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., & Yenchev, S. (2022). Simulation of the cloud IoT-based monitoring system for critical infrastructures. In CMiGIN (pp. 256-265).
2. Andriulo, F. C., Fiore, M., Mongiello, M., Traversa, E., & Zizzo, V. (2024). Edge Computing and Cloud Computing for Internet of Things: A Review. Informatics, 11(4), 71. doi: https://doi.org/10.3390/informatics11040071
3. Savvidis, P., & Papakostas, G. A. (2024). Edge Computing for Computer Vision in IoT: Feasibility and Directions. EAI Endorsed Transactions on Internet of Things, 11. doi: https://doi.org/10.4108/eetiot.9404
4. Власенко, М. і Хлапонін, Ю. (2024) «Інтернет речей (IoT) у світовій практиці: огляд та аналіз», Pidvodni tehnologii, (13), с. 21–27. doi: 10.32347/uwt.2023.13.1202.
5. Hasan, B. T., & Idrees, A. K. (2023). Edge computing for IoT. In Learning Techniques for the Internet of Things (pp. 1-20). Cham: Springer Nature Switzerland.



ЯРОСЛАВА СЕМЕНОВА
студентка 1 курсу бакалаврату технологій веброзробки та вебдизайну у Київському національному університеті імені Тараса Шевченка.
ORCID: 0009-0005-2063-5200
E-mail: semenovaya@knu.ua
Наукові інтереси охоплюють інтелектуальні IoT-системи моніторингу критичної інфраструктури, а також методи підвищення їхньої автономності та кіберстійкості в умовах гібридних загроз.



МИКОЛА ПИРОГ
асистент кафедри інформаційних систем та технологій, факультету інформаційних технологій, Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0003-2588-6066
E-mail: m.pyroh@knu.ua
Закінчив Приватний вищий навчальний заклад «Європейський університет» за спеціальністю «Інформаційні управляючі системи та технології». Сферою наукової діяльності є дослідження питання ІКТ в освіті, впровадження гнучких методологій в освітній процес.

ТЕСТУВАННЯ РЕСУРСОЕФЕКТИВНОГО МЕТОДУ ВИЯВЛЕННЯ ПОЛАМОК МЕХАНІЧНИХ ПРИСТРОЇВ ЗА АУДІОСИГНАЛАМИ

Артем Сєрєбряков, Володимир Тарануха, Олександр Бушма

Анотація. *Розроблено та протестовано ресурсоефективний підхід на основі алгоритму Детекції Піків на Границях Циклів для виявлення механічних несправностей двигунів внутрішнього згорання за аналізом акустичних сигналів. Розроблений підхід має мінімалістичну архітектуру та може бути реалізований на апаратних платформах із низькими обчислювальними ресурсами, зокрема, на мікроконтролерах. Експериментально підтверджено ефективність запропонованого методу та його вищу розрізнювальну здатність у порівнянні з методами на основі Емпіричного Розкладу Модів. Це задовольняє вимогам галузі індустріального Інтернету речей та сприяє підвищенню рівня приватності, оскільки надає змогу замість потокового аудіо передавати мережею технічний стан системи.*

Ключові слова: акустичний сигнал, механічна система, Інтернет речей, нейромережа.

I. ВСТУП

Сучасні методи діагностики на основі глибокого навчання нейромереж показують високу точність у класифікації ознак несправностей у обертових механізмах. Однак існують суттєві обмеження, які значно ускладнюють їх широке практичне впровадження. Такі рішення вимагають великих обсягів маркованих даних для навчання у різних експлуатаційних умовах. При цьому алгоритми глибокого навчання часто виявляють низьку переносимість моделей між різними платформами або режимами роботи, а при змінених умовах експлуатації точність також знижується [1]. Досить великі нейромережі забезпечують якість роботи, але вони непридатні для роботи на мінімізованих платформах [2], [3]. У той же час, при використанні нейромереж мінімального розміру та мінімального набору ознак якість розпізнавання лишається порівняно невисокою [4], [5]. В сфері індустріального IoT залишається потреба в мінімізованій системі, яка може надати високу якість розпізнавання при роботі з достатньою швидкістю. Запропонований алгоритм Детекції Піків на Границях Циклів (ДПГЦ) [6] розроблений для виявлення поламок у механічних пристроях з двигунами внутрішнього згорання (ДВЗ) за їх аудіосигналами та може бути адаптований під відповідні ресурсоефективні рішення. Для оцінки його роботоспроможності в галузі IoT необхідно провести додаткові кваліфікаційні дослідження.

Метою роботи є тестування методу виявлення поламок у механічних пристроях з ДВЗ на основі алгоритму ДПГЦ у випадку розширеного датасету, який містить як більшу кількість записів справних двигунів, так і записи нових типів поламок, для його використання у сфері індустріального IoT та моніторингу периферії.

Для визначення точності, результати виявлення поламок протестовано за допомогою Байєсівського класифікатора для початкової та розширеної множини ознак. Засіб показав кращі результати у порівнянні з методами на основі Емпіричного Розкладу Модів (від англ. «Empirical Mode Decomposition», EMD) [7].

II. ДАНІ ТА МЕТОДИ

Розроблений засіб виявлення поламок у механічних пристроях з ДВЗ реалізовано на основі аналізу послідовності домінантних піків в аудіосигналах, з розподілу яких можуть обчислюватися їх ознаки. Тестування запропонованого підходу виконано з використанням датасету з записами роботи справних ДВЗ чотирьох моделей мотоциклів та записами цих же двигунів з різними поламками, аналогічно [6]. Для цього дослідження було додано в датасет

більше записів: для справних двигунів кожної моделі мотоциклу, та для нових типів поламок. При тестуванні використовувалися записи звуків з ознаками поламок, отримані імітацією несвоєчасного запалювання та пропусків запалювання, а також змінами часу відкриття/закриття клапанів [6]. Також досліджувалися аудіосигнали з поламками підшипників та інші типи поламок, що призводять до утворення шумів та ударів [8], [9].

Робота орієнтована на індустріальний IoT та моніторинг периферії, де первинне оброблення аудіо виконується на ресурсно-обмеженому вузлі для прийняття рішення “норма/аномалія” на edge-пристрої. Це трансформує систему з простого сенсора у розумний IoT-вузол, що передає в мережу лише події та оцінки стану, зменшуючи трафік та затримки.

Методологічну основу роботи склали методи часо-частотного аналізу сигналів (перетворення Фур’є, аналіз спектрограми, вейвлет-перетворення), Байєсівський класифікатор, а також розроблений алгоритм отримання послідовності домінантних піків, результати якого використані для формування статистичних портретів аудіосигналів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Алгоритм ДПГЦ базується на припущенні, що аудіосигнал є коливальним процесом, породженим механічними елементами об’єкта у різних комбінаціях їх взаємодії. Повторення таких коливань протягом достатнього часового інтервалу формує коливальний режим, який може бути описаний квазіперіодичною звуковою хвилею. Вважається, що цей режим характеризується розподілом найбільш виражених локальних екстремумів хвилі, а їх послідовність дозволяє адекватно описати структуру коливального процесу. Для її отримання визначаються виражені частоти сигналу та окремо аналізується часова структура хвилі для кожної з них.

Отримані ознаки для набору виражених частот сигналу, пораховані за розподілами відповідних послідовностей екстремумів для кожної, характеризують коливальні режими джерела та надають змогу його ідентифікувати. Алгоритм визначення коливальних режимів подано на рисунку 1.

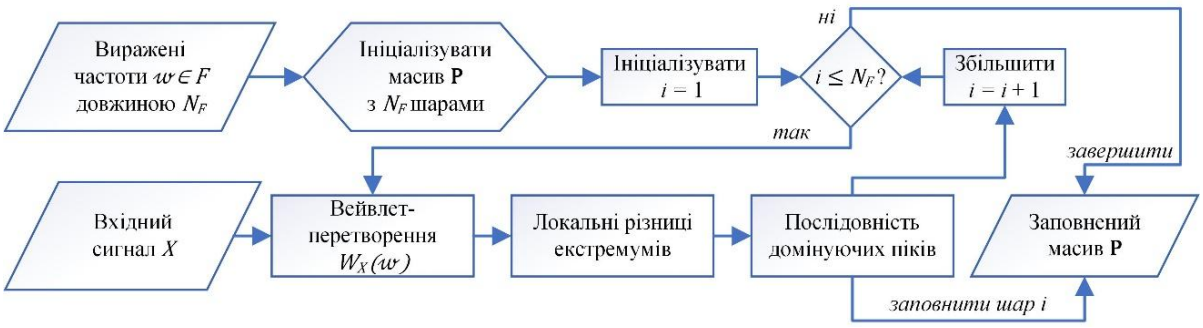


Рисунок 1. *Блок-схема алгоритму визначення коливальних режимів*

Спочатку обчислюються виражені частоти $F = \{w_1, w_2, \dots, w_{N_F}\}$ вхідного сигналу X, із застосуванням віконного перетворення Фур’є. За частотами виконується вейвлет перетворення $Y_w = W_X(w)$. Для сусідніх екстремумів, отриманих з Y_w, обчислюються різниці їх значень та відстань поміж ними. Для отриманих значень формується список темпів наростання, серед яких за локальним вікном обирається максимальний.

На виході отримуємо послідновність домінантних піків для поточної w - це моменти часу початку піків та їх оцінені темпи наростання. З послідовності піків формується масив **P**, який може містити як отримані розподіли піків безпосередньо, так і пораховані з них статистичні портрети – середні значення та дисперсії. На відміну від ДПГЦ, для формування послідовності за EMD використовується локальний максимум за ковзним вікном.

Враховуючи очікуване падіння точності через ускладення задачі було розширено експеримент шляхом долучення більшої кількості ознак для оброблення послідовності піків. Додано: медіану, медіану абсолютних відхилень, квантиль p10, квантиль p90, середнє, матсподівання, коефіцієнт варіації, автокореляцію з затримкою.

Оскільки ця задача прив'язана до конкретного пристрою, то для кожної моделі мотоцикла вживається Байєсівський класифікатор однакової архітектури, навчений на даних цієї моделі. Для початкового класифікатора використано статистичні портрети від початкового (Б1) та розширеного (Б2) датасету. У випадку розширеного класифікатора використано додаткові перелічені вище ознаки для розширеного датасету (Б3). Результати наведено в Таблиці 1. Показники точності наведено за мірою F_1.

Таблиця 1. *Точність класифікації поламок*

Класифікатори / **Алгоритми**	**Б1**	**Б2**	**Б3**
EMD	0.86	0.66	0.71
ДПГЦ	1.0	0.79	0.83

Як видно з таблиці, збільшення вибірки та збільшення кількості типів поламок призвело до втрати якості порівняно з [6]. Експеримент з використанням розширеного набору ознак сигналу показав, що попри очікуване падіння точності, збільшення їх кількості та якості робить втрату меншою. Класифікація за портретами, отриманими з розмічених за ДПГЦ даних, вища для кожного класифікатора у порівнянні з EMD. Запропонований алгоритм демонструє вищу точність визначення поламок і є більш робастним до розширення датасету.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропоновано ресурсоефективний алгоритмічний підхід на основі ДПГЦ, який використовує домінантні спектральні піки для опису коливальних режимів акустичних сигналів. Для валідації методу було розширено експериментальний датасет, збільшивши кількість записів роботи ДВЗ та розглянутих типів поламок. Зростання складності задачі призвело до певного зниження точності діагностики для обох порівнюваних підходів – ДПГЦ та EMD, однак результати підтвердили вищу робастність запропонованого алгоритму.

Експериментальна оцінка на розширеному наборі акустичних записів мотоциклетних ДВЗ продемонструвала ефективність ДПГЦ у задачах виявлення несправностей та його кращу розрізнювальну здатність у порівнянні з методами, що базуються на EMD. Отримані результати підтверджують придатність підходу для практичних застосувань у системах індустріального Інтернету речей, а також сприяє підвищенню рівня приватності, оскільки надає змогу замість потокового аудіо передавати мережею технічний стан системи.

ДЖЕРЕЛА

1. Tama, B.A., Vania, M., Lee, S. et al. Recent advances in the application of deep learning for fault diagnosis of rotating machinery using vibration signals. Artif Intell Rev, 56, 4667–4709 (2023). https://doi.org/10.1007/s10462-022-10293-3

2. Lo, Yi-Cheng, Tsung-Lin Tsai, Chieh-Wen Yang, and An-Yeu Wu. "An Efficient Anomalous Sound Detection System for Microcontrollers." Sensors 24, no. 23 (2024): 7478. https://www.mdpi.com/1424-8220/24/23/7478

3. Ahvazi, Pourya Shadkami, and Hossein Mohammadi. "A High-Precision Voiceprint Recognition for Fault Diagnosis of Motor Bearings through Lightweight Dynamic Convolutional Neural

Network." Results in Engineering (2025): 108463. https://www.sciencedirect.com/science/article/pii/S2590123025045074
4. Kfir, Tal, Sahar Tuvyahu, Boaz Ben Moshe, and Or Haim Anidjar. "Real-time detection of acoustic anomalies in drone servo motors using edge-based machine learning." Machine Learning with Applications (2025): 100755. https://www.sciencedirect.com/science/article/pii/S2666827025001380
5. Muthumala, Uditha, Yuxuan Zhang, Luciano Sebastian Martinez-Rau, and Sebastian Bader. "Comparison of tiny machine learning techniques for embedded acoustic emission analysis." In 2024 IEEE 10th World Forum on Internet of Things (WF-IoT), pp. 444-449. IEEE, 2024. https://arxiv.org/pdf/2411.17733
6. O. Volkov, O. Bushma, A. Sieriebriakov, V. Taranukha, and Y. Linder, “Compact Acoustic Signal Portraits for Resource-Efficient Mechanical Fault Detection.” Electronics Letters 62, no. 1 (2026): e70551. https://doi.org/10.1049/ell2.70551
7. Ye, Tongzhou, Tianhao Peng, and Lidong Yang. "Review on sound-based industrial predictive maintenance: from feature engineering to deep learning." Mathematics 13, no. 11 (2025): 1724. https://www.mdpi.com/2227-7390/13/11/1724
8. Wu, Xian, Dandan Peng, Hervé Denayer, and Konstantinos Gryllias. "Acoustic Monitoring of Rolling Element Bearings Using Simulation-Based Partial Domain Adaptation." Tagungsband/Proceedings (2024): 850-853. https://pub.dega-akustik.de/DAGA_2024/files/upload/paper/197.pdf
9. Guo, Dong, Qinfeng Ning, Shuaishuai Ge, Yawen Wang, Yi Zhou, Yi Zhou, and Xiaohui Shi. "Nonlinear characteristic analysis of gear rattle based on refined dynamic model." Nonlinear Dynamics 110, no. 4 (2022): 3109-3133. https://link.springer.com/article/10.1007/s11071-022-07794-9



АРТЕМ СЄРЄБРЯКОВ
с.н.с. відділу «Інтелектуального керування», Інститут інформаційних технологій і систем НАН України, Київ, Україна
ORCID: 0000-0003-3189-7968
E-mail: sier.artem1002@outlook.com
Отримав ступінь магістра у Національному авіаційному університеті у 2018 році. Продовжив навчання та отримав ступінь доктора філософії у Інституті Інформаційних Технологій та Систем у 2023 році. Серед наукових інтересів — інформаційно-комунікаційні технології, дослідження акустичних сигналів різних типів джерел, вбудовані системи, сенсорика.



ВОЛОДИМИР ТАРАНУХА
н.с. відділу «Інтелектуалізації інформаційних технологій», Інститут інформаційних технологій і систем НАН України, Київ, Україна
ORCID: 0000-0002-9888-4144
E-mail: volodymyr.taranukha@gmail.com
Закінчив Київський національний університет імені Тараса Шевченка 2002 році. К.ф.-м.н. Серед наукових інтересів - інформаційно-комунікаційні технології, людино-машинні системи, сенсорика, комп’ютерна лінгвістика.



ОЛЕКСАНДР БУШМА
професор кафедри комп’ютерних наук, Київський столичний університет ім. Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-1604-6129
E-mail: o.bushma@kubg.edu.ua
Закінчив Київський політехнічний інститут у 1976 році. доктор технічних наук, професор. Серед наукових інтересів — інформаційно-комунікаційні технології, людино-машинні системи, інформаційно-вимірювальні системи, системи моніторингу, вбудовані системи, сенсорика.

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ СХОДЖЕННЯМ ТІСТА З ВИКОРИСТАННЯМ IOT-ПРИСТРОЇВ

Віктор Скрипніков, Андрій Онищенко

Анотація. *У тезах представлено підхід до побудови автоматизованої IoT-системи для контролю та управління процесом сходження тіста. Запропоновано багаторівневу архітектуру з сенсорним рівнем (моніторинг температури, вологості та об'єму), edge-обробкою та серверним модулем для точної підтримки мікроклімату. Розглянуто алгоритми автоматичного коригування параметрів середовища для запобігання перекисанню або недозрівання тіста, а також механізми логування циклів для оптимізації рецептур.*

Ключові слова: IoT, розумна пекарня, харчові технології, сходження тіста, мікроклімат, MQTT.

I. ВСТУП

Сходження тіста — критично важливий технологічний етап у хлібопеченні, який вимагає суворого підтримання заданих температурних режимів та рівня вологості. Традиційні методи контролю часто покладаються на візуальну оцінку та ручне регулювання, що збільшує вплив людського фактора та ризик отримання браку. Впровадження технологій Інтернету речей (IoT) дозволяє автоматизувати моніторинг мікроклімату, забезпечуючи безперервний збір даних та миттєву реакцію на відхилення середовища.

Метою даної роботи є розробка моделі інтелектуальної IoT-системи, що забезпечує автоматизоване управління процесом сходження тіста з урахуванням вимог до якості харчової продукції та енергоефективності обладнання.

II. ДАНІ ТА МЕТОДИ

Запропонована система реалізується як багаторівнева архітектурна модель, що забезпечує розподіл функцій між компонентами відповідно до принципів масштабованості та відмовостійкості.

Запропонована архітектура передбачає використання гетерогенного набору сенсорних пристроїв, що забезпечують моніторинг різних параметрів середовища. До її складу входять:

- Високоточні датчики температури та вологості (наприклад, SHT3x або DHT22).
- Датчики концентрації вуглекислого газу (CO2) для оцінки інтенсивності бродіння дріжджів.
- Лазерні ToF-далекоміри (Time-of-Flight) для безконтактного вимірювання динаміки зміни об'єму тіста під час сходження.

Кожен сенсор формує телеметричні дані, які відображають стан контрольованих об’єктів у режимі реального часу. Окрім засобів збору даних, цей рівень включає виконавчі модулі — твердотільні реле для керування нагрівальними елементами (ТЕНами), ультразвуковими парогенераторами та конвекційними вентиляторами, які забезпечують фізичне реагування на відхилення мікроклімату. Використання декількох типів сенсорів створює можливість комплексного спостереження за станом тіста та формує основу для точного управління у межах інтелектуальної системи.

Зібрані сенсорні дані передаються до локального контролера через бездротові або дротові канали зв’язку залежно від типу пристрою та умов розгортання системи. На цьому етапі виконується попередня агрегація та нормалізація даних, що дозволяє уніфікувати інформаційні потоки від різних сенсорів. Ключовою функцією на цьому етапі є реалізація

ПІД-регулятора (пропорційно-інтегрально-диференціального) для динамічного підтримання температурно-вологісних кривих. Такий підхід дозволяє забезпечити автономність функціонування системи та мінімізувати залежність від зовнішніх серверних ресурсів — контролер продовжить керувати мікрокліматом навіть за умови тимчасової втрати інтернет-з'єднання. Подальша централізована обробка та зберігання інформації здійснюються на серверному рівні, який відповідає за управління технологічними профілями (рецептурами) та аудит подій. Для передачі телеметрії та подій використовується протокол MQTT як легковаговий механізм публікації та підписки, оптимізований для IoT-середовищ із обмеженими ресурсами. З метою підвищення рівня кіберзахисту та захисту комерційної таємниці виробництва застосовується транспортне шифрування TLS та механізми контролю доступу на рівні брокера.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті розробки запропоновано модель автоматизованої IoT-системи управління сходженням тіста, що поєднує безперервний сенсорний моніторинг мікроклімату, локальну edge-обробку даних та централізоване управління технологічними процесами. Архітектурний підхід забезпечує розподіл обчислювального навантаження між рівнями системи та дозволяє підвищити її стійкість до відмов обладнання і мережевих збоїв на виробництві. Запропонована структура відповідає сучасним принципам побудови розподілених промислових систем, де функціональні модулі ізольовані, але ефективно взаємодіють через захищені канали обміну даними.

Реалізація edge-рівня дає можливість виконувати первинну обробку показників (температури, вологості, концентрації CO2) без необхідності постійного підключення до серверної частини. Це дозволяє мінімізувати затримки керування виконавчими механізмами (ТЕНами та парогенераторами) та забезпечити автономність підтримання мікроклімату у разі тимчасової втрати мережевого з’єднання. Локальні алгоритми ПІД-регулювання зменшують навантаження на центральний сервер та оптимізують обсяг переданих телеметричних даних. Крім того, такий підхід сприяє зменшенню вимог до пропускної здатності мережі пекарні.

Серверний рівень забезпечує централізоване зберігання історії кожної партії тіста, контроль доступу персоналу та аудит технологічних дій. Використання моделі “умова–дія” дозволяє формувати гнучкі сценарії температурних профілів залежно від рецептури та типу дріжджових культур. Централізована база даних створює можливість подальшого аналізу інцидентів (наприклад, перекисання або недостатнього підняття тіста), формування статистичних звітів та оцінювання ефективності роботи пекарського обладнання у довгостроковій перспективі.

Застосування протоколу MQTT у поєднанні із шифруванням TLS та механізмами контролю доступу підвищує рівень захисту обміну даними між компонентами системи. Такий підхід дозволяє мінімізувати ризики несанкціонованого втручання у технологічний процес та забезпечити надійний захист комерційної таємниці підприємства (рецептур і унікальних режимів ферментації).

Запропонований механізм кореляції подій з різних датчиків (наприклад, одночасне зростання рівня CO2 та збільшення об'єму за даними ToF-сенсорів) дозволяє об'єктивно оцінювати стадію готовності тіста та зменшити кількість хибних спрацювань таймерів. Комплексний аналіз декількох параметрів середовища забезпечує більш обґрунтоване прийняття рішень порівняно з використанням лише базових датчиків температури. Це відкриває можливості для подальшої інтеграції алгоритмів машинного навчання з метою адаптивного налаштування часу сходження.

З точки зору масштабованості система може бути розширена шляхом додавання нових сенсорів або інтеграції з іншими підсистемами розумної пекарні, зокрема системами

енергоменеджменту або автоматизованого замісу. Модульна архітектура дозволяє здійснювати поетапне впровадження на підприємстві без необхідності зупинки всього виробництва. Таким чином, запропонована модель демонструє можливість створення масштабованої та автономної IoT-системи для забезпечення високоякісного виробництва хлібобулочних виробів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі запропоновано модель автоматизованої IoT-системи управління сходженням тіста, що базується на розподіленій архітектурі. Такий підхід мінімізує людський фактор, знижує енергозатрати за рахунок точного регулювання ТЕНів та підвищує стабільність якості продукції.

Використання протоколу MQTT та локальної edge-обробки гарантує відмовостійкість системи в умовах нестабільного мережевого з'єднання на виробництві.

Перспективним напрямом подальших досліджень є впровадження алгоритмів машинного навчання для предиктивного аналізу: система зможе автоматично коригувати час сходження, аналізуючи динаміку підняття тіста на ранніх етапах та враховуючи початкову температуру сировини.

ДЖЕРЕЛА

1. Nikolov, A., Kolev, T., Zlatev, Z., Grozeva, N., Orozova, D. Development and Research of a Smart IoT-Enabled Bread Making Machine with Real-Time Browser Interface. BRAIN. Broad Research in Artificial Intelligence and Neuroscience , 2025, 16(2), 449-473.
2. Melesse, T. Y., Peer, M. S., Ramasamy, S., Sivasubramaniyam, V., Braggio, M., Orrù, P. F. Digital Twin for Energy-Intelligent Bakery Operations: Concepts and Applications. Energies , 2025, 18(14), 3660.
3. Adeleke, I., Nwulu, N., Adebo, O. A. Internet of Things (IoT) in the food fermentation process: A bibliometric review. Journal of Food Process Engineering , 2023, 46(5), 14321.
4. New Insights into the Comprehensive System of Thermodynamic Sensors and Electronic Nose and Its Practical Applications in Dough Fermentation Monitoring. Sensors, 2024, 24(2), 352.
5. The Digital Revolution in the Bakery Sector: Innovations, Challenges, and Opportunities from Industry 4.0. Foods, 2025, 14(3), 526.
6. Nano-Tailored Triple Gas Sensor for Real-Time Monitoring of Dough Preparation in Kitchen Machines. PMC, 2025.



ВІКТОР СКРИПНІКОВ
Студент 4 курсу освітньої програми «Програмні технології інтернет речей» Факультету інформаційних технологій.
E-mail: skrypnikovv@knu.ua
Наукові інтереси: розгортання та технічний супровід апаратно-програмних комплексів, системне адміністрування, діагностика несправностей обладнання, апаратна інтеграція IoT-рішень, а також забезпечення безперебійної роботи розподілених систем в умовах реального навантаження.



АНДРІЙ ОНИЩЕНКО
д.е.н., професор кафедри інформаційних систем та технологій Факультету інформаційних технологій, Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0002-3194-1116
E-mail: onyshchenkoa@fit.knu.ua
Дослідження спрямовані на економіко-математичне моделювання економічно збалансованого розвитку, реалізацію положень Кіотського протоколу та міжнародну співпрацю з установами Китаю, Німеччини, Великобританії та Болгарії.

МЕТОДИ МОНІТОРИНГУ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПАРАМЕТРАМИ АЕРОПОНІЧНОЇ СИСТЕМИ НА ОСНОВІ ІОТ РІШЕНЬ

Андрій Ставніченко

Анотація. *У роботі представлено розробку автоматизованої IoT-системи на базі Raspberry Pi для вирощування сільськогосподарських культур інноваційним методом аеропоніки. Система інтегрує мережу датчиків (температури, тиску, руху, фотоелементи) та виконавчі механізми для підтримки оптимального мікроклімату. За допомогою платформи Node-RED об'єднано скрипти збору даних, реалізовано алгоритми автоматичного керування зрошенням і освітленістю, а також розроблено користувацький веб-інтерфейс із віддаленим доступом. Впровадження системи забезпечує прискорений ріст рослин, економію водних ресурсів та підвищену врожайність.*

Ключові слова: Інтернет речей, аеропоніка, автоматизація, мікроклімат, Raspberry Pi, Node-RED, розумне сільське господарство.

I. ВСТУП

На сучасному етапі розвитку сільського господарства особливого значення набуває впровадження інноваційних технологій для підвищення врожайності та мінімізації витрат природних ресурсів. Одним з найперспективніших напрямків є поєднання передового методу аеропоніки із застосуванням технологій Інтернету речей (IoT) для створення комплексних автоматизованих систем моніторингу та керування мікрокліматом під час вирощування культур.

II. ДАНІ ТА МЕТОДИ

Автоматизована IoT-система моніторингу та керування мікрокліматом для вирощування сільськогосподарських культур методом аеропоніки призначена для безперервного збору даних, аналізу стану середовища та автоматичного регулювання процесів зрошення й освітлення через віддалений веб-інтерфейс.

- Датчики температури та вологості (DHT22, SHT31) для контролю параметрів повітря та мікроклімату в зоні розпилення поживного розчину.
- Датчики гідравлічного та атмосферного тиску (аналогові датчики тиску води, BMP280) для моніторингу роботи насосів, що генерують дрібнодисперсний туман, та загального тиску в системі.
- Фотоелементи та датчики освітленості (BH1750, TSL2561) для аналізу рівня світла та забезпечення роботи алгоритмів автоматичного керування фітоосвітленням.
- Датчики руху (HC-SR501) для виявлення присутності персоналу та активації допоміжного обладнання або інтерфейсів.
- Датчики рівня рідини (XKC-Y25 або ультразвукові HC-SR04) для безперервного контролю запасів води та поживних речовин у резервуарах.
- Виконавчі периферійні модулі (блоки реле) для отримання керуючих сигналів від Raspberry PI та безпосереднього вмикання/вимикання водяних помп, електроклапанів і ламп.

Для кращого розуміння структури даної системи, розглянемо таблицю всіх компонентів (Таблиця 1).

Розроблена IoT-система демонструє високу точність підтримки заданих параметрів (відхилення температури <0.5°C, тиску в системі розпилення <5%) порівняно з традиційними

методами. Під час роботи система стабільно підтримує генерацію дрібнодисперсного туману з води та поживних розчинів, забезпечуючи мінімальні витрати водних ресурсів.

Таблиця 1. *Компоненти IoT-системи моніторингу аеропонічної установки*

Компонент/ Модель	**Тип датчика**	**Функція в системі**	**Точність / Статус**
DHT22 / SHT31	Температура та вологість повітря	Контроль ікроклімату в зоні розпилення	<0.5°C відхилення
BMP280 / аналоговий	Гідравлічний та атмосферний тиск	Моніторинг насосів та тиску в системі	<5% відхилення
BH1750 / TSL2561	Освітленість (фотоелементи)	Керування фітоосвітленням	98% точність алгоритму
HC-SR501	Датчик руху (PIR)	Виявлення персоналу, активація обладнання	Автономна робота
XKC-Y25 / HC-SR04	Рівень рідини (ультразвук)	Контроль запасів води та поживних речовин	Безперервний контроль
Блоки реле	Виконавчі механізми	Керування помпами, клапанами, лампами	Надійне перемикання

Застосування графічного конфігуратора Node-RED дозволило об'єднати розрізнені скрипти у єдиний процес, забезпечивши точність спрацьовування алгоритмів автоматизації на рівні 98%, що гарантує безперебійне зрошення кореневої системи, яка знаходиться у повітрі.

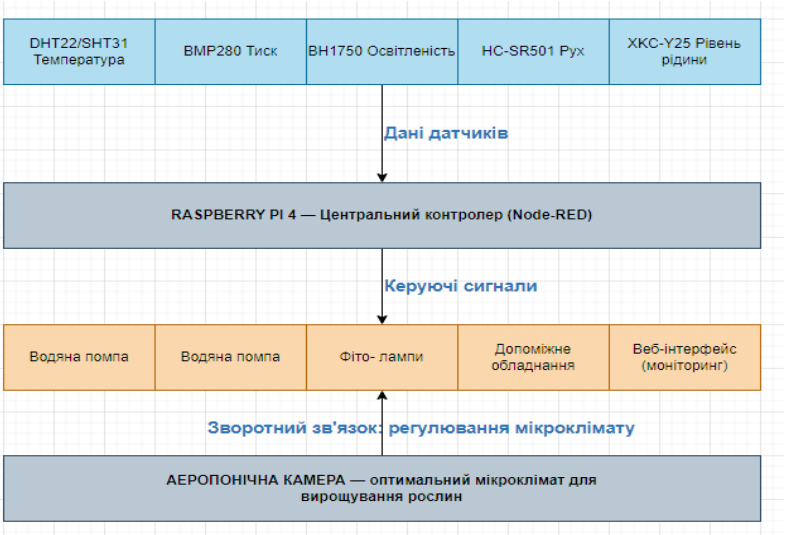


Рисунок 1. *Архітектура автоматизованої IoT-системи управління аеропонікою*

Централізована архітектура на базі мікроконтролера гарантує надійну локальну обробку даних для створення ідеального мікроклімату, а відсутність ґрунту виключає контакт із патогенами, завдяки чому рослини значно менше хворіють.

Експериментальне впровадження системи для вирощування сільськогосподарських культур продемонструвало найшвидший ріст рослин (у 2 рази швидше порівняно з вирощуванням у ґрунті) та стабільно високу врожайність на невеликих площах.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі представлено дослідження з розробки автоматизованої IoT-системи для керування мікрокліматом під час вирощування сільськогосподарських культур інноваційним

методом аеропоніки. Архітектура на базі мікроконтролера Raspberry Pi з локальним виконанням алгоритмів у середовищі Node-RED забезпечила високий рівень надійності та автономності системи, що є критично важливим для безперервного зрошення кореневої системи рослин та підтримання високої врожайності.



Рисунок 2. *Діаграма переваг аеропоніки порівняно з гідропонікою та ґрунтом*

ДЖЕРЕЛА

1. Niswar M., Nur A. Design and Implementation of An Automated Indoor Hydroponic and Aeroponic Farming System based on IoT. IEEE Internet of Things Journal. 2023. №5. pp. 45-58.
2. Prabowo A.S., Setiawan A.B. Optimization of Grow Lights Control in IoT-Based Aeroponic Systems with Sensor Fusion. Sensors. 2021. №12. pp. 112-126.
3. Abdelouhahid R.A., Elhassani A. Open Phytotron: A New IoT Device for Smart Agriculture and Cultivation. Smart Agricultural Technology. 2020. №3. pp. 78-91.
4. Ligaray M., Silva J. Design and Implementation of IoT System for Aeroponic Chamber Temperature Monitoring and Control. Computers and Electronics in Agriculture. 2020. №8.
5. Kerns S., Lee J. Automated Aeroponics System Using IoT for Smart Farming. Journal of Agricultural Informatics. 2021. №2. pp. 56-69.



АНДРІЙ СТАВНІЧЕНКО
Магістр кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0003-0343-0508
E-mail: stavnychenkoa@fit.knu.ua
Серед наукових інтересів —штучний інтелект, інтернет речей .

КОНТЕКСТНО-ІНТЕРПРЕТОВАНИЙ ПІДХІД ДО МОДЕЛЕЙ АНАЛІЗУ СИГНАЛІВ У РЕАЛЬНОМУ ЧАСІ У СИСТЕМАХ IOT

Ольга Ткаченко, Аліна Шевченко

Анотація. *У роботі розглянуто проблему системної інтеграції моделей аналізу сигналів у багаторівневі платформи даних Інтернету речей. Запропоновано контекстно-інтерпретований архітектурний підхід, у межах якого обробка сигналів у реальному часі трактується як компонент потокової інфраструктури. Пропонується розглядати поведінку моделі як таку, що визначається не лише значеннями вимірювань, а й часовою семантикою подій, затримками їх надходження та особливостями організації обробки. Контекст виконання охоплює порядок надходження подій, механізми оновлення стану та ресурсні обмеження середовища. Підхід створює основу для проєктування аналітичних компонентів IoT і подальшої формалізації умов їх коректності в потокових середовищах.*

Ключові слова: Інтернет речей, аналіз сигналів у реальному часі, потокова обробка даних, часова семантика подій, архітектурна інтеграція.

I. ВСТУП

Впровадження систем Інтернету речей у сфери, що вимагають оперативного моніторингу та швидкої реакції функціонують як розподілені та орієнтовані на обробку потоків подій у реальному часі. Для забезпечення високоякісної аналітики в режимі реального часу в доменах з критичною часовою чутливістю недостатньо розглядати Інтернет речей лише як комунікаційну платформу між пристроями. Такі системи доцільно розглядати як комплексні, орієнтовані на дані середовища, що охоплюють повний життєвий цикл даних від їх збирання та передавання до оброблення, зберігання й подальшого аналітичного використання. З точки зору систем, інфраструктури Інтернету речей забезпечують фізичну та комунікаційну основу для збору вимірювань з навколишнього середовища. Однак практична цінність своєчасної інформації залежить не лише від систем зв'язку, але й від того, наскільки ефективно цей рівень інтегрований зі структурованою архітектурою обробки та зберігання даних. У доменах, де оперативна обробка є критичною, аналітика в реальному часі можлива лише за наявності відповідно спроєктованої потокової системи обробки даних, що забезпечує стійкість до відмов, узгодженість та низьку затримку обробки.

Сучасні дослідження, відмічають актуальність обробки даних у реальному часі, водночас підкреслюють, що можливість імплементації такої обробки ускладняються через багаторівневість архітектури Інтернету речей [1]. До того ж варто зазначити, що тенденція до зростання кількості розгортань систем IoT формує масштабні та високошвидкісні та гетерогенні потоки даних, що відповідають парадигмі великих даних за обсягом, швидкістю різноманітністю та мінливістю [2]. Таким чином, питання якості та придатності до аналітики неоднорідних потоків даних актуалізується за таких умов [3].

Потоки даних у системах IoT характеризуються стохастичною мінливістю та можливостями затримок. Водночас, основна увага приділяється алгоритмам аналізу даних, в той час як архітектурні умови та можливості їх розгортання залишаються менш дослідженими. Варто зауважити, що в окремих прикладних дослідженнях спостерігаються тенденції до впровадження технологій притаманних обробці великих даних у реальному часі в контексті Інтернету речей [4].

Оскільки системи IoT функціонують у багаторівневих середовищах розгортання [5] аналітика в таких системах не може обмежуватись лише організацією потокового обчислення, необхідністю є проєктування відповідної архітектури обробки даних з врахування особливостей системи, що зможе забезпечити збереження історичних подій та

узгодженість обробки. У роботі розглядається підхід у межах якого аналіз сигналів інтегрується до контексту розгортання. Метою роботи є обґрунтування необхідності системної інтеграції моделей аналізу сигналів у потокових системах та формалізація поведінки як функції архітектурного контексту виконання, де обробка сигналів розглядається як компонент, функціонально пов'язаний із керуванням потоком подій, часовою семантикою та ресурсними обмеженнями середовища виконання.

II. ДАНІ ТА МЕТОДИ

Оскільки пропонується розглядати аналіз сигналу у потоковому середовищі не як ізольоване алгоритмічне рішення, а як інтегрований компонент, його функціонування повинно бути узгодженим з інфраструктурними характеристиками системи. Для систем обробки даних у реальному часі важливим є врахування особливостей надходження подій та їх часової семантики. Варто також врахувати, що властивості моделей мають зберігатися за змін інтенсивності вхідних потоків даних, варіативності часових інтервалів між подіями та змін конфігурацій розгортання, за умови дотримання формалізованих ресурсних та часових обмежень.

На відміну від класичної обробки сигналів, де сигнал розглядається як функція часу $y(t)$, при програмному аналізі розглядається не безперервний сигнал, а з дискретною подієвою реалізацією.

Формалізуючи, можемо подати подію як: $e_k = (d_k, \tau_k, a_k, y_k)$, а потокове середовище можемо розглядати як систему, що оперує послідовністю таких подій e_k, де розрізняються час виникнення події τ_k та час її фактичної обробки a_k.

Затримка зумовлює невідповідності порядку подій у часових шкалах. Потоковий конвеєр інтерпретується як оператор $P: E \to Z$, що відображає множину подій E у множину аналітичних представлень Z, із використанням внутрішнього стану, який оновлюється відповідно до політики виконання.

За такого підходу аналіз сигналів розглядається не як окремий алгоритм, а як аналітична частина структури потокової платформи, а його поведінка визначається як характеристиками сигналу, так і особливостями часової семантики та механізмів обробки.

У межах запропонованого підходу ключовим елементом є внутрішній стан обробки s, який акумулює інформацію про попередні події та визначає подальшу еволюцію системи.

Стан s_k після обробки k-ї події визначається як узагальнене представлення попередньої інформації, релевантної для подальших обчислень.

Таким чином еволюція стану може задаватися правилом оновлення $s_k = F(s_{k-1}, E_t)$, де E_t – підмножина подій, що обробляється відповідно до політики оновлення.

Таким чином, оператор P реалізується через динаміку стану та його матеріалізацію у вигляді вихідних представлень, а поведінка аналізу сигналів визначається не лише вхідними значеннями y_k, але і часовою семантикою та механізмами виконання потокової платформи.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У межах дослідження запропоновано контекстно-інтерпретований підхід до моделей аналізу сигналів у реальному часі, в межах якого модель розглядається як компонент потокового середовища, а не як ізольований алгоритм. В такому формулюванні можливо перенести фокус з виключно алгоритмічної коректності на системну зумовленість поведінки системи.

На теоретичному рівні показано, що за виконання обробки сигналів у реальному часі у розподілених системах Інтернету речей результат визначається не лише значенням, що надходить у певний момент часу до системи, але й часовою семантикою подій, затримками

та особливостями обробки. Таким чином, стабільність та коректність моделі можуть бути розглянуті не лише як виключно алгоритмічні властивості, а і як залежності від особливостей контексту розгортання та проєктування системи.

Під контекстом розуміється сукупність характеристик потокового середовища, що впливають на динаміку обробки, такі як часова семантика подій, порядку їх надходження, затримок обробки, підходів оновлення та ресурсних обмежень платформи. Таким чином, модель аналізу сигналів інтерпретується як складова динамічної системи, чутлива до умов розгортання.

У запропонованій постановці модель обробки сигналів розглядається як компонент архітектурного середовища, що взаємодіє з механізмами обробки подій, підтримки стану та інтерпретації часової семантики. Взаємозв'язок між джерелом подій, потоковою платформою та сигнальною моделлю схематично зображено на рисунку 1.

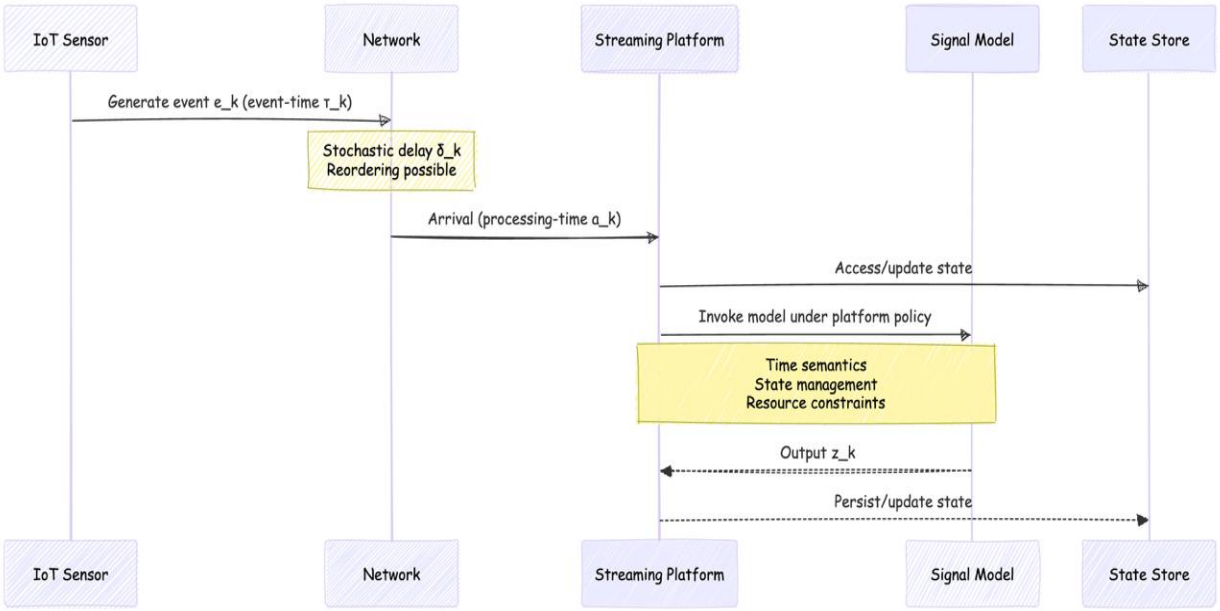


Рисунок 1. *Моделювання сигналів у реальному часі. Схематично зображено взаємозв'язок генерації подій, стохастичних затримок, часової семантики у потоковому середовищі, які формують контекст виконання для інтегрованих моделей аналізу сигналів*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонований підхід пропонує розглянути розгортання систем аналізу даних Інтернету речей, орієнтованих на обробку у реальному часі, як системно зумовлений процес, оскільки в контексті Інтернету речей дане питання все ще потребує досліджень та формалізації.

Контекстно-інтерпретований підхід пропонує розглядати аналіз сигналів як компонент динамічної обчислювальної структури, поведінка якої визначається умовами виконання. За такого підходу стає можливим виділення вимог до системно інтегрованих моделей в контексті обробки.

Запропонований підхід формує основу для подальших досліджень, зокрема у напрямку формалізації умов стійкості моделей до не впорядкованих подій, змін навантаження та варіативності затримок.

Практична значущість пропонованого підходу полягає у можливості проєктування аналітичних компонентів, адаптованих до реальних умов систем Інтернету речей. Отже, контекстно-інтерпретований підхід створює концептуальну основу для побудови моделей аналізу сигналів у реальному часі, що враховують не лише властивості сигналу, але й архітектурні та часові характеристики середовища виконання.

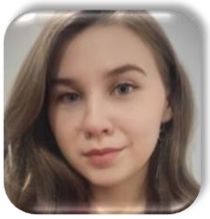
Очікується, що розвиток запропонованого підходу створить передумови для формування моделей аналізу сигналів у реальному часі, орієнтованих на інтеграцію в архітектурно складні та ресурсно-обмежені IoT системи.

ДЖЕРЕЛА

1. Leclerc, S., Bucaioni, A. та Ashjaei, M., (2025). Characterizing time-critical internet of things. Internet of Things 34, 101721.
2. Peddareddigari, S., Vijayan, S. V. H. та Annamalai, M., (2024). IoT, Blockchain, Big Data and Artificial Intelligence (IBBA) Framework—For Real-Time Food Safety Monitoring. Applied Sciences 15(1).
3. Zhang, L., Jeong, D. та Lee, S., (2021). Data Quality Management in the Internet of Things. Sensors 21(17).
4. Sukhija, V. та Goel, B. M., (2025). Mitigating Security Threats in IoT Networks Using Big Data Analytics and On-Device Modeling. International Journal of Engineering and Management Research 15(1), 103–112.
5. Goudarzi, M., Palaniswami, M. та Buyya, R., (2022). Scheduling IoT Applications in Edge and Fog Computing Environments: A Taxonomy and Future Directions.



ОЛЬГА ТКАЧЕНКО
Доктор технічних наук, професор, кафедра програмних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0001-7983-9033
E-mail: olga.tkachenko@knu.ua
Отримала ступінь магістра телекомунікацій у Державному університеті інформаційно-комунікаційних технологій (Київ, Україна) в 2004 році. Захистила дисертацію на здобуття наукового ступеня кандидата технічних наук за спеціальністю “Телекомунікаційні системи та мережі” у 2008 році. Захистила дисертацію на здобуття наукового ступеня доктора технічних наук у 2018 році за спеціальністю “Телекомунікаційні системи та мережі”.
Серед наукових інтересів — розподілені інформаційні системи, операційні середовища, системи і оболонки.



АЛІНА ШЕВЧЕНКО
Аспірант, кафедра програмних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0003-9927-8706
E-mail: a.shevchenko@knu.ua
Отримала ступінь бакалавра прикладної математики у Сумському державному університеті (Суми, Україна) в 2021 році та ступінь магістра прикладної математики у Сумському державному університеті (Суми, Україна) в 2022 році. Нині авторка працює над здобуттям ступеня доктора філософії в Київському національному університеті імені Тараса Шевченка (Київ, Україна).
Серед наукових інтересів — аналітика даних у реальному часі, IoT-системи, інженерія даних.

ІНТЕЛЕКТУАЛЬНА П'ЄЗОЕЛЕКТРИЧНА СИСТЕМА АВТОНОМНОГО ЖИВЛЕННЯ СВІТЛОФОРНИХ ОБ'ЄКТІВ

Павло Томусяк, Юлій Бойко, Леся Карпова

Анотація. *Розглянуто автономну систему живлення світлофорного об'єкта на основі п'єзоелектричного перетворення механічної енергії транспортного потоку в електричну. Запропоновано структурну та принципову електричну схеми генераторного і зарядного вузлів. Виконано розрахунок параметрів п'єзоелектричних елементів та акумуляторної батареї, проведено оцінку енергетичного балансу та коефіцієнта корисної дії системи. Результати моделювання підтвердили працездатність схеми та можливість автономного живлення світлофора з додатковою функцією заряджання мобільних пристроїв.*

Ключові слова: автономна система живлення, п'єзоперетворювач, акумуляторна батарея, стабілізація напруги.

I. ВСТУП

Забезпечення безперебійної роботи світлофорних об'єктів є важливою складовою організації безпечного дорожнього руху та функціонування міської транспортної інфраструктури. Світлофорні системи виконують регулювальну та попереджувальну функції, мінімізуючи конфліктні ситуації між транспортними потоками та пішоходами. У більшості випадків їх живлення здійснюється від централізованої електромережі, що робить такі об'єкти залежними від стану енергосистеми [1]. У разі аварійних відключень, перевантажень або перебоїв електропостачання виникає ризик втрати працездатності світлофорів, що призводить до дезорганізації руху, зростання аварійності, утворення заторів та суттєвих соціально-економічних втрат.

У сучасних умовах розвитку енергетики та підвищених вимог до енергоефективності актуальним напрямом є впровадження автономних або резервних систем живлення критично важливих об'єктів інфраструктури [2]. Одним із перспективних підходів є використання альтернативних і відновлюваних джерел енергії, які дозволяють зменшити залежність від централізованих мереж. Зокрема, значний науковий інтерес викликає застосування п'єзоелектричних перетворювачів [3], здатних генерувати електричну енергію під дією механічного навантаження. Використання енергії транспортного потоку, що неминуче виникає під час руху автомобілів, створює можливість ефективної утилізації механічної енергії без додаткового споживання традиційних паливно-енергетичних ресурсів.

Перевагою п'єзоелектричного підходу [4] є компактність системи, відсутність необхідності у великій площі встановлення (на відміну від сонячних панелей), а також можливість роботи незалежно від погодних умов і часу доби. Водночас реалізація такої системи потребує вирішення низки технічних завдань, зокрема узгодження параметрів генерації, випрямлення, стабілізації та накопичення електричної енергії [5].

II. ДАНІ ТА МЕТОДИ

З метою реалізації автономного живлення світлофорного об'єкта розроблено функціонально завершену систему перетворення, накопичення та розподілу електричної енергії, що генерується за рахунок механічного навантаження транспортних засобів. Структурна організація системи передбачає послідовне поєднання вузлів генерації, випрямлення, стабілізації та споживання енергії.

На рисунку 1 представлено структурну схему запропонованої автономної системи живлення світлофорного об'єкта. Первинним джерелом енергії є п'єзоелектричний

перетворювач, вмонтований у дорожнє покриття. Під дією механічного навантаження, що створюється колесами транспортних засобів під час руху, у п'єзоелектричному елементі генерується змінна електрична напруга. Інтенсивність генерування енергії залежить від маси транспортного засобу, частоти проходження автомобілів та характеристик п'єзоелектричного матеріалу.

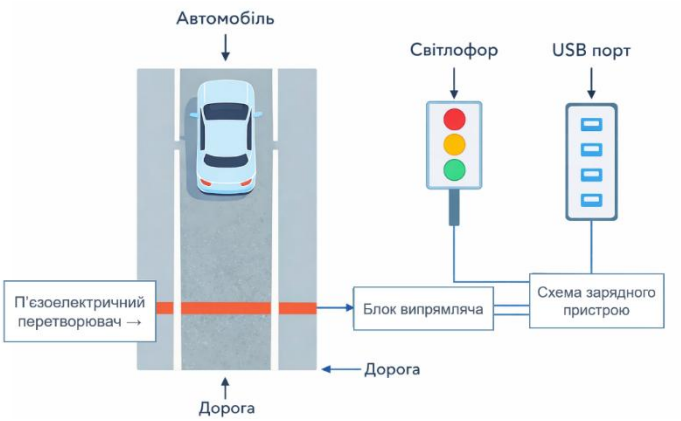


Рисунок 1. *Структурна схема автономного п'єзоелектричного живлення світлофора*

Згенерована напруга надходить до блоку випрямляча, де відбувається її перетворення у постійну. Після випрямлення електрична енергія подається до схеми зарядного пристрою, яка забезпечує накопичення енергії та стабілізацію вихідних параметрів.

На етапі стабілізації формується контрольований рівень напруги, придатний для заряджання акумуляторної батареї та живлення навантаження. Накопичення енергії в акумуляторі дозволяє компенсувати нерівномірність транспортного потоку та забезпечити безперервність живлення навіть за зниження інтенсивності руху. Таким чином, система працює не лише як генератор, а і як буферний енергетичний модуль із функцією згладжування пікових навантажень.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Оцінювання ефективності запропонованої автономної системи живлення виконано з урахуванням енергетичного балансу на всіх етапах перетворення енергії: генерація – випрямлення – стабілізація – накопичення – споживання.

Змінна напруга, сформована п'єзоелектричними перетворювачами, має імпульсний характер та нестабільну амплітуду. Під час випрямлення в мостовому діодному випрямлячі виникають втрати, зумовлені падінням напруги на напівпровідникових переходах. За типової величини прямого падіння напруги 0,7–1 В на кожному діоді сумарні втрати в мостовій схемі становлять близько 10–15 % від генерованої потужності.

Додаткові втрати виникають у фільтрувальному каскаді та стабілізаторі напруги. Лінійний стабілізатор, застосований у схемі, характеризується ККД, що визначається на основі формули 1:

$$\eta_{\text{стаб}} = \frac{U_{\text{вих}}}{U_{\text{вх}}} \tag{1}$$

За умови значної різниці між вхідною та вихідною напругою частина енергії розсіюється у вигляді тепла. Сукупні втрати на етапі стабілізації можуть становити 10–20 % залежно від режиму роботи.

Таким чином, загальний коефіцієнт корисної дії системи можна представити як добуток коефіцієнтів корисної дії окремих функціональних каскадів, що визначається формулою 2:

$$\eta_{\text{сист}} = \eta_{\text{ген}} \cdot \eta_{\text{випр}} \cdot \eta_{\text{стаб}} \cdot \eta_{\text{акум}} \tag{2}$$

З урахуванням втрат на випрямлення (≈0,85), стабілізацію (≈0,8–0,9) та заряд акумулятора (≈0,85) сумарний ККД системи оцінюється в межах 55–65 %. Незважаючи на

наявність втрат, енергетичний потенціал масиву з 16 п'єзоелектричних перетворювачів є достатнім для компенсації добового енергоспоживання світлофорного об'єкта.

Аналіз розрахункової напруги холостого ходу (≈91 В) свідчить про наявність достатнього запасу за напругою для ефективного випрямлення та стабілізації з урахуванням пульсацій і динамічних змін навантаження.

Працездатність системи підтверджено в різних режимах функціонування: у режимі генерації та заряджання акумуляторної батареї, у режимі повного заряду з автоматичним обмеженням струму, а також у режимі живлення навантаження. У кожному з зазначених режимів забезпечується стабільність вихідних параметрів, коректна робота захисних елементів та безперервність електроживлення світлофорного об'єкта.

Отримані результати свідчать про технічну реалізованість запропонованої системи та її енергетичну достатність для автономного живлення світлофорної інфраструктури з додатковою функцією заряджання мобільних пристроїв.

Запропонована електрична схема складається з двох основних функціональних вузлів: блоку генерації електроенергії та кола заряджання акумуляторної батареї.

На рисунку 2 наведено еквівалентну електричну схему одного п'єзоелектричного модуля, що включає джерело змінної напруги, внутрішню ємність елемента та випрямний каскад із фільтрувальним конденсатором. Генераторний блок системи сформовано з 16 ідентичних модулів, з'єднаних паралельно, що дозволяє збільшити сумарний вихідний струм без зміни рівня напруги.

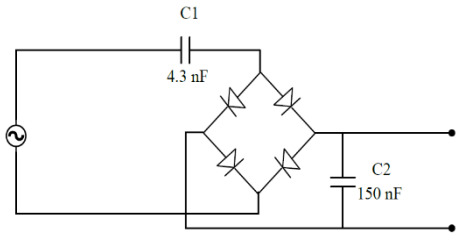


Рисунок 2. *Еквівалентна схема заміщення п'єзоелектричного перетворювача*

Змінна напруга від генераторного блоку надходить до зарядного кола, де здійснюється її випрямлення мостовим діодним випрямлячем та згладжування фільтрувальним конденсатором. Подальша стабілізація напруги виконується інтегральним регулятором, який забезпечує підтримання необхідного рівня зарядної напруги та коректний режим заряджання акумуляторної батареї.

Для запобігання зворотному струму використано захисний діод, що виключає розряджання акумулятора у випадку відсутності генерації. Контроль досягнення повного заряду реалізовано за допомогою вузла на основі стабілітрона та транзистора, що забезпечує автоматичне обмеження або припинення зарядного струму. Індикація режимів роботи здійснюється світлодіодами, а інформація про рівень заряду акумуляторної батареї відображається на рідкокристалічному дисплеї. Таким чином, запропонована електрична схема забезпечує ефективне випрямлення, стабілізацію, накопичення та контрольоване використання електричної енергії, генерованої п'єзоелектричними перетворювачами, що підвищує надійність та автономність системи живлення.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована автономна система живлення світлофорного об'єкта на основі п'єзоелектричного перетворення механічної енергії транспортного потоку продемонструвала технічну доцільність та енергетичну спроможність для забезпечення роботи навантаження. Проведені розрахунки та результати комп'ютерного моделювання підтвердили узгодженість параметрів генерації, накопичення та споживання електроенергії.

Аналіз енергетичного балансу показав, що навіть з урахуванням втрат у випрямлячі, стабілізаторі та акумуляторній батареї сумарний коефіцієнт корисної дії системи забезпечує можливість автономного функціонування світлофорного об’єкта. Використання масиву п’єзоелектричних елементів дозволяє масштабувати систему залежно від інтенсивності транспортного потоку.

Практична реалізація запропонованої системи може бути доцільною на ділянках із високою інтенсивністю руху та в умовах обмеженого доступу до централізованих мереж електроживлення.

ДЖЕРЕЛА

1. Бойко, Ю., Карпова, Л., & Гончар, А. (2026). Інтелектуальна багаторівнева система збору для бездротової енергії. Herald of Khmelnytskyi National University. Technical sciences, (1), 184–188.
2. Ковальчук, П., Бойко, Ю., & Карпова, Л. (2025). Інверторний DC-DC перетворювач для енергопостачання інформаційних систем. Інформаційні системи та технології: результати і перспективи: матеріали 2-ї Міжнародної науково-практичної конференції (5 березня 2025 р.) (с. 237–240). Київ: ФІТ КНУТШ.
3. Mou, K., & Ji, X. (2025). Using piezoelectric technology to harvest energy from pavement: A review. Journal of Traffic and Transportation Engineering (English Edition), 12(1), 68–86.
4. He, Q., & Briscoe, J. (2024). Piezoelectric energy harvester technologies: Synthesis, mechanisms, and multifunctional applications. ACS Applied Materials & Interfaces, 16(23), 29491–29520.
5. Al Ghazi, A., et al. (2025). Advances in interface circuits for self-powered systems: Piezoelectric energy harvesting. Sensors, 25(13), 4029.



ПАВЛО ТОМУСЯК
Здобувач ступеню бакалавра з електронних комунікацій та радіотехніки, група ЕКРс-23-1, у Хмельницькому національному університеті.
E-mail: boiko_julius@ukr.net
Здобувач працює над кваліфікаційною роботою на тему «Автономна система живлення електронних пристроїв». Наукові інтереси: системи збору та перетворення альтернативної енергії, п’єзоелектричні перетворювачі, автономні системи живлення об’єктів інфраструктури, оптимізація енергетичного балансу та підвищення енергоефективності електронних систем.



ЮЛІЙ БОЙКО
д.т.н., професор, професор кафедри телекомунікацій, медійних та інтелектуальних технологій, Хмельницький національний університет.
ORCID:0000-0003-0603-7827
E-mail: boykoym@khmnu.edu.ua
Отримав ступінь доктора технічних наук за спеціальністю «Радіотехнічні пристрої та засоби телекомунікацій» у Державному університеті телекомунікацій (Київ, Україна) у 2015 році. Наукові інтереси: обробка сигналів, синхронізація, телекомунікації, кодування, електронні компоненти, діагностика, інформаційні системи.



ЛЕСЯ КАРПОВА
к.т.н., доцент, доцент кафедри телекомунікацій, медійних та інтелектуальних технологій, Хмельницький національний університет.
ORCID ID: 0000-0001-5015-2107
E-mail: rtlesya@gmail.com
Отримала ступінь кандидата технічних наук за спеціальністю «Радіотехнічні та телевізійні системи» у Хмельницькому національному університеті у 2012 році. Наукові інтереси: телекомунікації, електронні компоненти, проєктування та оптимізація радіотехнічних систем, бездротова передача даних, антенні системи.

IOT-СИСТЕМА ЗАБЕЗПЕЧЕННЯ КОМФОРТНИХ УМОВ ПРОЖИВАННЯ ЛЮДЕЙ З ДОДАТКОВИМИ ПОТРЕБАМИ

Софія Ушакова, Ольга Кравченко

Анотація. *Розробка IoT-системи для забезпечення комфортних умов проживання людей з додатковими потребами передбачає автоматизацію управління температурою, освітленням, вологістю та іншими параметрами середовища. Така система дозволяє адаптувати умови житла до індивідуальних потреб користувачів, забезпечуючи зручність, безпеку та автономність. Дослідження фокусується на ефективності впровадження IoT-технологій у повсякденне життя людей з обмеженими можливостями, покращуючи їхнє середовище проживання.*

Ключові слова: IoT, система для людей з додатковими потребами, комфорт, безпека, автоматизація, розумний будинок.

I. ВСТУП

Сучасні виклики, зокрема війна в Україні, створюють нові соціальні потреби, серед яких зростає кількість людей з обмеженими можливостями. Військові конфлікти призводять до травм, інвалідності та інших обмежень, що змушує значну частину населення стикатися з труднощами в повсякденному житті. У таких умовах важливою стає адаптація та покращення умов життя для людей з обмеженими можливостями, щоб забезпечити їм більше автономії та незалежності. Рішенням цього питання може стати розробка та впровадження інноваційних технологій, зокрема систем на основі Інтернету речей (IoT), що дозволяють автоматизувати процеси і створювати комфортне середовище для кожного користувача. Тому розробка IoT-систем для забезпечення комфортних умов проживання людей з додатковими потребами[1] є надзвичайно актуальною і перспективною на сьогоднішній день.

Інтернет речей (IoT) відкриває нові можливості для забезпечення комфортних умов проживання людей з додатковими потребами. Завдяки інтеграції розумних пристроїв, таких як датчики температури, вологості, освітленості та системи безпеки, створюються умови для автоматичного управління параметрами навколишнього середовища, що покращує якість життя. IoT-системи дозволяють адаптувати житловий простір під індивідуальні потреби користувачів, забезпечуючи їхній комфорт, безпеку та автономність. Це дозволяє людям з обмеженими можливостями відчувати більшу незалежність у повсякденному житті та зменшити необхідність у сторонній допомозі.

II. ДАНІ ТА МЕТОДИ

У розробленій IoT-системі для забезпечення комфортних умов проживання людей з додатковими потребами використовуються сенсори для збору даних про температуру, вологість, освітленість та рух у приміщеннях. Дані передаються через бездротові технології, такі як Wi-Fi, ZigBee та MQTT[2], на центральний сервер для обробки. Алгоритми аналізують ці дані та коригують умови в будинку, автоматично змінюючи параметри середовища відповідно до потреб користувача. Система також забезпечує інтуїтивно зрозумілий інтерфейс для користувачів і захист даних, підвищуючи комфорт, безпеку та автономність осіб з додатковими потребами. Для аналізу даних використовуються методи машинного навчання, що дозволяють системі адаптуватися до змінних умов середовища та оптимізувати роботу. Всі передані дані шифруються для забезпечення конфіденційності та захисту особистої інформації користувачів. Впровадження таких технологій забезпечує

високу точність управління параметрами середовища та дозволяє досягти максимального комфорту для користувачів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті була розроблена IoT-система для забезпечення комфортних умов проживання людей з додатковими потребами, яка автоматизує управління температурою, вологістю, освітленням та безпекою в розумному будинку. Для детального опису процесів роботи системи було використано діаграму діяльності, що представлена нище на Рисунку 1, яка наочно відображає основні етапи її функціонування. Збір даних з сенсорів починається з вимірювання параметрів навколишнього середовища, таких як температура, вологість та освітленість. Потім ці дані передаються до серверу, де за допомогою алгоритмів здійснюється їх обробка. Якщо параметри не відповідають заданим значенням, система ініціює коригування умов, наприклад, змінюючи температуру або освітленість, а також інформує користувача через мобільний додаток.

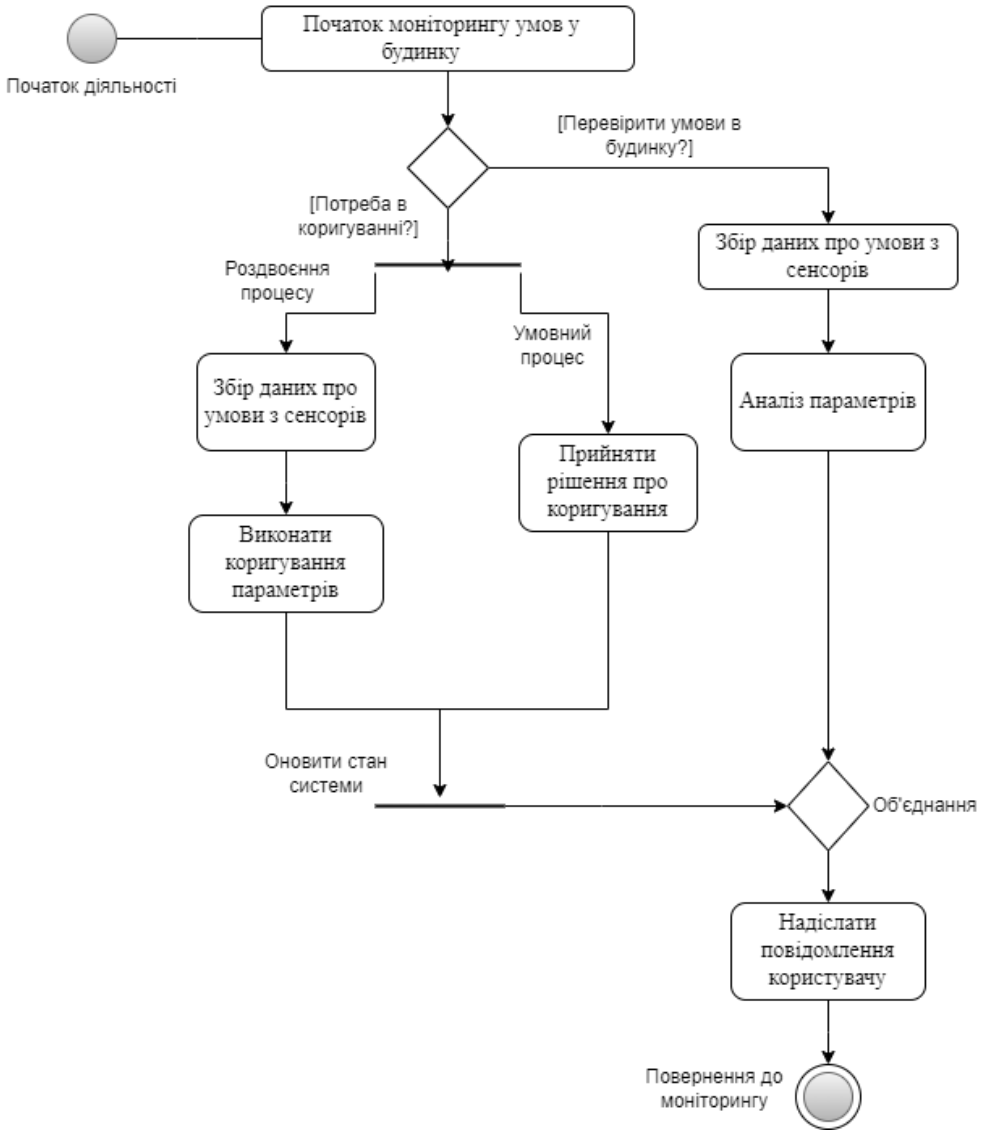


Рисунок 1. *Діаграма діяльності IoT-системи для забезпечення комфортних умов проживання в будинку.*

Процес взаємодії між компонентами системи також був змодельований за допомогою діаграми послідовності[4] на Рисунку 2. Вона показує, як дані передаються від сенсорів до центрального аналізатора, який, отримавши інформацію, проводить порівняння з оптимальними значеннями для кожного параметра. Якщо система виявляє, що значення не відповідають необхідним умовам, вона передає команду до коригуючого модуля для виконання відповідних змін, таких як регулювання температури, вологості або освітлення. Після виконання коригувань система надає зворотний зв'язок і може повторно оцінює ефективність змін, що дозволяє їй підтримувати постійний комфорт і безпеку в приміщенні. Ця діаграма підкреслює точність послідовність дій у системі, яка забезпечує автоматичну адаптацію середовища до змінних умов.

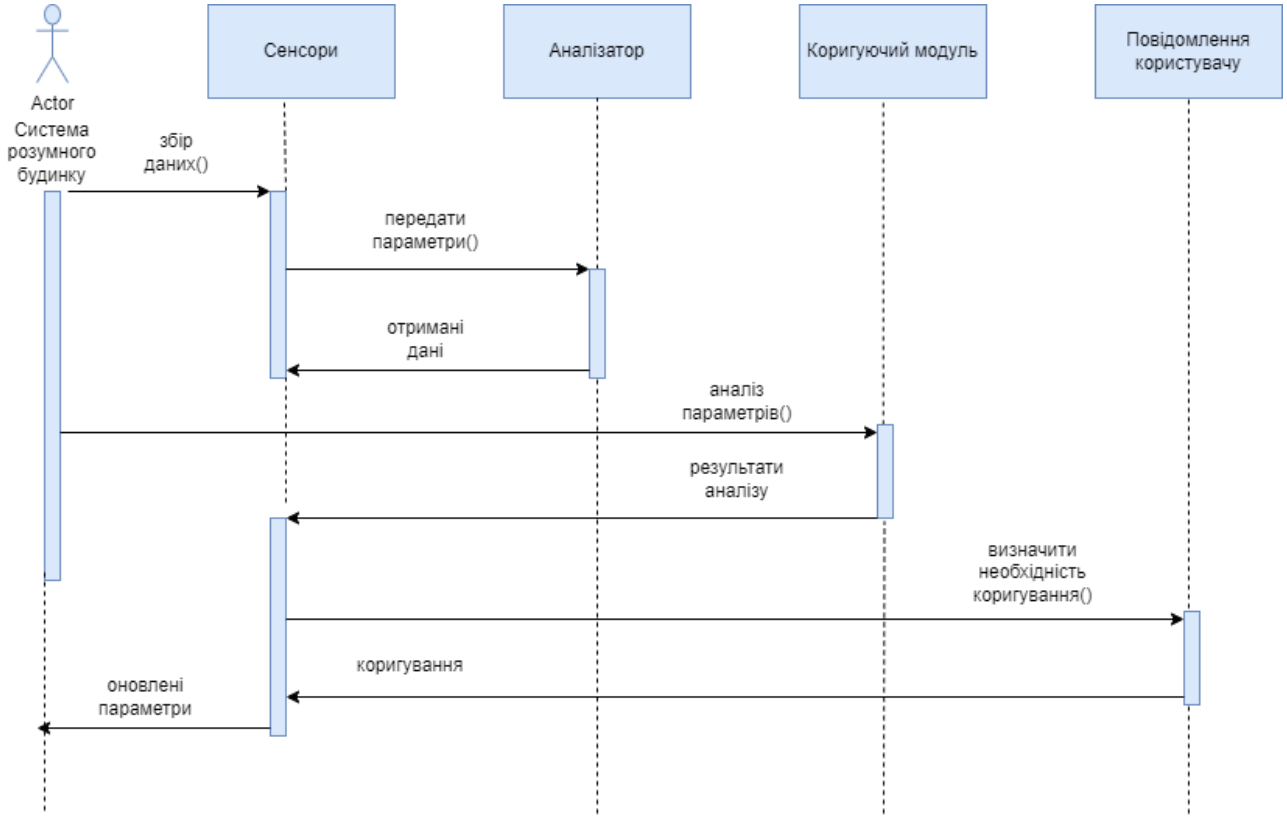


Рисунок 2. *Діаграма послідовності IoT-системи для забезпечення комфортних умов проживання в будинку.*

Інтеграція алгоритмів для автоматичного коригування умов дозволяє адаптувати систему до індивідуальних потреб користувачів, забезпечуючи їм високий рівень автономії. Розроблена система автоматично моніторить параметри навколишнього середовища, своєчасно реагує на зміни та підтримує комфортні умови без необхідності в додатковому втручанні.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Аналіз результатів показав, що система забезпечує високий рівень точності при вимірюванні параметрів середовища завдяки інтеграції сучасних сенсорів. Вона ефективно реагує на зміни в умовах приміщення та автоматично коригує температурні, освітлювальні та інші умови, що створює оптимальне середовище для людей з додатковими потребами. Це дозволяє користувачам не залежати від сторонньої допомоги в підтриманні комфорту.

Розроблена IoT-система є потужним інструментом для поліпшення якості життя людей з обмеженими можливостями. Таким чином, IoT-система забезпечує високий рівень автоматизації і адаптивності до умов середовища, що робить її важливим інструментом для покращення умов проживання людей з додатковими потребами. Система демонструє свою ефективність у забезпеченні комфорту, знижуючи потребу в сторонній допомозі та надаючи користувачам більшу автономність у повсякденному житті.

Система має значний потенціал для подальшого розвитку та удосконалення, оскільки її можна адаптувати для інтеграції з новітніми технологіями, такими як 5G, штучний інтелект та більш точні сенсори, що дозволить ще ефективніше контролювати та адаптувати середовище для користувачів. У майбутньому система може бути вдосконалена завдяки розширеній автоматизації процесів, покращеному прогнозуванню потреб користувачів і гнучким налаштуванням, що забезпечать більшу персоналізацію та зручність. Це дозволить створювати ще більш інклюзивне середовище, яке адаптується до змінних потреб та вимог користувачів.

ДЖЕРЕЛА

1. IoT-based Smart Home System for People with Disabilities. URL:https://www.cogniteq.com/blog/iot-people-disabilities-how-technology-makes-their-lives-better
2. Інформація про MQTT. URL: https://fiberroad.com/uk/why-is-mqtt-an-important-part-of-iot/
3. D. B. Rawat, M. B. Y. Soni, "Design and Implementation of IoT-based Smart Home for Elderly and Disabled People," Journal of Electrical Engineering & Technology, vol. 15, no. 2, pp. 633-640, 2020.
4. S. M. Yousef, A. Z. Abidin, "Sequence Diagram and UML Tools for Software Development," International Journal of Advanced Computer Science and Applications, vol. 12, no. 9, pp. 1-8, 2021.
5. A. S. R. Anjaneyulu, M. L. Mazumder, and P. K. S. R. Rao, "Smart Home Automation for Elderly and Disabled: IoT-based Approach," Springer Smart Innovation, Systems and Technologies, vol. 20, pp. 155-164, 2022.



СОФІЯ УШАКОВА
студентка 4 курсу кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка (Київ, Україна).
E-mail: sofia.ushakova15@gmail.com
Наукові інтереси: Розробка адаптивних IoT-систем для покращення якості життя людей з обмеженими можливостями. Аналіз і дослідження протоколів зв'язку для IoT-систем в умовах розумного будинку.



ОЛЬГА КРАВЧЕНКО
к.т.н., доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка (Київ, Україна).
ORCID: 0000-0002-9669-2579
E-mail: olha.kravchenko@knu.ua
Наукові інтереси: Проєктування систем моніторингу та прогнозування з урахуванням правил штучного інтелекту на основі поведінкової економіки. Застосування IoT.

RULE-BASED DIGITAL TWIN ДЛЯ ЗАБЕЗПЕЧЕННЯ НОРМАТИВНОЇ ВІДПОВІДНОСТІ У ВИБУХОНЕБЕЗПЕЧНИХ РОБОТАХ

Даніїл Філатов

Анотація. *У роботі розглянуто підхід до побудови rule-based Digital Twin для контролю нормативної відповідності у роботах з вибухонебезпечними середовищами та матеріалами. Основу підходу становлять формалізація нормативних вимог у вигляді машинно-читаних правил, використання event log / digital thread та формування evidence пар. Запропоноване рішення орієнтоване на підвищення простежуваності, виявлення відхилень і забезпечення доказовості виконання вимог.*

Ключові слова: Digital Twin; нормативна відповідність; rule-based systems; event log; audit trail; вибухонебезпечні роботи

I. ВСТУП

Охорона праці та безпека (OHS) у критично важливих для безпеки сферах охоплює не лише документальне забезпечення, а й питання узгодженості, простежуваності та підзвітності. У роботах з підвищеним рівнем ризику, зокрема там, де наявні вибухонебезпечні середовища та матеріали, нормативні вимоги та регламентуючі документи з охорони праці й безпеки визначають необхідні умови виконання робіт: допуски, обмеження, контроль зон, облік, зберігання, порядок дій та перевірок. На практиці відповідність цим вимогам часто спирається на розрізнені артефакти — тексти нормативів, локальні інструкції, журнали, акти та підписи відповідальних осіб. Така фрагментованість ускладнює оперативне виявлення відхилень, відтворення послідовності подій і формування доказової основи відповідності фактичного перебігу виробничого процесу встановленим вимогам. [1, 2].

Підхід цифрових двійників (Digital Twin, DT) у safety-critical доменах розглядається як спосіб узгодження даних процесу та контексту робіт у межах єдиної моделі стану. Водночас для завдань нормативної відповідності ключового значення набувають: (1) перетворення текстових вимог у машинно-читані правила; (2) відтворюваність перевірок на основі подієвих даних; (3) інтерпретованість результатів у формі «вимога → факти → висновок → рекомендована дія»; та (4) формування доказового сліду (audit trail), придатного для аудиту й розслідувань. [2-4].

II. ДАНІ ТА МЕТОДИ

У дослідженні використано нормативні та регламентуючі документи з охорони праці й безпеки, а також описані сценарії виконання робіт, пов’язаних із поводженням із вибуховими матеріалами [1]. Як дані для подальшої формалізації розглядаються вимоги нормативних актів, локальні процедури підприємств, журнали обліку, записи про допуски, перевірки, переміщення та інші події, що характеризують фактичний перебіг виробничого процесу. Такий набір джерел дає змогу поєднати регуляторний, організаційний та операційний контури в межах єдиного підходу до перевірки відповідності.

Запропонований підхід орієнтований на побудову rule-based Digital Twin (DT) для забезпечення простежуваної нормативної відповідності в операціях, пов’язаних із вибухонебезпечними роботами та поводженням із вибуховими матеріалами. Його методичну основу становить поєднання подієвого представлення процесів і механізму доказового підтвердження виконання або порушення вимог. У межах такого підходу правила формують

логічний зв'язок між текстом нормативу, фактичними подіями процесу та висновком про відповідність [3, 4].

Підхід передбачає: формування моделі предметної області, у якій набір сутностей уточнюється відповідно до вибраних нормативних вимог і сценаріїв; побудову подієвого представлення процесів у вигляді event log / digital thread для забезпечення простежуваності; розробку бібліотеки машинно-читаних правил; а також побудову карти доказовості (evidence map / audit trail), що пов’язує правила з мінімально достатнім набором даних і подій для підтвердження виконання вимоги або фіксації її порушення.

Подієве представлення процесів розглядається як послідовність подій із часовими мітками, учасниками, ідентифікаторами об’єктів та контекстом операції, що створює основу для відтворюваних перевірок і подальшого аналізу відхилень. На контекстній діаграмі (Рис. 1) показано взаємодію системи з основними зовнішніми джерелами та споживачами інформації: регуляторними джерелами, підприємством, операційними системами та журналами, а також аудитом, керівництвом і HSE як отримувачами звітності та пакетів доказів.

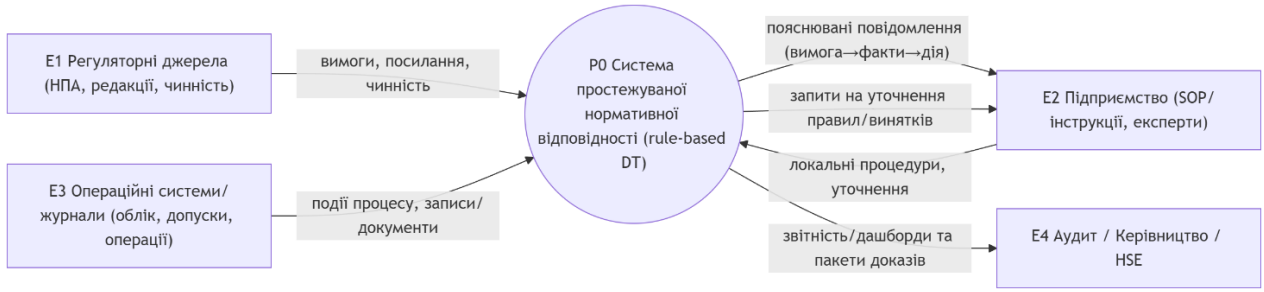


Рисунок 1. *Контекстна діаграма rule-based Digital Twin*

Підхід передбачає інтеграцію кількох взаємопов’язаних компонентів: моделі предметної області, подієвого представлення процесів, бібліотеки машинно-читаних правил і карти доказовості. У межах такого підходу правила розглядаються як зв’язувальна ланка між текстом нормативу, фактами виконання операцій і висновком про відповідність. Діаграма відображає ключові інформаційні потоки — надходження вимог і подій процесу до системи та формування пояснюваних повідомлень, запитів на уточнення правил/винятків і звітних матеріалів. [3, 4].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

За результатами проведеного дослідження сформовано ключові елементи запропонованого підходу та напрями його подальшої перевірки. Виокремлено таксономію типових «вузьких місць» формалізації вимог, що охоплює питання застосовності, винятків, деонтики, чинності/версійності та вимог до доказів. Запропоновано також шестирівневу модель переходу від нормативного тексту до виконуваних перевірок на подієвих даних («текст → структура → семантика → правила → виконання → докази»), яка задає послідовність перетворення вимоги на перевірювану умову.

Така модель дає змогу формалізувати логіку цього переходу, зберігаючи простежуваність між текстовим джерелом вимоги, її машинно-читаним представленням, результатом перевірки та доказовою основою висновку. Окремо сформовано попередню рубрику оцінювання класів інструментів - workflow/EHS/PTW-платформ і rule/decision/policy engines - з фокусом на executable compliance, зокрема простежуваність до джерела, керування версіями, інтерпретованість, повноту audit trail і можливість регресійного тестування [3, 4].

Розроблено шаблон проміжного артефакту Rule Card для стандартизованого переходу від пункту нормативу до правила з фіксацією контексту, умов і винятків, потрібних даних,

доказів, джерела та чинності. Завершальним елементом є план стендової апробації на відтворюваних сценаріях із синтетичними журналами подій.

У сукупності ці напрацювання окреслюють структурну та методичну основу підходу, а також створюють підґрунтя для подальшого обговорення його науково-практичного внеску та можливостей апробації.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонований підхід дає змогу розглядати нормативну відповідність не як сукупність розрізнених документальних підтверджень, а як формалізований і простежуваний процес, пов’язаний із фактичним перебігом операцій. У цьому контексті науково-практичний внесок підходу полягає у формуванні стандартизованого ланцюжка переходу від нормативного тексту до виконуваних перевірок і відтворюваних доказів, а також у визначенні вимог до інструментів, здатних забезпечувати executable compliance у DT-орієнтованих системах. [3, 4].

Оцінювання підходу передбачає використання сценаріїв нормальної роботи та типових порушень на основі синтетичних event log із подальшою кількісною валідацією за метриками coverage, detection rate, explainability та audit readiness. Очікується, що запропонований підхід забезпечить відтворювані перевірки відповідності, прозоре пояснення їхніх результатів і формування повного доказового сліду для аудитів та післяінцидентних розслідувань. Подальша робота передбачає перевірку підходу та уточнення правил з урахуванням винятків і контекстних обмежень локальних процедур підприємств. [2].

ДЖЕРЕЛА

1. UN SaferGuard (UNODA). 2021. International Ammunition Technical Guidelines (IATG) 07.10: Safety and Risk Reduction (Version 3). United Nations Office for Disarmament Affairs. [online]. Доступно: https://data.unsaferguard.org/iatg/en/V3_IATG-07.10_en.pdf.
2. Park J.-S., Lee D.-G., Jimenez J. A., Lee S.-J., Kim J.-W. 2023. Human-Focused Digital Twin Applications for Occupational Safety and Health in Workplaces: A Brief Survey and Research Directions. Applied Sciences, 13(7), 4598. [online]. Доступно: https://doi.org/10.3390/app13074598.
3. Andrew Mowbray, Philip Chung, Graham Greenleaf. 2023. Representing legislative Rules as Code: Reducing the problems of 'scaling up'. Computer Law & Security Review, 48, 105772. [online]. Доступно: https://doi.org/10.1016/j.clsr.2022.105772.
4. Enrico Francesconi, Guido Governatori. 2023. Patterns for legal compliance checking in a decidable framework of linked open data. Artificial Intelligence and Law, 31(3), 445-464. [online]. Доступно: https://doi.org/10.1007/s10506-022-09317-8.



ДАНІЇЛ ФІЛАТОВ
Аспірант, кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0004-7064-591X
E-mail: daniel.filatov.2001@gmail.com
Напрями досліджень включають цифрові двійники для безпеки, правила як код (Rules-as-Code), подієву простежуваність (digital thread) та доказовість нормативної відповідності.

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МОНІТОРИНГУ СТАНУ ПАЦІЄНТІВ В IOT СИСТЕМАХ

Юрій Ярошенко, Володимир Дружинін

Анотація. *У роботі представлено розробку IoT-системи моніторингу стану пацієнтів у клінічному середовищі. Система інтегрує мережу носимих медичних сенсорів (пульсоксиметр, термометр, датчик тиску, акселерометр) та механізми автоматичного виявлення відхилень від норми. Передача даних здійснюється за протоколом WebSocket до серверної частини на базі Python Flask, обробка — з використанням адаптивної моделі порогового сповіщення та алгоритму Isolation Forest. Розроблений мобільний додаток надає медперсоналу зведений перегляд стану палат, показники пацієнтів у реальному часі та систему push-сповіщень. Впровадження системи забезпечує безперервний контроль стану пацієнтів, зниження кількості хибних тривог та підвищення оперативності медичного персоналу.*

Ключові слова: Інтернет речей, моніторинг пацієнтів, IoT, виявлення аномалій, мобільний додаток, медичні сенсори, клінічна інформаційна система.

I. ВСТУП

Моніторинг стану пацієнтів є одним із ключових завдань сучасної медицини, від ефективності якого безпосередньо залежить якість лікування та своєчасність реагування на критичні зміни. Традиційні підходи до спостереження за показниками здоров'я передбачають ручне зняття даних медичним персоналом, що є трудомістким процесом і не забезпечує безперервності контролю. Технології Інтернету речей відкривають нові можливості для автоматизованого збору, передачі та аналізу медичних даних у реальному часі. Проте існуючі IoT-рішення у медицині мають ряд недоліків: недостатню адаптивність до індивідуальних норм пацієнта, відсутність інтегрованих механізмів виявлення аномалій та обмежені можливості для персоналу клініки щодо перегляду зведеного стану палат. Метою даної роботи є розробка моделей та методів підвищення ефективності моніторингу стану пацієнтів в IoT-системах, а також реалізація мобільного додатку для клінічного персоналу.

II. ДАНІ ТА МЕТОДИ

Розроблена IoT-система моніторингу стану пацієнтів складається з трьох рівнів: рівня пристроїв, рівня передачі даних та рівня обробки і відображення інформації. На рівні пристроїв використовуються носимі медичні сенсори: пульсоксиметр, для вимірювання кисню в крові, термометр, датчик артеріального тиску.

Передача даних здійснюється за протоколом WebSocket до серверної частини на базі Python Flask. На рівні обробки застосовується адаптивна модель порогового сповіщення з урахуванням індивідуальних норм пацієнта, а також метод виявлення аномалій на основі алгоритму Isolation Forest.

Мобільний додаток надає клінічному персоналу зведений перегляд стану палат, список пацієнтів із поточними показниками, журнал тривог та детальну картку кожного пацієнта з графіками динаміки показників.

Нижче можемо переглянути структурну схему архітектури (Рисунок 1) та порівняльну таблицю вже існуючих систем (Таблиця 1).

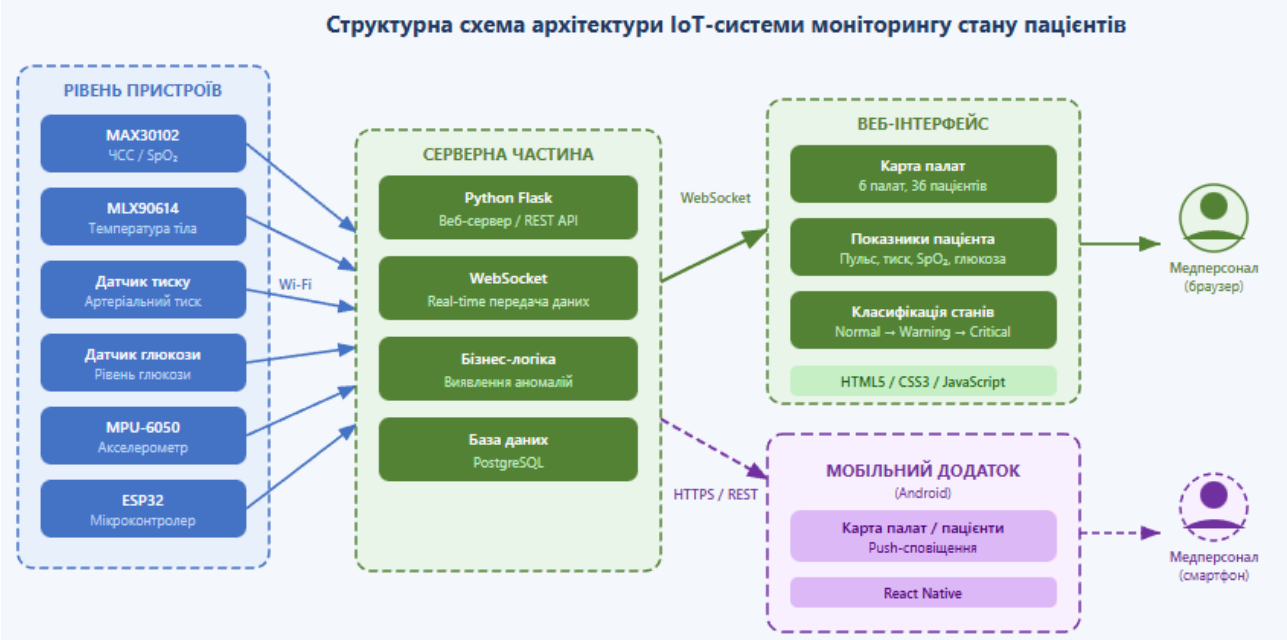


***Рисунок 1**. Структурна схема архітектури*

***Таблиця 1.** Порівняльна таблиця існуючих систем моніторингу*

Система	Показники	Мобільний додаток	Сповіщення	Адаптивні пороги	Виявлення аномалій
Philips HealthSuite	ЧСС, SpO_2, темп.	✓	✓	✗	✗
Apple Health (ResearchKit)	ЧСС, ЕКГ, акселерометр	✓	✓	✗	✗
Google Health (Fitbit)	ЧСС, SpO_2, сон	✓	✓	✗	✗
HealthFog (Tuli et al., 2020)	ЧСС, ЕКГ, тиск	✗	✓ (mail)	✗	✓
Розроблена система	**ЧСС, SpO_2, темп., тиск, акселерометр**	✓	✓ **(push)**	✓	✓

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Розроблена система забезпечує безперервний збір показників стану пацієнтів з інтервалом оновлення не більше 5 секунд. Адаптивна модель порогового сповіщення дозволяє знизити кількість хибних тривог порівняно з системами із фіксованими порогами, оскільки враховує індивідуальні базові показники кожного пацієнта.

Мобільний додаток реалізує відображення поточного стану всіх палат у вигляді інтерактивної карти з кольоровою індикацією стану (норма / увага / критично), перегляд детальних показників кожного пацієнта в реальному часі, push-сповіщення при виявленні відхилень, а також перегляд архіву показників у вигляді часових графіків.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі представлено дослідження з розробки IoT-системи моніторингу стану пацієнтів та мобільного додатку для клінічного персоналу. Запропонована адаптивна модель порогового сповіщення та метод виявлення аномалій на основі Isolation Forest забезпечують вищу точність і меншу кількість хибних тривог порівняно з існуючими підходами. Розроблений мобільний додаток надає персоналу зручний інструмент для контролю стану пацієнтів у реальному часі.

ДЖЕРЕЛА

1. Ahad A., Tahir M., Aman Sheikh M. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. IEEE Access. 2019. Vol. 7. pp. 100747–100762.
2. Islam S.M.R., Kwak D., Kabir H. The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access. 2015. Vol. 3. pp. 678–708.
3. Kang M., Park E., Cho B.H. Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices. International Neurourology Journal. 2018. Vol. 22, №2. pp. 76–82.
4. Gatouillat A., Badr Y., Massot B., Sejdić E. Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine. IEEE Internet of Things Journal. 2018. Vol. 5, №5. pp. 3810–3822.
5. Tuli S., Basumatary N., Gill S.S. HealthFog: An Ensemble Deep Learning Based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in Integrated IoT and Fog Computing Environments. Future Generation Computer Systems. 2020. Vol. 104. pp. 187–200.



ЮРІЙ ЯРОШЕНКО
студент, ОП Програмні технології Інтернету речей, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0004-6904-8966
E-mail: yaroshenkoyu@fit.knu.ua
здобуває ступінь магістра комп'ютерних наук у Київському національному університеті імені Тараса Шевченка (Київ, Україна). Серед наукових інтересів – системи комп'ютерного моніторингу та контролю.



ВОЛОДИМИР ДРУЖИНІН
д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@fit.knu.ua
Коло наукових інтересів: методи та алгоритми машинного навчання в радіолокаційних системах, радіомоніторинг та радіочастотний менеджмент, багатопозиційна радіолокація.

Section

Digital Technology of Project Management

Секція

Цифрові технології управління проєктами

A MOBILE APPLICATION FOR LEARNING FOREIGN LANGUAGES AS A SOLUTION FOR MICROLEARNING: APPLICATION CONCEPT AND GAMIFICATION TOOLS

Viktoriia Bytska, Vadym Ziuziun

Abstract. *The research considers the concept of a mobile application for studying foreign vocabulary, which is based on a combination of spaced repetition, microlearning and gamification as functional components of a single educational system. Existing approaches to studying foreign vocabulary are analysed and their main drawbacks are identified. Based on this, the conceptual principles of the application are formulated. Special attention is paid to the gamification system as a functional mechanism for supporting motivation and forming a sustainable habit of daily learning.*

Keywords: mobile application, vocabulary learning, spaced repetition, microlearning, gamification, personalization of learning

I. INTRODUCTION

The effective acquisition of vocabulary has always been and remains a residual factor in learning foreign languages, the latter being the basis for the development of speech skills. Without an adequate vocabulary base, it becomes challenging to comprehend texts, articulate ideas, or participate in meaningful interaction, thereby limiting the functional use of the target language. Traditional approaches to vocabulary learning, such as rote memorisation and dictionary-based exercises, often prove insufficient in ensuring long-term retention and sustained engagement. These methods often do not engage learners, provide little context for the use of words, and do not take into account individual learning styles or needs.

The rapid digitalization of education opens up new opportunities for developing innovative solutions in the field of foreign language learning. In particular, a promising direction is the creation of digital applications that combine interactive exercises, spaced repetition systems, and gamification tools. According to the research, «The Influence of Gamification on English Vocabulary Retention in Online Learning Platforms» [0], the introduction of game-based learning strategies, particularly through interactive games and systematic exposure to new vocabulary, has a positive effect on the acquisition of new words for English as L2 learners. Her findings suggest that this approach not only yields positive results in the context of vocabulary memorisation, but also increases the level of motivation.

Moreover, the integration of digital learning environments aligns with contemporary patterns of information consumption and professional development, where technology-mediated learning has become an integral part of everyday practice. As a result, digitally supported vocabulary acquisition represents not only a methodological innovation but also a response to broader socio-technological changes in modern education.

II. APPLICATION CONCEPT

The main idea is to create a mobile application that combines the principles of spaced repetition, contextual learning and microlearning in a single daily practice. There are many similar solutions on the market, but most of them either overload the user with content and functionality, or are reduced to simply viewing flashcards without a systematic logic of repetition. At this time, the proposed concept of the application is between these extremes, offering a clearly dosed daily

session, where the number of words is deliberately limited. It is planned not due to simplification, but as a methodological solution based on the principles of human memory.

The key difference of the application is that learning here is not a linear accumulation of new material. The repetition system is based on an algorithm according to which each word marked by the user as learned does not disappear from the learning process. It returns after certain intervals of time - at first more often, then less often, in accordance with the Ebbinghaus forgetting curve. The study «Enhancing Vocabulary Acquisition and Retention: The Role of Spaced Repetition in Language Learning» [0], conducted at a Thai university with the participation of 30 students who studied 104 words for a month using a structured interval repetition schedule, recorded a significant increase in the average score from 11.57 to 21.93 points, and the level of vocabulary retention after completing the practice remained at about 79%, which convincingly proves the effectiveness of spaced repetition as a method of long-term vocabulary acquisition and justifies its integration into the basis of the application's learning algorithm. It also ensures the transfer of vocabulary from short-term to long-term memory without the need to consciously plan repetition. Each session organically combines new words with a return to previously learned, and the words themselves are presented not in isolation, but through short situational contexts, which bring the learning process closer to natural language experience. The system automatically tracks which words need repetition, forming a personalized learning route without the need to manually configure anything.

Another feature of the application is the rethinking of the progress system, where instead of the standard CEFR A1-C2 level scale, the application uses metaphorical landmarks tied to real language situations, which makes progress tangible and motivating. Combined with passive contact with words through a widget and AI-supported pronunciation, this forms a holistic ecosystem of daily interaction with language not as a learning task, but as a habitual part of the day.

III. KEY ELEMENTS OF GAMIFICATION

Gamification in the context of mobile educational applications involves the integration of game mechanics into a non-migratory environment in order to increase user engagement and maintain their motivation to regularly interact with content. Within the application, it is planned to implement gamification not as a decorative element, but as a functional system, each component of which performs a specific role in the learning process. The table below lists the key gamification elements, their functional purpose, method of implementation, and priority in development (Table 1).

IV. INTENDED OUTCOMES AND USER BENEFITS

The implementation of the application is aimed at achieving a comprehensive result in which methodological efficiency, user experience and technological component work as a single system.

1. *Vocabulary growth*. The main measurable result is the user's assimilation of at least 150 lexical units per month – an indicator achievable thanks to daily structured sessions of seven words, an interval repetition algorithm and regular knowledge testing through exercises and tests. In addition, the result is planned to be achieved without the need to allocate significant time or exert excessive effort, because the microformat of learning allows you to build it into the usual rhythm of the day without feeling burdened.
2. *Pronunciation development*. A separate expected result is the improvement of the user's pronunciation. The integration of AI-sounding and the function of recording your own pronunciation allows the user not only to memorize words visually, but also to form correct phonetic patterns from the first stages of learning. In combination with contextual examples of use, this ensures the assimilation of the word in full.

3. *Sustained motivation and habit formation*. An equally important result is a qualitative change in the user's attitude towards the learning process. Most people who try to learn a language on their own do not face a lack of resources, but a lack of motivation and regularity. That is why the gamification system is built in such a way as to maintain engagement not through one-time bursts of interest, but through the formation of a stable habit. Streak mechanics, a multi-level reward system for different types of achievements, and visualization of progress through metaphorical levels create an environment in which the user receives positive reinforcement at each stage, regardless of whether he has just started learning or already has a significant vocabulary.
4. *Personalized learning experience*. In parallel with the motivational dimension, the application is planned to provide deep personalization of the learning process. The ability to choose thematic categories, level of difficulty, and form his own word lists allows each user to adapt the application to specific goals. The repetition algorithm automatically takes into account individual progress, determining which words need additional consolidation and which can be postponed for a longer interval. So each user's learning path is unique, even if the initial content is the same.

Table 1. *Planned gamification elements in the system*

Gamification element	**The goal is to engage the user in learning in the app**	**Method of implementation**	**Development priority**
Daily limit «7 words per day» (5 new + 2 for repetition)	Forming a habit of regular study and preventing overload	Automatic daily word updates; includes 5 new words and 2 for review; words are selected based on previous mistakes and user level	1
Flashcards with mini-context	Improving memory through associations and contextual learning	The card contains a word, translation, short sentence/situation; flip button; ability to listen to pronunciation; difficulty adaptation to the user's level	2
Interactive tests	Reinforcing the material and supporting active participation	Exercises like: match the word and the meaning, fill in the blank, choose the correct option; automatic grading; hints for errors	1
Weekly and monthly tests	Motivation for long-term learning and self-assessment of progress	Automatic generation of tests based on words marked as «studied»; various types of questions; user progress statistics; results notification	2
Streak system (series of days without gaps)	Forming a stable study habit and daily activity	Counter of consecutive days without gaps; visualization of the series (strip) in the form of a graph; reminder about gaps; integration with the application calendar	2
Rewards and achievements system	Increased intrinsic motivation and a sense of progress	Badges and achievements: 3 days without missing, repeated old words, passed weekly test; visual effects; notification about receiving an award	3
Personal word lists	Individualizing learning and increasing engagement	Ability to create personal word lists; training of individual lists; repetition statistics; integration with daily plan	3
Creative levels (instead of A1-C2)	Creating emotional attachment and a sense of accomplishment	Levels: Podcast Listener (500 words), Netflix Watcher (1000 words), Book Reader (2000 words); progress display; motivational messages	4

Thus, the application will represent a personal environment for the systematic and conscious development of lexical competence, accessible at any time and adapted to the real needs of the modern user.

V. DISCUSSIONS AND CONCLUSION

The research considers the concept of a mobile application for learning foreign vocabulary, which is based on scientifically sound methods – spaced repetition, microlearning and contextual word learning. The existing approaches to learning vocabulary are analysed and their main shortcomings are identified: the lack of a systematic logic of repetition, a low level of user involvement and ignoring individual needs. Based on this, the conceptual principles of the application are formulated, which occupies an intermediate position between platforms overloaded with functionality and simple sets of flash cards.

Special attention is paid to the gamification system, which is considered as a functional mechanism for supporting motivation. The article describes specific game mechanics and determines their role in forming a sustainable habit of daily learning.

The expected results and value for the user include both quantitative indicators (mastering at least 150 lexical units per month) and qualitative changes (development of pronunciation, formation of motivation and personalization of the learning process). It is concluded that the integration of the interval repetition algorithm, gamification and microformat of learning into a single ecosystem allows creating an effective environment for the systematic development of lexical competence in the conditions of modern digital education.

REFERENCES

1. Arif U. Q. (2025), «The Influence of Gamification on English Vocabulary Retention in Online Learning Platforms», Jurnal Pendidikan dan Pembelajaran Indonesia (JPPI), vol. 5, no. 2, pp. 1044-1053, doi: 10.53299/jppi.v5i2.1468.

2. Saksittanupab P. (2024), «Enhancing Vocabulary Acquisition and Retention: The Role of Spaced Repetition in Language Learning», Journal of Modern Learning Development, vol. 9, no. 5, pp. 205-215. URL: https://so06.tci-thaijo.org/index.php/jomld/article/view/273598



VIKTORIIA BYTSKA
First-year master's student in IT project management at Taras Shevchenko National University of Kyiv
ORCID: 0009-0002-5107-1098
E-mail: vika.bytska@knu.ua
Research interests: IT project management, computer science, foreign languages, gamification of learning.



VADYM ZIUZIUN
Ph.D., Associate Professor, Associate Professor of the Department of Management Technologies, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv
ORCID: 0000-0001-6566-8798
E-mail: vadym.ziuziun@knu.ua
Since 2022, he has been working as an associate professor at the Department of Management Technologies at Taras Shevchenko National University of Kyiv. The experience of scientific and pedagogical activity is 13 years. Research interests: project management, risk management, information technology, transport technologies, ecology and environmental protection technologies, management.

DIGITAL TRANSFORMATION MODELS OF PROJECT MANAGEMENT SYSTEMS IN DEVELOPMENT COMPANIES

Volodymyr Kochuma

Abstract. *The theses consider the features of management systems of development companies and approaches to their digital transformation. The current state of digitalization in the development industry of Ukraine is analyzed, key challenges and opportunities are identified. An overview of transformation models is presented, including Agile transformation, digital maturity models (Digital Maturity Models), and specific approaches for the development business. The example of the company KAN Development illustrates the practical application of a combined approach to the digital transformation of the project management system. Prospects for further research are identified, conclusions are formulated.*

Keywords: project management, digital transformation, development company, transformation model

I. INTRODUCTION

Development companies in Ukraine and around the world are faced with the need for a fundamental transformation of management systems under the influence of the digitalization of the economy. Traditional approaches to managing construction projects, based on paper document flow, disjointed information systems and sequential decision-making processes, are proving to be insufficiently effective in the context of increasing project complexity, increased stakeholder demands and the need to accelerate market entry. The development business is characterized by a high level of capital intensity, long project implementation cycles (from 2 to 5+ years), the involvement of multiple contractors and subcontractors, a complex regulatory framework and the need to coordinate dozens of parallel processes. These features create both significant challenges for digital transformation and huge potential for increasing efficiency through the implementation of digital solutions. According to McKinsey research, the construction industry is one of the least digitized in the world, lagging behind manufacturing, retail and logistics. However, this very lag creates opportunities for achieving competitive advantages through the early implementation of digital technologies. Companies that successfully transform their management systems demonstrate an increase in productivity by 14-15%, a reduction in costs by 4-6% and a reduction in project implementation times by 10-20%. However, the digital transformation of development companies cannot be a simple implementation of software - it requires systemic changes in the organizational structure, business processes, personnel competencies and corporate culture. For successful transformation, a structured approach is required, based on proven models and adapted to the specifics of the development business. The purpose of the study is to analyze existing models of digital transformation and determine the most suitable approaches for transforming the management systems of development companies based on digitalization.

II. DATA AND METHODS

The study is based on an analysis of academic literature on project management, digital transformation and construction management, publications of consulting companies, industry reports and thematic case studies. To analyze the state of digitalization of the development industry in Ukraine, public company data, industry reviews and expert assessments were used.

The research methodology includes a comparative analysis of digital transformation models to identify their strengths and limitations in the context of the development business, a structural and functional analysis of development company management systems to identify critical points that require digitalization and determine priority areas of transformation, a case method for a detailed

consideration of the company KAN Development regarding the implementation of digital transformation and a synthetic approach to developing an integrated transformation model that combines elements of different frameworks and is adapted to the specifics of development companies.

III. RESULTS AND ANALYSIS

The management system of a development company is a complex multi-level structure that combines strategic management of a project portfolio, operational management of individual projects and functional management of supporting processes. The analysis shows that most Ukrainian developers are in the early stages of digital transformation. A typical “digital landscape” of an average development company includes: basic office applications (Microsoft Office, email), financial systems for accounting, a CRM system for sales management (often insufficiently integrated), individual specific solutions (estimating programs, design systems), lack of or weak integration between systems, a significant share of paper-based document flow, limited use of analytics and forecasting.

Key challenges of digitalization include: fragmentation of information systems and lack of a single source of data, resistance to change from staff, especially experienced specialists, difficulty integrating with contractor and partner systems, lack of standardized processes, which complicates automation, limited digital competencies, uncertainty of ROI from digital investments.

Let’s describe the models of transformation of management systems.

1. Agile Transformation Model.

Agile transformation, which originated in the software development industry, is gaining popularity in other industries, including construction and development. The model is based on the principles of flexibility, iterativeness, cross-functional collaboration, and customer value orientation.

Key elements for development companies.

Agile Portfolio Management – managing a project portfolio as a dynamic set of initiatives, where prioritization is based on value creation and strategic alignment, rather than rigid long-term planning.

Iterative Development – breaking large projects into phases/stages of construction with the ability to adapt subsequent phases based on feedback from the first. For example, the first stage of a residential complex acts as a pilot, based on which subsequent stages are adjusted.

Cross-functional Teams – creating project teams that include representatives of different functions (design, construction, sales, finance) to increase the speed of decision-making and reduce communication gaps.

Customer Centricity – systematically incorporating customer feedback into the design and construction process. Using digital platforms for communication with buyers, virtual tours, and customization of plans.

Applicability for developers: Agile approaches are most effective in development companies that implement serial projects (multi-tiered residential complexes, typical shopping malls). Applicability limitations are related to regulatory requirements (design documentation is approved at the beginning) and contractual obligations with contractors.

2. Digital Maturity Models.

Digital maturity models provide a framework for assessing the current state of an organization's digitalization and determining the path to higher levels of maturity.

MIT CISR Digital Maturity Model identifies four maturity levels:

Beginners – experimenting with digital technologies without a clear strategy. Typical for Ukrainian developers: separate digital initiatives (website, CRM) without integration.

Fashionistas – actively implementing digital technologies, but without transforming the operating model. Risk: investments in technology without business results.

Conservatives – focus on optimizing existing processes through digitalization, but avoid radical changes. Strong operational efficiency, but limited innovation.

Digirati (Digital Leaders) – combine digital and leadership maturity, transforming the business model. Characterized by an integrated digital ecosystem, data-driven decision making, and an innovative culture.

The Gartner Digital Business Maturity Model considers maturity through five dimensions:

- Strategy: from ad-hoc initiatives to a digital strategy integrated with the business strategy;
- Leadership: from skepticism to active digital leadership of top management;
- Culture: from resistance to change to a culture of experimentation and innovation;
- Organization: from silo structures to agile cross-functional teams;
- Technology: from legacy systems to an integrated digital platform.

Applicability for developers: Maturity models provide a diagnostic tool for self-assessment and defining transformation priorities. They are especially valuable for multi-year transformation planning with phased achievement of target states. It is recommended to adapt general models taking into account the specifics of the development business.

3. Construction Digital Transformation Framework.

Specific frameworks for the construction industry emphasize technologies and processes characteristic of this industry.

Key areas of digitalization: Building Information Modeling (BIM) – digital 3D models of buildings that integrate geometric, technical, and economic information and serve as a single source of data for all project stakeholders. IoT and Smart Construction – use of sensors, drones, and wearable electronics for construction site monitoring, quality control, occupational safety, and material tracking. Digital Twins – digital copies of physical objects that allow simulating various scenarios, optimizing operations, and predicting problems. Cloud-based Collaboration Platforms – platforms for collaboration between all project participants (developer, architects, engineers, contractors) with access to up-to-date information in real time. Advanced Analytics and AI – cost and time forecasting, schedule optimization, and automation of routine processes (documentation review, compliance monitoring). Applicability for developers: Technology-oriented frameworks provide a specific list of digital solutions for implementation. It is critical to align technology investments with business priorities and organizational readiness.

4. Integrated Transformation Model.

Analysis of the models shows that the most effective for development companies is an integrated approach that combines: Strategic vision and transformation roadmap (from maturity models), Flexible principles of work organization (from Agile), Industry-specific technologies (from Construction frameworks), Focus on people and organizational culture.

This model includes five parallel transformation streams:

1. Strategy and governance: defining a digital vision, creating a digital transformation office, assigning roles and responsibilities.

2. Processes: standardizing and optimizing business processes, implementing Agile practices where appropriate.

3. Technologies: building an integrated digital platform, implementing industry-specific solutions (BIM, IoT).

4. Data and analytics: creating a single source of data, developing analytical capabilities, data governance.

5. People and culture: developing digital competencies, change management, creating a culture of innovation.

The prerequisites for transforming the management system based on digitalization in KAN Development, one of the leading developers in Ukraine, are: information gaps between departments and projects, delays in decision-making due to the need to consolidate data from different sources, difficulties in monitoring the implementation of construction schedules, limited opportunities for analyzing project effectiveness and forecasting, insufficient transparency for clients regarding the status of their construction objects. We propose a transformation project life cycle model consisting of the following phases.

Phase 1: Creating the foundation for transformation:

- Implementation of a corporate ERP system to integrate finance, procurement, and contract management;
- Updating the CRM system with integration with ERP;
- Creation of a Digital Transformation Office reporting directly to the CEO;
- Digital literacy: training of top management and key employees.

Phase 2: Digitizing project management:

- Implementation of a project management platform (adaptation of Microsoft Project Online);
- Pilot implementation of BIM on new projects;
- Mobile applications for construction sites (progress reports, quality control);
- Implementation of electronic document flow.

Phase 3: Analytics and customer experience:

- Building a data warehouse and Power BI dashboards for portfolio analytics;
- Launching a customer portal for buyers with visualization of construction status;
- Implementation of a risk management system with predictive analytics;
- Expansion of BIM to all new projects.

Phase 4: Intelligent systems:

- AI-powered tools for cost and schedule forecasting;
- IoT sensors on construction sites for real-time monitoring;
- Automation of document approval and coordination processes;
- Digital twin for a flagship project.

Transformation should be accompanied by restructuring and organizational changes, which should include the creation of cross-functional project teams with representatives from different departments, the introduction of the role of “project digital champion”, changing KPIs for project managers to include digitalization metrics, and a digital competency development program for all levels of staff. The expected results of projects to transform the management systems of development companies based on digitalization are the following operational improvements: Reduction of reporting time by 60%, increase in the accuracy of project completion time forecasting from 65% to 87%, reduction of deviations from the project budget from 8-12% to 4-6%, acceleration of decision-making: from an average of 5-7 days to 1-2 days. Expected business results

include an increase in the number of simultaneous projects from 8 to 12 without a proportional increase in overhead, an increase in project margins by 2-3 pp. due to better cost control, an increase in sales speed by 15% due to improved customer experience, strengthening the reputation as an innovative developer, which makes it easier to attract investments. Risks and challenges to the success of a digital transformation project are: resistance to change among experienced company professionals, difficulties in integrating with contractor systems, the need to balance standardization and flexibility for different types of projects. In this context, the following important principles of a digital transformation project can be identified: the importance of top management sponsorship, the need for quick wins to maintain the momentum of the transformation, the critical role of learning and change management, the advantage of a phased approach over a "big bang" transformation.

IV. DISCUSSION AND CONCLUSION

The study shows that successful digital transformation of development companies' management systems requires a systemic approach that goes beyond the simple implementation of technologies. None of the models considered is a universal solution – each has its own advantages and limitations in the context of the development business. According to the results of the study, the following recommendations can be identified for increasing the efficiency of projects for transforming the management systems of a development company based on digitalization.

1. The need for an integrated approach.

The most effective is a combined model that combines strategic planning (from maturity models), flexible organization principles (from Agile), industry-specific technologies and a focus on organizational culture. Development companies cannot apply "pure" Agile due to regulatory restrictions, but can adapt its principles to increase flexibility where possible.

2. Phased approach and quick wins.

The KAN Development case confirms the effectiveness of a phased approach with a focus on quick wins. This allows you to demonstrate the value of transformation to stakeholders, maintain the momentum of change, and adjust the course based on the experience gained. "Big bang" approaches have a higher risk of failure due to the complexity of development management systems.

3. Criticality of leadership and culture.

Technology is an enabler, but not a driver of transformation. Success depends on active sponsorship by top management, the formation of a culture of innovation, and investments in the development of digital competencies of personnel. Companies that focus exclusively on technology risk becoming "fashionistas" according to the MIT classification - having technology without transforming the business.

4. Taking into account the specifics of the development business.

When adapting general transformation models, it is critically important to take into account the specifics of development: long project cycles, regulatory complexity, dependence on contractors, capital intensity. This affects the choice of technologies, the speed of transformation and success metrics.

5. The value of integration and data.

Fragmentation of systems is one of the biggest obstacles to effective management. Creating an integrated digital platform with a single source of data is the foundation for advanced capabilities (analytics, AI, automation). Investments in data governance and data quality have a high ROI in the long term.

The digital transformation of development companies is at an early stage, and the next 5-10 years will determine which companies will be able to take advantage of the opportunities of digitalization to achieve competitive advantages, and which will be left behind in an era when digital technologies are becoming not an option, but a necessity for survival in the industry. Promising areas of further research are empirical studies of the impact of digital transformation on the financial performance of developers, analysis of barriers to transformation in small and medium-sized companies, study of the impact of the regulatory environment on the speed of digitalization of the industry, research on the application of emerging technologies (blockchain for land registry, AR/VR for project visualization, AI for automated code compliance checking).

REFERENCES

1. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Eighth Edition and The Standard for Project Management (2026). Project Management Institute, 408 p.
2. Bonanomi, M. M., Hall, D. M., Staub-French, S., Tucker, A., & Talamo, C. (2022). The impact of digital transformation on the construction industry: A review. Journal of Construction Engineering and Management, 148(6), 03122002.
3. Osunsanmi, T. O., Aigbavboa, C. O., & Oke, A. E. (2023). Construction 4.0: The future of the construction industry in the Fourth Industrial Revolution. Frontiers in Built Environment, 9, 1103193.
4. Tezel, A., Papadonikolaki, E., Yitmen, I., & Hilletofth, P. (2021). Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. Frontiers of Engineering Management, 8(4), 564-577.
5. Winch, G. M., & Cha, J. (2023). Digital transformation in project-based organizations: A systematic review and future research agenda. International Journal of Project Management, 41(2), 102448.



VOLODYMYR KOCHUMA
PhD student, Department of project management, Kyiv National University of Construction and Architecture, Kyiv. Ukraine
ORCID: 0009-0008-7203-3940
E-mail: kochuma_vh-2022@knuba.edu.ua
Scientific interest lies in the field of project management, digitalization models and methods, transformation of project management systems in development, value-oriented approach.

HYBRID BLOCKCHAIN ARCHITECTURE FOR TRUSTED DOCUMENT AUTHENTICATION: A THEORETICAL FRAMEWORK FOR ENTERPRISE IT SOLUTIONS

Assylbek Muratbek, Yenlik Begimbayeva

Abstract. *The digital transformation of document circulation faces a fundamental conflict between public transparency and the necessity of data privacy. Traditional centralized registries suffer from single points of failure and lack cross-organizational trust. This paper proposes a theoretical hybrid blockchain architecture that integrates public (Ethereum) and private (Hyperledger Fabric) ledgers to resolve the "publicity-confidentiality" dilemma. By decoupling cryptographic anchoring from sensitive data management, the model provides a scalable solution for secure document authentication. Furthermore, the architecture is formalized as a pedagogical case study for IT architects, bridging the gap between foundational DLT theory and complex industrial requirements.*

Keywords: Blockchain, Hybrid Architecture, Document Authentication, Hyperledger Fabric, Ethereum.

I. INTRODUCTION

The digitalization of document circulation has introduced systemic vulnerabilities regarding data integrity. Traditional centralized systems rely on a Single Point of Trust, which remains susceptible to unauthorized tampering and lacks cross-organizational transparency. Blockchain technology has been recognized for its ability to enhance transparency and trust across complex supply chains [1]. However, organizations face a significant "transparency challenge" where excessive data exposure conflicts with sensitive business intelligence [2].

As of 2026, privacy has transitioned from a niche feature to a mandatory requirement for the mass adoption of decentralized applications. For research centered on the "Development of identification or document authentication systems," this paper identifies a critical friction between immutable ledgers and modern privacy regulations like GDPR [3]. We propose a hybrid model that resolves this trilemma by decoupling the "Proof of Existence" from the "Data Governance" layer.

II. DATA AND METHODS

This study employs a Research through Design (RtD) methodology to formalize an architectural pattern through iterative conceptual modeling and UML diagramming.

A. Theoretical Framework

Following the theoretical framework for balancing transparency and privacy in industrial ecosystems [4], this study formalizes a dual-stream architecture. The design integrates accountability protocols to ensure that anonymity does not compromise the legal validity of the authenticated documents [5].

B. Logical Tiered Architecture

The methodology conceptualizes a separation of concerns into two distinct functional layers:

The Public Anchoring Layer (Ethereum): This layer acts as the "Global Root of Trust." It stores only the SHA-256 cryptographic fingerprints and timestamps, providing immutable proof without revealing content.

The Private Governance Layer (Hyperledger Fabric): This layer manages the document lifecycle, including sensitive metadata and access control policies governed by smart contracts (Chaincode).

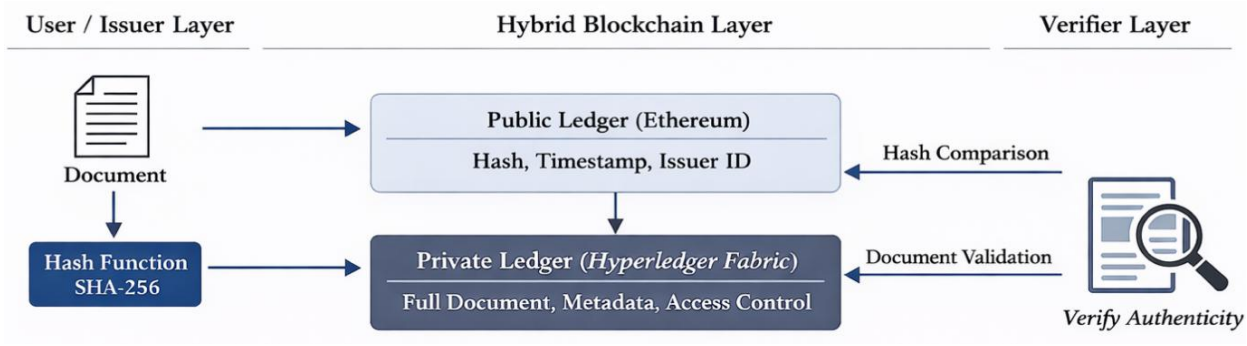


Figure 1. *Conceptual Schema of the Hybrid Authentication System*

III. RESULTS AND ANALYSIS

The primary result is the formalization of the Synchronized Relayer Pattern, which bridges heterogeneous ledgers. The hybrid model effectively synthesizes the strengths of isolated DLT deployments as shown in Table 1.

Table 1. *Theoretical Comparison of Architectural Models*

Evaluation Parameter	**Public Ledger**	**Private Ledger**	**Proposed Hybrid Model**
Data Privacy	Low (Publicly visible)	High (Consortium only)	High (Selective Disclosure)
Verification Trust	Global (Decentralized)	Local (Permissioned)	Global (Publicly Anchored)
Regulatory Compliance	Low (Immutable PII)	Moderate (Controlled)	High (PII Decoupling)
Operational Cost	High (Variable Gas fees)	Low (Fixed costs)	Optimized (Min. Anchoring)

The analysis of operational costs aligns with recent findings that optimized transparency can significantly reduce verification and financing expenses [6]. Furthermore, the results confirm the critical trade-offs identified in global supply chain DLTs [7], showing that the hybrid model stabilizes performance while maintaining consumer privacy [8].

IV. DISCUSSION AND CONCLUSION

The proposed hybrid blockchain architecture provides a theoretically sound solution for the modern document authentication crisis. While the model resolves the privacy-transparency conflict, it introduces architectural complexity, particularly regarding the reliability of the Relayer (Oracle) that synchronizes the two tiers.

In conclusion, this framework bridges the gap between enterprise control and public trust. It serves as a vital component for graduate research on identification systems, providing a clear technical roadmap for developers and IT architects. Future work will focus on the standardization of inter-blockchain communication (IBC) protocols to ensure the safety and liveness of the cross-chain synchronization process.

REFERENCE

1. Zayed, E.O. and Hatem, M. (2026), 'Blockchain, transparency and trust in supply chains: Insights from professionals' perceptions', Journal of Transport and Supply Chain Management, vol. 20, a1255. doi: 10.4102/jtscm.v20i0.1255.
2. Sedlmeir, J. et al. (2022), 'The transparency challenge of blockchain in organizations', Electronic Markets, vol. 32, pp. 1779–1794. doi: 10.1007/s12525-022-00536-0.
3. Akanfe, O., Lawong, D. and Rao, H.R. (2024), 'Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities', Government Information Quarterly, vol. 41, no. 2, 101851. doi: 10.1016/j.giq.2024.101851.
4. Islam, S. et al. (2022), 'Transparency-privacy trade-off in blockchain-based supply chain in industrial Internet of Things', IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 1234–1245. doi: 10.1109/TII.2022.9781216.
5. Ibraheem, I.O., Tosho, A.U., Saka, K. and Aremu, B.L. (2025), 'The trade-off between anonymity and accountability in blockchain: A framework for secure and compliant systems', International Journal of Computer and Information Technology, vol. 14, no. 5. [Online]. Available at: https://ijcit.com/index.php/ijcit/article/view/503.
6. Zheng, M. et al. (2026), 'Exploring the impact of blockchain technology on supply chain transparency and corporate financing costs', International Journal of Production Economics, vol. 282, 109123. doi: 10.1016/j.ijpe.2025.109123.
7. Hakkarainen, T., Colicev, A. and Pedersen, T. (2024), 'A perspective on three trade-offs of blockchain technology for the global strategy of the MNC', Global Strategy Journal, vol. 14, no. 3, pp. 635–654. doi: 10.1002/gsj.1509.
8. Karaduman, M. (2025), 'Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand', Applied Sciences, vol. 15, no. 9, 5168. doi: 10.3390/app15095168.



ASSYLBEK MURATBEK
2nd-year master's student at Astana IT University, Astana, Kazakhstan
E-mail: kennio057@gmail.com
Research interests focus on decentralized systems and information security within enterprise environments. Scientific work is dedicated to the development of hybrid blockchain architectures for trusted document authentication and establishing theoretical frameworks for secure enterprise IT solutions.



YENLIK BEGIMBAYEVA
PhD, associate professor, Head of the Cybersecurity Department, Energo University, Almaty, Kazakhstan
ORCID: 0000-0002-4907-3345
E-mail: Ye.begimbayeva@aues.kz
Scopus Author ID - 57191071133 Yenlik Begimbayeva's research interests include cybersecurity, cryptography, and information security. Her work focuses on post-quantum cryptography, code-based cryptographic systems, and the development of secure quantum key distribution protocols. She also studies the security of decentralized and distributed network architectures.

PSYCHOLOGICAL DETERMINANTS OF ADDICTIVE BEHAVIOR IN YOUTH UNDER CONDITIONS OF DIGITALIZATION

Vladlen Lisnevsky

Abstract. *This study investigates psychological determinants of addictive behavior among university students in the context of digitalization. The research integrates cognitive-behavioral, neuropsychological, and self-regulation approaches to examine impulsivity, emotional dysregulation, coping strategies, and self-control as predictive factors. Quantitative analysis reveals significant associations between emotional dysregulation, impulsivity, avoidant coping, and addictive tendencies, while self-control demonstrates a protective role. The findings expand theoretical models of behavioral addiction and support the implementation of structured prevention programs in higher education.*

Keywords: addictive behavior; youth; digitalization; impulsivity; emotional dysregulation; self-regulation; coping strategies; executive functioning; prevention.

I. INTRODUCTION

The phenomenon of addictive behavior has undergone substantial transformation in the context of digital globalization. While classical addiction research predominantly focused on substance dependence, contemporary psychological discourse increasingly recognizes behavioral addictions as equally significant forms of maladaptive engagement [5]. Digital platforms provide continuous exposure to highly stimulating content, personalized reinforcement algorithms, and immediate feedback mechanisms, which collectively intensify reward-processing cycles [4]. From a neuropsychological perspective, addictive behavior is closely associated with dopaminergic reward pathways and impaired executive control. In young adults, incomplete maturation of prefrontal cortical structures contributes to reduced inhibitory control and heightened impulsivity. These neurodevelopmental characteristics intersect with psychosocial stressors such as academic pressure, identity uncertainty, and social comparison amplified by social media environments [3]. The integrative theoretical framework of this study combines cognitive-behavioral theory, self-regulation theory, and stress-coping models. Cognitive distortions, including overestimation of reward value and underestimation of long-term consequences, reinforce maladaptive engagement patterns. Simultaneously, deficits in emotional regulation increase reliance on external stimuli for mood modulation [1]. Thus, addictive behavior may function as an emotion-focused coping mechanism aimed at temporary reduction of psychological discomfort [2].

The empirical research utilized a cross-sectional quantitative design. The sample consisted of 134 university students aged 18–24 years (M = 20.8; SD = 1.6). Participants were recruited through institutional announcements and voluntarily completed the assessment battery. The psychometric instruments included: Barratt Impulsiveness Scale (BIS-11); Difficulties in Emotion Regulation Scale (DERS); Brief COPE Inventory; Self-Control Scale; and Addictive Behavior Risk Index. All instruments demonstrated satisfactory reliability (Cronbach's α ranged from. 0.79 to 0.88). Data analysis included descriptive statistics, Pearson correlation analysis, hierarchical regression modeling, and effect size estimation.

The research procedure involved four sequential stages:

1. theoretical modeling and hypothesis formulation;
2. standardized data collection;
3. statistical verification of predictive relationships;
4. development of applied prevention algorithm based on empirical findings.

II. DATA AND METHODS

Statistical findings confirmed significant positive correlations between addictive behavior indicators and impulsivity (r = 0.51), emotional dysregulation (r = 0.57), and avoidant coping strategies (r = 0.42). Self-control demonstrated a statistically significant negative association (r = –0.47), confirming its protective regulatory role. Hierarchical regression analysis indicated that emotional dysregulation accounted for 29% of variance in addictive behavior. The inclusion of impulsivity increased explained variance to 38%, while avoidant coping further expanded predictive strength to 43%. These findings suggest cumulative effects of emotional and behavioral dysregulation mechanisms.

The correlation coefficients are visually presented in Figure 1. The diagram illustrates the comparative magnitude of psychological predictors and confirms that emotional dysregulation exerts the strongest direct effect on addictive tendencies, while self-control functions inversely.

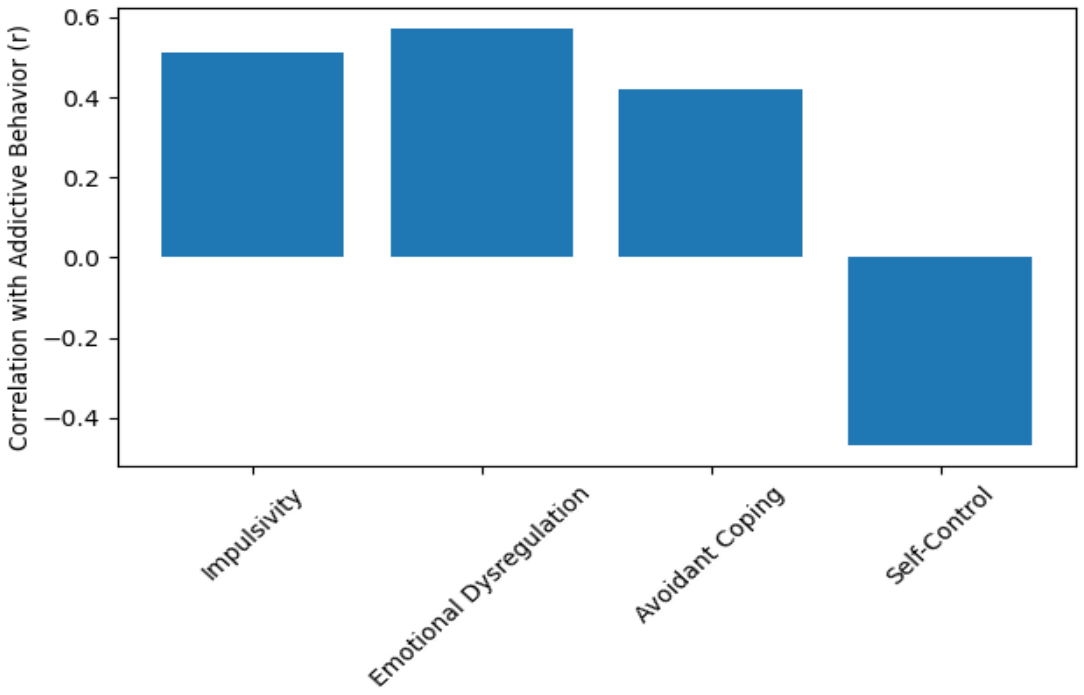


Figure 1. *Correlation coefficients of psychological predictors of addictive behavior*

The obtained results support the hypothesis that addictive vulnerability among youth is primarily rooted in emotional regulation deficits combined with impulsive behavioral tendencies. Digital environments amplify these vulnerabilities by providing rapid reward cycles and reducing exposure to delayed gratification processes. Avoidant coping strategies further reinforce maladaptive engagement patterns by preventing constructive problem-solving and emotional processing. The protective role of self-control underscores the importance of executive functioning skills in mitigating addiction risk.

Psychological interventions aimed at strengthening regulatory capacities, enhancing emotional awareness, and restructuring maladaptive cognitions may significantly reduce susceptibility to addictive behavior.The theoretical contribution of this research lies in the integrative explanatory model that synthesizes personality traits, emotional processes, and environmental reinforcement structures. Unlike traditional unidimensional models of addiction, the present framework emphasizes dynamic interaction between internal psychological mechanisms and digital context factors.

Figure 2 illustrates the predictive structure of the regression model explaining addictive behavior among university students. Emotional dysregulation accounted for 29% of the variance in addictive behavior scores, representing the strongest individual predictor. The inclusion of impulsivity increased the explanatory power of the model to 38%, while the addition of avoidant coping strategies resulted in a total explained variance of 43%. These results confirm that addictive behavior emerges from the cumulative interaction of emotional and behavioral dysregulation factors rather than from a single personality trait. The model supports the conclusion that interventions targeting emotional regulation and impulse control are likely to produce the greatest preventive effect.

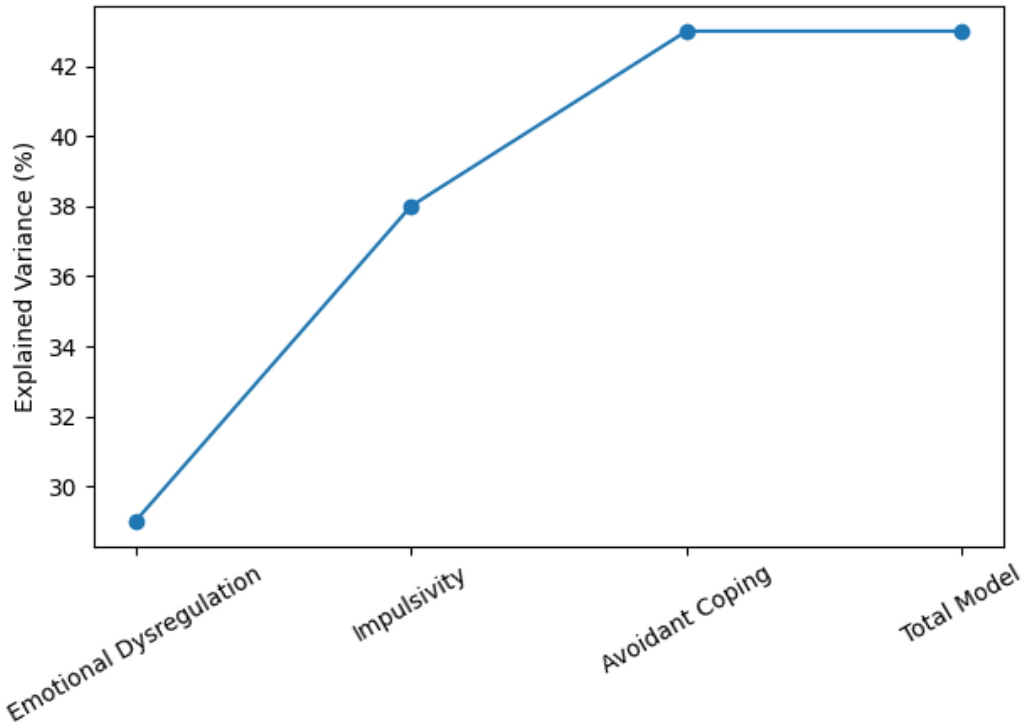


***Figure 2**. Predictive Model of Addictive Behavior*

Based on empirical findings, a structured prevention algorithm was developed including: psychological screening; psychoeducation regarding neurobiological mechanisms of addiction; emotional regulation training using cognitive-behavioral techniques; impulse control exercises; coping strategy restructuring; and longitudinal follow-up assessment. Such intervention programs may be integrated into university psychological services and preventive mental health initiatives. Early identification of high-risk students combined with targeted skill development may significantly reduce addictive tendencies and enhance psychological resilience.

III. RESULTS AND ANALYSIS

The developed algorithm includes sequential interconnected stages. At the first stage, psychological screening and primary diagnostics are conducted using standardized methods to determine the level of risk and to form groups of low, moderate, and high risk. The second stage includes psychoeducation concerning the psychological and neurobiological mechanisms of addiction formation, the role of reinforcement, stress, and factors that provoke addictive behavior. The third stage is aimed at the development of emotional regulation skills using cognitive-behavioral techniques, including identification of triggers and cognitive restructuring.

The fourth stage includes training of impulse control and strengthening of self-control through the development of reaction delay skills, activity planning, and self-monitoring. The fifth stage involves the formation of adaptive coping strategies through the replacement of avoidant coping with problem-oriented and supportive strategies. The sixth stage includes repeated assessment of results and supportive follow-up using the T0–T1–T2 scheme to verify the stability of changes. The practical significance of the algorithm lies in the implementation of the stepped-care principle — from basic preventive measures for low- and moderate-risk groups to more intensive individual support for high-risk groups, which increases the efficiency of resource utilization in educational institutions.

IV. DISCUSSION AND CONCLUSION

Addictive behavior among youth in the digital era is significantly associated with emotional dysregulation, impulsivity, avoidant coping strategies, and reduced self-control. The expanded integrative model provides empirical support for targeted psychological prevention strategies within higher education institutions. Future research should incorporate longitudinal and neurocognitive methodologies to clarify causal mechanisms and developmental trajectories of addiction vulnerability. The obtained results confirm that addictive behavior among student youth is formed under the influence of the interaction of psychological factors, among which emotional dysregulation, impulsivity, avoidant coping strategies, and reduced self-control play the leading role. The identified relationships made it possible to construct an integrative model of psychological predictors of addictive behavior and to develop a structured prevention algorithm aimed at early identification of risk and correction of key mechanisms of its formation. The proposed approach contributes to increasing students' psychological resilience and may be used in the system of psychological support of higher education institutions as a scientifically grounded basis for the prevention of addictive disorders.

REFERENCES

1. Beck A. T., Wright F. D., Newman C. F., Liese B. S. (2011), Cognitive Therapy of Substance Abuse. New York: Guilford Press. 354 p.
2. Gross J. J. (2015), Emotion regulation: Current status and future prospects // Psychological Inquiry. Vol. 26, No. 1. P. 1–26.
3. Tangney J. P., Baumeister R. F., Boone A. L. (2004), High self-control predicts good adjustment, less pathology, better grades, and interpersonal success // Journal of Personality. Vol. 72, No. 2. P. 271–324.
4. Volkow N. D., Morales M. (2015), The brain on drugs: From reward to addiction // Vol. 162, No. 4. P. 712–725.
5. Young K. S., de Abreu C. N. (2011), Internet Addiction: A Handbook and Guide to Evaluation and Treatment. Hoboken, NJ : John Wiley & Sons, 312.



VLADLEN LISNEVSKY
2nd year postgraduate student in psychology at Taras Shevchenko National University of Kyiv.
ORCID: 0009-0004-5488-1111
Email: vladlen2000@ukr.net
Graduated from Taras Shevchenko National University of Kyiv with a Bachelor of Sociology degree in 2021 and a Master of Psychology degree in 2023. Scientific interests: longevity psychology and macroeconomics.

DEVELOPMENT OF PROJECT RISK SIMULATOR USING THE MONTE CARLO METHOD

Viktor Putrenko, Yuriy Oliyarnyk, Nataliia Pashynska

Abstract. *Software development projects are characterized by significant uncertainty in task durations and external risk factors. This paper presents the development of a software risk simulator that integrates the Critical Path Method (CPM) with Monte Carlo simulation for quantitative project duration analysis. The tool enables probabilistic modeling of activity estimates and global risks, generating distributions of possible completion times. Implemented in Python within a Jupyter environment, the simulator provides scenario-based forecasts and risk prioritization outputs, supporting more informed and transparent project management decision-making.*

Keywords: project management, Monte Carlo simulation, quantitative risk analysis, Critical Path Method, project duration estimation, probabilistic modeling.

I. INTRODUCTION

In contemporary business environments, software projects play a crucial role in driving digital transformation and organizational competitiveness. However, statistical evidence consistently shows high failure rates and budget overruns in IT initiatives. The deterministic approaches traditionally used in project scheduling often underestimate uncertainty and fail to reflect the variability inherent in software development processes.

The Critical Path Method (CPM) remains one of the most widely applied scheduling techniques. While CPM provides a structured framework for identifying task dependencies and calculating minimum project duration, it assumes fixed activity durations. In practice, activity durations are uncertain and may vary significantly due to technical complexity, changing requirements, and resource constraints [1].

The Monte Carlo method, originally developed in the mid-20th century for probabilistic modeling, has become a powerful tool for quantitative risk analysis. In project management, it enables repeated random sampling from defined probability distributions to simulate a range of possible project outcomes. The result is not a single deterministic estimate but a probability distribution of completion times [2; 3].

The objective of this study is to design and implement a simulator for quantitative risk analysis of software projects using Monte Carlo simulation integrated with CPM. The proposed system aims to provide a practical and accessible alternative to commercial tools such as Oracle Crystal Ball, Primavera Risk Analysis, which are often costly or complex for smaller teams.

II. DATA AND METHODS

The developed simulator integrates two methodological components:

1. Critical Path Method (CPM) - to determine baseline project duration based on activity dependencies.

2. Monte Carlo Simulation - to incorporate uncertainty into activity durations and global project risks.

For each simulation iteration, random values are generated for activity durations according to predefined probability distributions. The CPM network is recalculated, and the total project duration is obtained. Repeating this process for a large number of iterations produces a probabilistic distribution of completion times.

The system accepts two primary input datasets in Microsoft Excel format:

1. Project Activities Dataset: Activity ID and name, Complexity level, Predecessors, Resource assignment, Duration estimates (single-point or three-point: optimistic, most likely, pessimistic).

2. Global Project Risks Dataset: Risk ID and name, Likelihood percentage, Impact estimates (optimistic, most likely, pessimistic), Distribution type.

Global risks are modeled as percentage adjustments to total project duration. For each risk R_j, its expected influence is calculated as:

$$R_j = p_j \cdot I_j \quad (1)$$

where p_j is probability and I_j is impact. Impact values I_j are percentages or duration increase, thus $0 \le I_j \le 1$.

In this case we have:

$$E_k = A_k \cdot \sum_{j=1}^{M}(1 + R_j) = A_k \cdot \sum_{j=1}^{M}(1 + p_j I_j) \quad (2)$$

there E_k, $k=1, K$ is the duration estimate obtained on the k-th iteration of Monte Carlo simulation, A_k – duration estimate calculated prior to general risks factor application basing on project activities, usually using CPM or other method.

The simulator supports:

1. Triangular distribution.
2. PERT distribution.

The PERT distribution is particularly suitable for project management because it smooths extreme values and better represents expert-based three-point estimates.

The system architecture follows the C4 model at the Component level. The implementation consists of four main classes:

UI Configurator - interactive parameter configuration.

Data Container - validation and storage of input data.

Execution Engine - Monte Carlo simulation logic and CPM recalculation.

Risk Simulator - user interaction and orchestration layer.

The solution is implemented in Python 3.8 using Jupyter Notebook. Key libraries include NumPy and Pandas for data manipulation and random sampling.

III. RESULTS AND ANALYSIS

The simulator produces several analytical outputs.

1. Probability Distribution of Project Duration. The Monte Carlo simulation results in a probability density function (PDF) and cumulative distribution function (CDF). These functions allow project managers to estimate:

- Probability of completing the project before a given deadline.
- Expected project duration (mean).
- Standard deviation and variance.
- Confidence intervals.

Instead of a single estimate (e.g., 120 days), managers receive percentile-based values such as: P50 (median scenario), P80 (moderate risk scenario), P95 (high-confidence scenario).

2. CPM Network Visualization. The system automatically generates a project network diagram highlighting the critical path. This visualization helps identify activities with zero float that most strongly influence total duration.

3. Tornado Chart is generated to show the correlation between individual risks and overall project duration. Risk factors are ranked according to their influence magnitude.

This enables prioritization of mitigation strategies by focusing on the most impactful risks rather than treating all risks equally (Fig.1).

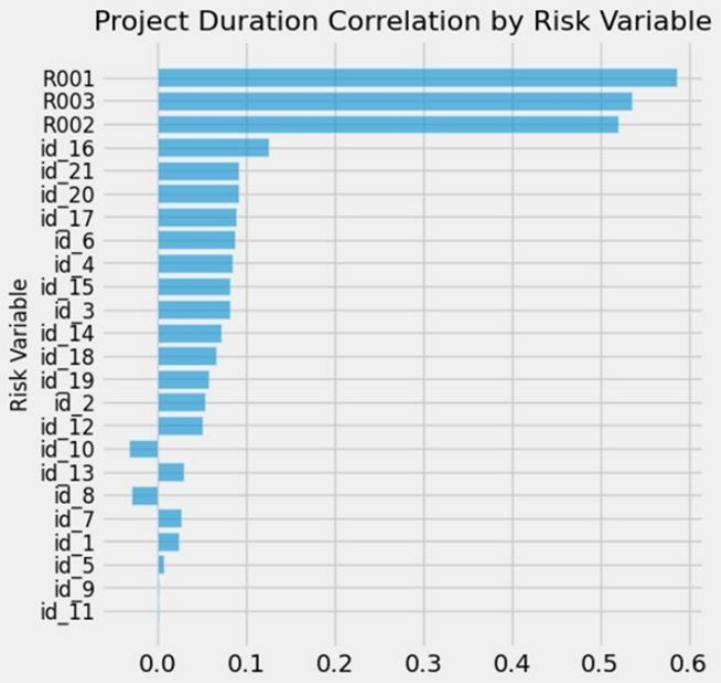


Figure 1. *Tornado Chart*

4. Scenario-Based Estimates. The simulator calculates project duration estimates under: Low-risk scenario, Moderate-risk scenario, High-risk scenario. Such structured outputs enhance strategic planning and communication with stakeholders (Fig. 2).

Project Duration Estimates:

Risk Scenario	Probability	Effort Estimate	Explanation
High Risk	80.000000	1000.890000	Project Duration value is less or equal to 1000.89 with probability of 80.0 %
Moderate Risk	90.000000	1082.320000	Project Duration value is less or equal to 1082.32 with probability of 90.0 %
Low Risk	97.500000	1206.290000	Project Duration value is less or equal to 1206.29 with probability of 97.5 %

Figure 2. *Project Duration Estimates by Scenario*

5. Practical Implications. Compared to commercial solutions, the developed tool demonstrates:

- Lower cost (open-source environment).
- High transparency of algorithms.
- Flexibility in configuration.
- Ease of adaptation to different project types.

IV. DISCUSSION AND CONCLUSION

The integration of CPM and Monte Carlo simulation provides a powerful framework for quantitative risk analysis in software projects. The deterministic nature of traditional scheduling methods often leads to overly optimistic timelines. By contrast, probabilistic simulation acknowledges uncertainty and provides a distribution of possible outcomes.

The developed simulator addresses several limitations of existing commercial solutions: high licensing costs, complexity and steep learning curves, limited customization options.

The use of Python and Jupyter Notebook ensures accessibility and adaptability. The modular class-based architecture allows further extensions, including: cost risk analysis, resource-constrained scheduling, integration with agile metrics, AI-based risk parameter calibration.

However, the study also identifies limitations:

- Accuracy depends on the quality of input estimates.
- Independence between risks is assumed.
- Large-scale enterprise integrations require additional development.

In conclusion, the proposed Monte Carlo-based risk simulator represents a practical and scalable solution for quantitative analysis of software project uncertainty. It enhances managerial decision-making by transforming deterministic schedules into probabilistic risk-informed forecasts.

Future research may focus on incorporating machine learning techniques for automatic estimation of distribution parameters and dynamic risk modeling in agile environments.

REFERENCES

1. Bara M. (2025) Enhanced Monte Carlo simulation for project risk analysis: integrating cost and schedule impacts with time-shifted risks and dependency modeling. Applied Operations and Analytics. 2025. Vol. 1, No. 1. P. 1-15. DOI: https://doi.org/10.1080/29966892.2025.2552675
2. Acebes F., Curto D., González-Varona J.M., Pajares J. (2024) Monte Carlo simulation for project risk prioritisation. Proceedings of the 17th International Conference on Industrial Engineering and Industrial Management (ICIEIM) - XXVII Congreso de Ingeniería de Organización (CIO2023). 2024. P. 455-460. DOI: https://doi.org/10.1007/978-3-031-57996-7_78
3. Pashynska N., Putrenko V. (2024) Military Situation Awareness: Ukrainian Experience // Applied Cybersecurity & Internet Governance 2024, Volume 3(1): 122-146 DOI: https://doi.org/10.60097/ACIG/190341



VIKTOR PUTRENKO
Doctor of Technical Sciences, Professor of the Department of Information Technologies American University Kyiv, Ukraine
ORCID: 0000-0002-0239-9241
E-mail: putrenko10@gmail.com
In 2008, he obtained the scientific degree of Candidate of Technical Sciences at the National Academy of Sciences of Ukraine and the degree of Doctor of Technical Sciences in system analysis at the National Technical University of Ukraine's "Ihor Sikorsky Kyiv Polytechnic Institute." Research interests: interdisciplinary research on sustainable development using modern data analysis and information technologies.



YURIY OLIYARNYK
MSc of the Department of Information Technologies American University Kyiv, Ukraine
ORCID: 0009-0003-0633-7245
E-mail: yuoliyarnyk@gmail.com
Research interests: IT project management, computer science, risk management, business analytics.



NATALIIA PASHYNSKA
PhD, Assistant of the Department of Intellectual Technologies Taras Shevchenko National University of Kyiv, Ukraine
ORCID: 0000-0002-0133-688X
E-mail: nat.pashynska@gmail.com
Received her PhD degree in 2009 from the National Academy of Sciences of Ukraine. Since 2016 she has been working at the Faculty of Information Technologies Taras Shevchenko National University of Kyiv.
Research interests: data mining, quality management, geoinformatics, GIS analysis.

MODEL OF TECHNOLOGICAL MATURITY OF ARTIFICIAL INTELLIGENCE USE IN BANKING INFORMATION SYSTEMS

Kristina Shostal, Vadym Ziuziun

Abstract. *The paper proposes a model of technological maturity for the use of artificial intelligence (AI) in banking information systems. The model combines user engagement, productivity, and economic efficiency indicators with security and quality requirements. Maturity levels and criteria for transitioning between them are formed, evaluation metrics (ER, DR, ROI) and practical interventions for scaling AI in a regulated environment are provided.*

Keywords: technological maturity, artificial intelligence, banking information systems, adoption, quality control, information security.

I. INTRODUCTION

The use of artificial intelligence in banking information systems has gradually shifted from isolated experiments to broader application scenarios in recent years. AI tools are used to support software development processes, analyze text data and customer inquiries, work with internal knowledge bases, and automate operational and compliance processes. At the same time, in a regulated banking environment, the mere technical availability of such tools does not guarantee their systematic and sustainableuse.

In practice, there is often a gap between providing access to artificial intelligence tools and achieving measurable results from their use. This gap is due to insufficient formalization of work processes, the lack of clearly defined criteria for quality and effectiveness, increased information security requirements, and uneven levels of user engagement with AI. As a result, the potential of the technology is only partially realized, and the scaling of AI use is not systematic.

The purpose of this work is to develop a model of technological maturity for the use of artificial intelligence in banking information systems. The proposed model allows for a structured description of the stages of AI development, the definition of criteria for transition between them, and the formation of a system of indicators for assessing the level of user engagement and the achieved effect. Particular attention is paid to the formation of practical recommendations for increasing the maturity of AI use in a regulated environment.

II. DATA AND METHODS

The proposed model of technological maturity is based on a combination of quantitative and qualitative indicators. Quantitative indicators are used to assess the level of user engagement with artificial intelligence tools, the amount of time saved, and the overall economic effect. In addition, proxy metrics of engineering productivity are taken into account, in particular the dynamics of change flow in software repositories. Qualitative indicators reflect the level of maturity of organizational processes, including the presence of information security standards, quality control mechanisms, action logging, as well as approaches to user training and support.

The engagement rate (ER) characterizes the share of regular users, which includes irregular and daily users, in the total number of users. The daily rate (DR) reflects the share of users who use artificial intelligence tools on a daily basis. The economic effect of using AI is assessed through the indicator of annual working time savings H_{year} and its financial equivalent S_{year}. The return on investment is determined using the ROI indicator, which is calculated as the ratio of the economic effect obtained to the annual costs of using the tools.

The calculation of key indicators is carried out according to the following ratios:

$$ER = \left(\frac{N_{occasional} + N_{daily}}{N_{total}}\right) \cdot 100\ \%; \quad (1)$$

$$DR = \frac{N_{daily}}{N_{total}} \cdot 100\%; \quad (2)$$

$$H_{year} = \sum (N_i \cdot h_i \cdot 52); \quad (3)$$

$$S_{year} = H_{year} \cdot C_{hour}. \quad (4)$$

To illustrate the approach to assessing the economic effect of using artificial intelligence tools, an example of calculating annual working time savings for specific user groups is provided. Table 1 shows the initial data and the results of calculating annual time savings based on the number of users and average weekly time savings.

Table 1. *Example of calculating annual working time savings from using AI tools*

User group	N (persons)	h (hours/week)	Annual savings: N·h·52 (hours/year)
Daily users	67	4,1	67·4,1·52 = 14 271
Irregular users	70	2,0	70·2,0·52 = 7 280
Total ($\boldsymbol{H_{year}}$)			21 551

III. RESULTS AND ANALYSIS

3.1. User engagement and adoption rate

The level of actual use of artificial intelligence tools should be interpreted as a user engagement funnel, reflecting a gradual transition from non-use to daily use. This approach allows the implementation process to be managed through targeted organizational and training interventions aimed at transitions between different user groups: from those who do not use AI tools to inactive access holders, irregular users, and, ultimately, daily users.

As shown in Figure 1, the structure of user engagement in the sample with a total number of $N_{total} = 400$ developers is uneven. In particular, 180 people do not use artificial intelligence tools, 83 are inactive license holders, about 70 belong to the group of irregular users, while approximately 67 people use AI on a daily basis.

Based on the data provided, the DR indicator is $67/400, or\ 16{,}75\%$. The share of regular users (irregular + daily) forms the ER indicator $\approx (70 + 67)/400 = 34{,}25\%$. In addition, an aggregated indicator of current engagement of 62% is used with a target of 80% +, reflecting the transition from partial integration to systematic use of AI tools.

The discrepancy between ER and the aggregate indicator highlights the need to establish «activity» criteria in measurement policies (e.g., weekly active users and monthly active users). Practically manageable goals should be to increase the share of daily users and reduce the share of inactive access owners. The practical conclusion for managing the level of technological maturity is that the main effect of using AI tools is generated by a cohort of regular users. Accordingly, the managed goals should be to increase the share of daily users and reduce the share of inactive access owners.

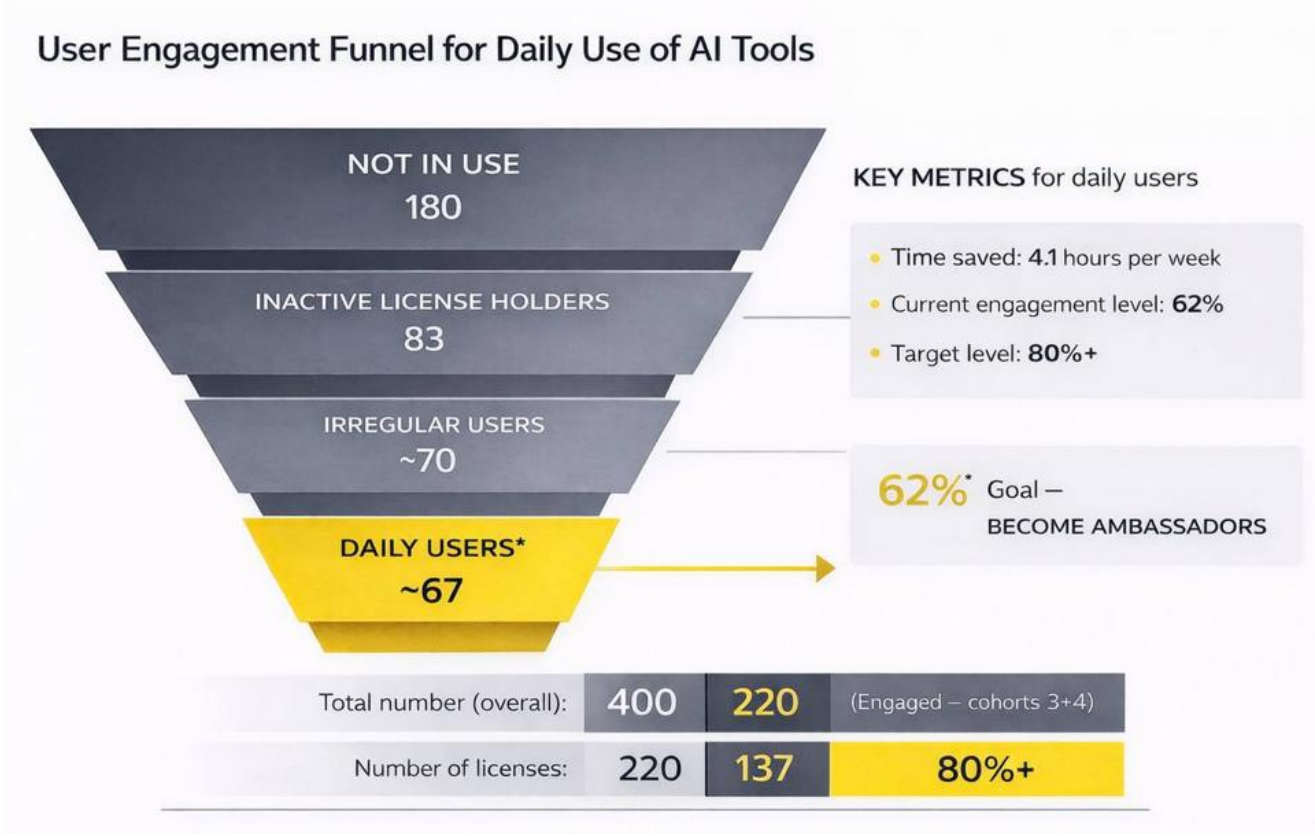


Figure 1. *Funnel for attracting users to levels of technological maturity in AI use*

3.2. Productivity and quality control in a regulated environment

For daily users, the average time savings is 4.1 hours per week. In addition, proxy performance metrics are recorded (for example, a +60% increase in pull requests during a selected period), as well as a 10-fold reduction in the time required to perform routine tasks. However, in banking information systems, increased speed must be accompanied by enhanced quality control.

A dual-loop control model is recommended: (1) automated verification loop (security standards, architectural rules, logging, compliance with conventions), (2) expert review loop (verification of business logic, edge cases, integrations, regulatory implications). Maturity increases with the presence of a feedback loop, where typical errors are used to update verification rules and AI interaction templates.

3.3. Economic efficiency and thresholds for transition between levels

Economic feasibility is assessed based on annual labor savings. Given the current parameters of $H_{year} = 21{,}551$ hours/year and an average hourly cost of $C_{hour} \approx 35 - 36$, the result is $S_{year} \approx \$\,750 - 776$ thousand per year. Annual tool (license) costs are estimated at ≈ $ 53 thousand, resulting in an $ROI\ of \approx 15\times$.

For practical use of the model, transition thresholds are proposed: level 1 (experimental) – DR < 5% and no standards; level 2 (controlled access) – $DR\ 5 - 10\%$ and basic security policies; level 3 (partial integration) – $DR\ 10 - 20\%$, $ER\ 25 - 50\%$ and formalized scenarios; level 4 (systemic use) – $DR > 20\%$, ER > 50% and integrated quality control loops, audit and governance.

***Table 2**. Quantitative indicators of engagement and effectiveness (aggregated data)*

Indicator	**Meaning**
Total number of users (N_{total})	400
Number of licenses	220
Not in use	180
Inactive license holders	83
Irregular users	≈ 70
Daily users	≈ 67
DR (daily / total)	16,75%
ER (irregular + daily/ total)	≈34,25%
Average time savings (daily)	4,1 hours/week
Annual time savings (H_{year})	21 551 hour/year
Financial effect (S_{year})	≈ US$750–776 thousand /year
Cost of tools	≈ US$53,000/year
ROI	≈ 15×
Current engagement (aggregated)	62%
Target indicator	80%+

***Table 3.** Model of technological maturity of AI use in banking information systems*

Level	**Signs**	**Criteria (thresholds)**	**Key mechanisms**
1. Experimental	Isolated attempts, lack of standards and control	DR < 5%	Pilots, risk assessment, basic training
2. Controlled access	Access granted, significant proportion inactive	DR 5-10%; lowering inactive	Security policies, onboarding, library of basic scenarios
3. Partial integration	Stable scenarios in individual processes	DR 10-20%; ER 25–50%	Tests/reviews, request templates, mentoring, quality metrics
4. Systematic use	AI – the standard «default» tool	DR > 20%; ER > 50%; goal 80%+	Governance, audit, logging, dual-circuit quality control, continuous improvement

IV. DISCUSSION AND CONCLUSIONS

The proposed model of technological maturity provides a tool for assessing the actual state of AI use in banking information systems, where security and quality control are critical. The practical value of the model lies in the ability to link adoption with manageable goals (DR, ER), economic effect (H_{year}, ROI), and process maturity (control contours, governance).

To increase maturity, it is advisable to use interventions linked to transitions in the funnel: (1) for inactive users – short scenarios of "first success" and removal of access barriers; (2) for irregular users – standards for teamwork with AI, templates, and mentoring; (3) for daily users – quality control tools, auditing, and development of internal ambassadors. The target of 80%+ is achieved when the use of AI becomes part of standardized processes and is supported by a system of metrics.

REFERENCES

1. ISO/IEC (2023), ISO/IEC 23894:2023. Information technology - Artificial intelligence - Guidance on risk management, International Organization for Standardization, Geneva.
2. NIST (2023), Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology.
3. McKinsey Global Institute (2023). The economic potential of generative AI: The next productivity frontier, McKinsey & Company.
4. OECD (2021). Artificial Intelligence in Finance and Banking: Opportunities and Policy Considerations, Organisation for Economic Co-operation and Development.



KRISTINA SHOSTAL
First-year master's student in IT project management at Taras Shevchenko National University of Kyiv.
ORCID: 0009-0009-0010-1841
E-mail: kristina.shostal@knu.ua
Graduated with a bachelor's degree in Journalism and Social Communication from Taras Shevchenko National University of Kyiv in 2023. For the past three years have been head of IT communications at Raiffeisen Bank. Research interests: digital transformation in financial services, product excellence and agile practices, platform-based operating models (cloud and FinOps), and the role of data and AI in customer-centric banking.



VADYM ZIUZIUN
Ph.D., Associate Professor, Associate Professor of the Department of Management Technologies, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv
ORCID: 0000-0001-6566-8798
E-mail: vadym.ziuziun@knu.ua
Since 2022, he has been working as an associate professor at the Department of Management Technologies at Taras Shevchenko National University of Kyiv. The experience of scientific and pedagogical activity is 14 years. Research interests: project management, risk management, information technology, transport technologies, ecology and environmental protection technologies, management.

BRIDGING THE CULTURAL GAP: THE ROLE OF COMMUNICATION TECHNOLOGIES AND STUDENT BOUNDARY SPANNERS IN UNIVERSITY-INDUSTRY COLLABORATION

Andrii Utvenko, Vadym Ziuziun

Abstract. *This paper explores the critical role of communication technologies in enhancing University-Industry Collaboration (UIC) within the Triple Helix model. While traditional literature emphasizes explicit technology transfer, the relational processes driven by student "boundary spanners" require robust digital communication frameworks. By examining hybrid project management and Connectivist learning theories, this study highlights how digital platforms, shared portals, and unstructured networking tools mitigate cultural gaps. The findings underscore the necessity of advanced communication strategies to transform academic-industry linkages into resilient innovation ecosystems.*

Keywords: University-industry collaboration (UIC), communication technologies, boundary spanners, hybrid project management, digital platforms.

I. INTRODUCTION

In the modern knowledge-based economy, collaborative innovation between societal institutions is an imperative. The Triple Helix model serves as a foundational macro-level framework for understanding these dynamic interactions among universities, industry, and government. However, the key barriers to successful University-Industry Collaboration (UIC) frequently revolve around institutional incompatibility and the divergence of stakeholders' goals.

Historically, the literature has evaluated technology transfer primarily through explicit outputs, such as patents and co-publications, often overlooking the deeply social and relational processes required for successful knowledge exchange. A critical gap in this dynamic is the "cultural gap" between academia and industry, which must be navigated by human capital. Students and early-career researchers act as essential "boundary spanners" and "knowledge vessels" who traverse this cognitive and cultural distance [3].

As collaborative innovation becomes increasingly globalized, the mechanisms of knowledge sharing are rapidly evolving, highlighting an urgent need to systematically investigate the role of communications and advanced communication technologies.

Current studies indicate that digital platforms are frequently underutilized in UICs.

Therefore, this paper aims to analyze how the integration of digital mediums, hybrid project management, and Connectivist approaches can optimize communication pathways, thereby ensuring the adaptive continuity of university-industry interactions [5].

II. DATA AND METHODS

This conceptual paper draws on a systematic review of recent literature regarding micro-level project management and network theories in UICs.

To fully understand the mechanics of knowledge exchange and communication, the study evaluates collaboration through the lens of Connectivism. In this paradigm, learning and knowledge generation are viewed not as isolated processes, but as the capacity to establish, traverse, and leverage interconnected digital and social networks [5].

The methodological framework applies a hybrid project management approach to analyze communication strategies. This involves examining the balance between structured methodologies (formal communication plans) and the flexibility of Agile frameworks (organic networking).

The analysis focuses on how specific digital communication environments alter the geographical and cognitive distance between partners and support the "network competence" of the collaboration [2].

III. RESULTS AND ANALYSIS

The analysis reveals that effective UIC is heavily dependent on the communication capabilities of students acting as strategic "boundary spanners". These actors absorb academic theory and translate it into practical industrial applications, necessitating robust communication channels to transfer both tacit and explicit knowledge [3, 4].

The application of hybrid project management offers a structural solution for aligning divergent expectations. Formal communication planning which involves setting clear objectives, defining responsibilities, and establishing milestones provides a necessary roadmap that mitigates early misunderstandings.

Conversely, organic and agile communication practices fostered through digital tools promote rapid adaptation to new scientific findings and build intercultural awareness [1, 3].

Crucially, the integration of specific communication technologies significantly impacts the ability of boundary spanners to navigate knowledge networks. Technologies such as dedicated "Shared Portals" for integrated project management, digital innovation hubs, and social media tools facilitate continuous idea sharing.

Viewed through a Connectivist lens, these emerging digital platforms deeply alter collaboration dynamics.

A central finding is the evolving nature of trust-building. Collaborative experience creates familiarity and builds the interpersonal trust necessary for long-term adaptive continuity. Researchers must now ask whether digital collaboration environments can complement or even substitute the trust-building processes that have traditionally relied on face-to-face interactions.

Optimizing UICs requires a delicate balance between formal communication plans and informal, "organic" digital networking to mitigate conflicts and enhance overarching network competence [1].

IV. DISCUSSION AND CONCLUSION

This study reconceptualizes the micro-level dynamics of the Triple Helix model by positioning the student boundary spanner at the center of digitally mediated UICs. The findings demonstrate that while formal project management methodologies are critical, the systemic integration of advanced communication technologies is equally vital for bridging the cultural gap between academia and industry.

Digital tools, such as shared portals and innovation hubs, serve as the infrastructure through which Connectivist learning and tacit knowledge transfer occur. By balancing structured communication with unstructured digital networking, organizations can facilitate the adaptive continuity required for long-term success.

However, the conceptual mechanisms proposed including hybrid project management and integrated digital communication frameworks must be empirically tested across a broader range of scientific disciplines, firm sizes, and regional innovation systems. Future research should continue to investigate the intersection of micro-level project management, advanced communication technologies, and the systemic mobility of human capital. Providing actionable insights in these areas is essential to transform fragile university-industry linkages into resilient, self-sustaining ecosystems of open innovation.

REFERENCES

1. Fernandes, G., Tassari, G., Rocha, L., Ferreira, L. M. D. F., Santos, J., Ribeiro, P., Barroso, D., & Bacelar Pinto, E. (2023). Useful Project Management Practices in Collaborative R&D&I Projects. Procedia Computer Science, 239, 1062—1069. https://doi.org/10.1016/j.procs.2024.06.270
2. Fernandes, G., & O'Sullivan, D. (2023). Project management practices in major university-industry R&D collaboration programs – a case study. The Journal of Technology Transfer, 48(1), 361—391. https://doi.org/10.1007/s10961-021-09915-9
3. Abu Sa'a, E., & Yström, A. (2025). Shaping knowledge ecosystems through University–industry collaboration: Exploring the 'second-order' impact of knowledge sharing. Industry and Innovation, 0(0), 1—21. https://doi.org/10.1080/13662716.2025.2560932
4. Ziuziun, V. (2026). SUBSTANTIATION OF THE CONCEPT OF COGNITIVE VISCOSITY FOR OPTIMIZING AGILE TEAM MANAGEMENT. European Open Science Space, 69—73. https://doi.org/10.70286/EOSS-19.01.2026.001.69-73
5. Khan, I. M., Edwards, E., Ianicelli, B. M., Ahmed, W., Hardey, M., & Eremionkhale, G. (2025). University-industry collaboration for academic success and employability: A connectivist perspective. Studies in Higher Education, 0(0), 1—21. https://doi.org/10.1080/03075079.2025.2545606



ANDRII UTVENKO
PhD student, Department of Management Technologies, Taras Shevchenko National University, Kyiv, Ukraine
ORCID: 0009-0006-1900-6420
E-mail: andrii.utvenko@knu.ua
Received the B.S. degree in Applied Physics in 2014, the M.S. degree in Applied Economics in 2016, and the M.S. degree in Project Management in 2018, all from Taras Shevchenko National University (Kyiv, Ukraine). Research interests include communication and communicative technologies in project management, as well as the application of artificial intelligence in project management.



VADYM ZIUZIUN
Associate Professor of the Department of Management Technologies, Taras Shevchenko National University, Kyiv, Ukraine
ORCID: 0000-0001-6566-8798
E-mail: vadym.ziuziun@knu.ua
Since 2022, he has been working as an associate professor at the Department of Management Technologies at Taras Shevchenko National University of Kyiv. The experience of scientific and pedagogical activity is 14 years. Research interests: project management, risk management, information technology, transport technologies, ecology and environmental protection technologies, management.

ЦИФРОВІ ІНСТРУМЕНТИ ПІДТРИМКИ УПРАВЛІННЯ ПРОЄКТАМИ В СУЧАСНИХ ОРГАНІЗАЦІЯХ

Ольга Бондаренко

Анотація. *У статті досліджено цифрові інструменти підтримки управління проєктами, що використовуються в сучасних організаціях. Проаналізовано основні категорії програмного забезпечення для управління проєктами, зокрема хмарні платформи, засоби комунікації та системи відстеження задач. Визначено переваги цифровізації проєктного менеджменту, а також ключові виклики впровадження таких рішень. Запропоновано критерії вибору інструментів залежно від масштабу та специфіки організації.*

Ключові слова: управління проєктами, цифрові інструменти, хмарні платформи, проєктний менеджмент, цифрова трансформація, програмне забезпечення, організаційна ефективність.

I. ВСТУП

Цифрова трансформація бізнес-середовища зумовлює зростаючий попит на ефективні інструменти управління проєктами. Сучасні організації дедалі частіше звертаються до спеціалізованих програмних рішень, що дозволяють оптимізувати планування, координацію та контроль виконання проєктів [1]. Розвиток хмарних технологій, штучного інтелекту та мобільних додатків суттєво розширив функціональні можливості таких платформ.

Управління проєктами як дисципліна набуло нових форм із поширенням гнучких методологій (Agile, Scrum, Kanban), що вимагає від організацій переосмислення традиційних підходів до менеджменту. Цифрові інструменти стали невід'ємною складовою сучасного проєктного офісу, забезпечуючи прозорість процесів, вимірюваність результатів та оперативність комунікацій [2]. Особливої актуальності це набуває в умовах розподіленої роботи та глобалізації команд, коли традиційні механізми контролю та координації втрачають свою ефективність.

Водночас ринок програмних рішень для управління проєктами демонструє стрімке зростання: за прогнозами аналітиків, його обсяг до 2027 року перевищить 15 млрд доларів США. Це свідчить про масштабний попит з боку організацій різних галузей та розмірів і підкреслює важливість науково обґрунтованого підходу до вибору та впровадження таких інструментів [3].

Метою дослідження є систематизація та аналіз цифрових інструментів підтримки управління проєктами, визначення їхніх переваг і недоліків, а також розробка рекомендацій щодо вибору оптимального рішення для організацій різного масштабу та галузевої приналежності.

II. ДАНІ ТА МЕТОДИ

Дослідження базується на аналізі наукових публікацій за 2020–2025 роки, присвячених цифровізації управління проєктами, а також на огляді технічної документації провідних платформ: Jira, Asana, Microsoft Project, Trello, monday.com та Notion. Методологічну основу роботи становлять методи порівняльного аналізу, систематизації та класифікації.

Для оцінки інструментів запропоновано систему критеріїв, що охоплює: функціональність (планування задач, управління ресурсами, звітність), зручність інтерфейсу, масштабованість, можливості інтеграції з іншими системами, вартість ліцензування та рівень підтримки. Аналіз проводився за даними звітів Gartner, Forrester та публікацій у фахових виданнях з управління проєктами.

Додатково враховувався рівень зрілості екосистеми інтеграцій кожної платформи, оскільки сучасні організації, як правило, використовують кілька цифрових інструментів одночасно і потребують їх безперебійної взаємодії.

Категоризацію інструментів здійснено за такими ознаками:

- платформи для планування та відстеження задач (task management);
- засоби командної комунікації та співпраці;
- системи документообігу та управління знаннями;
- аналітичні платформи та інструменти звітності.

Таблиця 1. *Порівняльна характеристика цифрових інструментів управління проєктами*

Інструмент	Основні функції	Методологія	Тип організації
Jira	Відстеження задач, спринти, беклог, звітність, інтеграції	Agile/Scrum	Середній/Великий бізнес
Asana	Проєкти, задачі, часові лінії, портфелі	Agile/Waterfall	Малий/Середній бізнес
monday.com	Дошки, автоматизація, дашборди, CRM	Гнучка	Будь-який масштаб
MS Project	Діаграми Ганта, ресурси, бюджет, EVM	Waterfall	Великий бізнес
Trello	Канбан-дошки, чеклисти, картки	Kanban	Малий бізнес

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз дозволив виявити ключові тенденції ринку інструментів управління проєктами. Станом на 2024 рік понад 77% організацій використовують спеціалізоване програмне забезпечення для управління проєктами, що свідчить про масштабну цифровізацію проєктного менеджменту [3]. Найпоширенішими серед корпоративних користувачів залишаються Jira та Microsoft Project, тоді як у малому бізнесі домінують Trello та Asana.

Як показано в Таблиці 1, вибір інструменту суттєво залежить від методології управління проєктами та масштабу організації. Платформи, що підтримують Agile-підхід, демонструють вищий рівень задоволеності користувачів у командах чисельністю від 5 до 50 осіб. Для великих організацій із складними проєктними портфелями критичного значення набуває наявність функцій управління ресурсами та інтеграції з ERP-системами.

Дослідження виявило, що впровадження цифрових інструментів скорочує час на адміністрування проєктів у середньому на 23%, підвищує своєчасність виконання задач на 18% та зменшує кількість комунікаційних помилок на 31% [4]. Водночас, серед основних перешкод впровадження респонденти називають опір персоналу змінам (64%), складність міграції даних (48%) та вартість ліцензій (39%). Варто зазначити, що найвищий ефект від впровадження демонструють організації, які поєднують цифрові інструменти з формалізованими процесами управління проєктами та регулярним навчанням персоналу.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати дослідження підтверджують, що вибір цифрового інструменту управління проєктами має здійснюватись з урахуванням комплексу організаційних, технологічних та фінансових чинників. Універсального рішення не існує — ефективність платформи

визначається ступенем її відповідності специфіці проєктів, культурі організації та кваліфікації команди.

Перспективними напрямами розвитку цифрових інструментів є інтеграція технологій штучного інтелекту для прогнозування ризиків і автоматизації рутинних операцій, розвиток no-code/low-code рішень для кастомізації платформ без залучення розробників, а також поглиблення аналітичних можливостей у режимі реального часу [5]. Ці тенденції відповідають стратегічним потребам сучасних організацій у підвищенні операційної ефективності та конкурентоспроможності.

Окремої уваги заслуговує питання цифрової зрілості організацій: успішність впровадження інструментів управління проєктами значною мірою залежить від готовності персоналу, рівня цифрової культури та наявності відповідної інфраструктури. Організації з низьким рівнем цифрової зрілості ризикують отримати формальне впровадження без реальної зміни практик роботи, що нівелює потенційні переваги обраних рішень.

Подальші дослідження доцільно спрямувати на розробку моделі зрілості цифрового управління проєктами, яка дозволить організаціям діагностувати поточний стан та визначати пріоритети розвитку інструментального забезпечення.

ДЖЕРЕЛА

1. Dingsøyr, T., Moe, N.B. and Seim, E.A. (2018) ‘Coordinating knowledge work in multiteam programs: Findings from a large-scale agile development program’, Project Management Journal, 49(6), pp. 64-77. https://doi.org/10.1177/8756972818798980.
2. Marnewick, C. and Marnewick, A.L. (2020) ‘The Demands of Industry 4.0 on Project Teams’, IEEE Transactions on Engineering Management, 67(3), pp. 933-945. https://doi.org/10.1109/TEM.2019.2899350.
3. Project Management Institute (PMI) (2024) Pulse of the Profession 2024: The Future of Work. URL: https://www.pmi.org/learning/thought-leadership/pulse.
4. Papke-Shields, K.E. and Boyer-Wright, K.M. (2017) ‘Strategic planning characteristics applied to project management’, International Journal of Project Management, 35(2), pp. 169-179. https://doi.org/10.1016/j.ijproman.2016.10.015
5. Marcelino-Sádaba S., Pérez-Ezcurdia A., Lazcano A. M. E. (2022) Using Project Management as a Way to Sustainability. Sustainability, 14(3), 1-22.



ОЛЬГА БОНДАРЕНКО
асистент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-0024-8789
E-mail: olha.bondarenko@knu.ua
Фахівець у галузі інформаційних систем, телекомунікацій та радіомовлення. Практичний досвід роботи у сфері телекомунікацій та медіаінфраструктури понад 8 років. Досвід викладання в університетах України понад 3 роки.
Наукові інтереси – інформаційно-комунікаційні системи, системи радіомоніторингу, мультисенсорні технології та IoT.

РОЗРОБКА ПРОЄКТУ СТВОРЕННЯ CRM-СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ ДІЯЛЬНОСТІ МЕРЕЖІ КВІТКОВИХ МАГАЗИНІВ

Лілія Гаркушко, Любов Кубявка

Анотація. *У роботі обґрунтовано розробку проєкту створення веб-CRM системи для автоматизації діяльності мережі квіткових магазинів. Проаналізовано особливості операційних процесів роздрібної торгівлі квітами, зокрема багатоканальне приймання замовлень, необхідність оперативного контролю залишків і ризики втрат через обмежений строк зберігання рослин. Визначено основні проблеми існуючої організації роботи, пов'язані з фрагментованим обліком даних, ручною обробкою замовлень і складністю формування фінансової звітності. Запропоновано проєктну модель CRM-системи, що передбачає централізоване управління замовленнями, клієнтською базою, складськими операціями та аналітикою. Очікуваним результатом впровадження є підвищення точності обліку товарних залишків, зменшення втрат продукції та скорочення часу підготовки управлінської звітності.*

Ключові слова: CRM-система, автоматизація, управління замовленнями, інтеграції, управління проєктом.

I. ВСТУП

Операційна діяльність мережі квіткових магазинів має характерні ознаки: висока швидкість обробки замовлень, залежність якості сервісу від точності залишків у точках продажу та значні ризики втрат через обмежений строк придатності рослин. За відсутності єдиного інформаційного джерела замовлення надходять з різних каналів, частина даних фіксується вручну, а облік залишків і руху товару ведеться неузгоджено між точками. Це призводить до помилок у доступності позицій, складних уточнень із клієнтами, додаткового навантаження на персонал та затримок в підготовці фінансової звітності. Результатом дослідження є концептуальна модель та проєктна документація веб-CRM системи, що забезпечує централізоване управління операційними процесами мережі квіткових магазинів.

Наукова новизна роботи полягає у поєднанні підходів управління IT-проєктами та автоматизації операційних процесів роздрібної торгівлі квітами з урахуванням специфіки швидкопсувного товару та багатоканального приймання замовлень.

II. ДАНІ ТА МЕТОДИ

Вхідними даними для розробки проєкту виступають опис поточних бізнес-процесів мережі квіткових магазинів, перелік ролей користувачів, очікування власника щодо аналітики та контролю, потреби персоналу в централізованому веденні замовлень, залишків, поставок і звітності, а також обмеження щодо часу, ресурсів і порядку впровадження.

Для управління проєктом автоматизації застосовано такі методи, прийняті в міжнародному стандарті управління проєктами [2]:

- аналіз проблемної ситуації та формування цілей проєкту;
- ідентифікація стейкхолдерів і оцінка їхнього впливу на проєкт;
- структуризація робіт за допомогою WBS та розподіл відповідальності;
- календарно-ресурсне планування етапів реалізації;
- визначення ризиків, залежностей і контрольних точок;
- поетапне формування функціонального обсягу системи відповідно до інкрементної моделі.

Для цього проєкту обрано інкрементну модель розробки. Для цього проєкту такий підхід є доцільним, оскільки дає змогу спочатку реалізувати найбільш критичні для бізнесу

функції, щоб автоматизувати найкритичніші сфери операційної роботи, а також перевіряти рішення на практиці та уточнювати вимоги між інкрементами.

У межах проєкту доцільно виділити такі інкременти:

- **Реліз 1**: управління замовленнями та клієнтами;
- **Реліз 2**: облік залишків, поставок, переміщень і списань;
- **Реліз 3**: звітність, бухгалтерські дані, аналітика для власника;
- **Реліз 4**: розширення інтеграцій, адміністрування доступів і оптимізація процесів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Результатом роботи є проєктний опис веб CRM-системи як єдиного джерела операційних даних для мережі магазинів з наскрізним контролем життєвого циклу замовлення та пов'язаних складських операцій. У результаті аналізу бізнес-процесів мережі квіткових магазинів було сформовано функціональну структуру CRM-системи, що забезпечує інтеграцію процесів приймання замовлень, управління клієнтською базою, контролю складських залишків та формування управлінської звітності.

Функціонал. Система складається з модулів, що відповідають одній чи кільком вкладкам в навігації:

– Модуль замовлень: централізована реєстрація замовлень і ведення статусів по ним, інтеграція з Instagram для автоматичного створення замовлення з директу;

– Модуль клієнтів: база зі всіма клієнтами що робили замовлення в одному з магазинів мережі, картки клієнтів та історія взаємодій;

– Модуль інвентаризації, що в навігації розділений на вкладки "Каталог", "Поставки", "Переміщення", "Списання", "Облік залишків". Допомагає старшому флористу контролювати залишки на складі та на основі цієї інформації створювати квіткові композиції з наявних рослин. Облік списань допомагає відслідкувати фінансові втрати бізнесу та якісніше приймати рішення щодо закупки тих чи інших видів рослин.

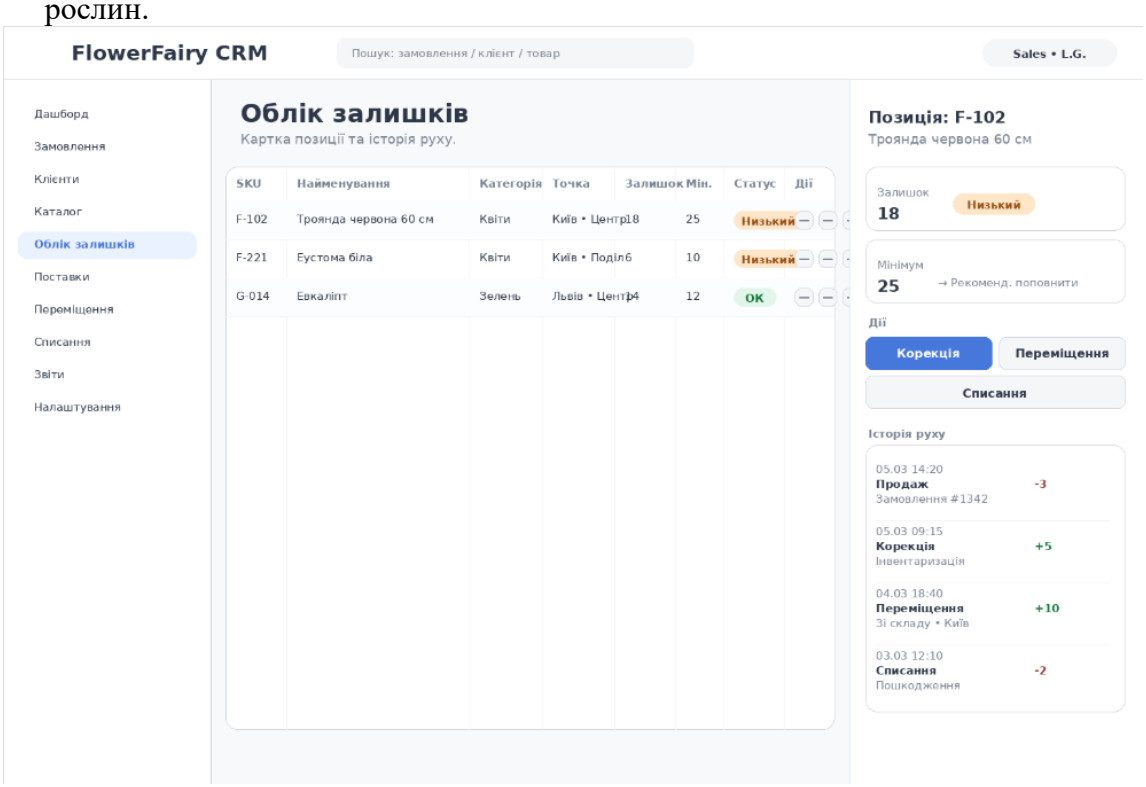


Рисунок 1. *Прототип вкладки "Облік залишків"*

– Модуль звітності: створений для бухгалтерів компанії задля автоматизованого створення фінансової звітності на основі даних про замовлення, списання, поставки товар.
– Модуль управління ролями та доступами, яка в інтерфейсі відповідає влкадці “Налаштування”. Передбачено розмежування доступів за типовими ролями (продажі/операції/виробництво/облік/адміністрування/власник) для зниження помилок і підвищення відповідальності за дані.

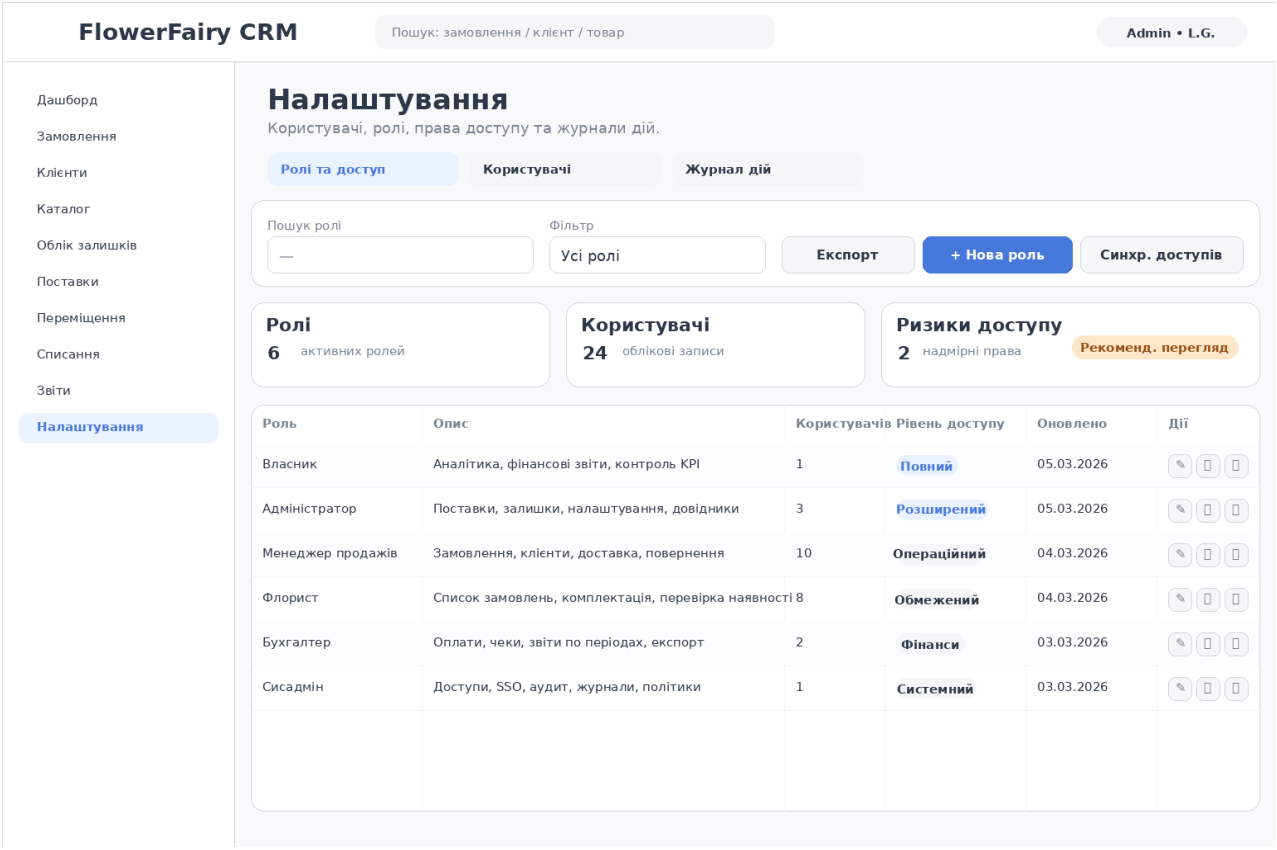


Рисунок 2. *Прототип екрану налаштувань ролей*

Структура робіт проєкту. Сформовано структуру робіт проєкту, що охоплює ініціацію, планування, проєктування, розробку, тестування, впровадження та завершення. На відміну від Waterfall моделі, реалізація функціональності передбачається інкрементно, тобто частинами, кожна з яких створює окрему цінність для бізнесу.

Визначення артефкатів проєкту: Vision&Scope документ, беклог з задачами у форматі User Stories, матриця стейкхолдерів, WBS, ресурсний план, календарний план, реєстр ризиків, вимоги до якості та план комунікацій.

Оцінка ефективності впровадження проєкту. Ефективність проєкту після впровадження пропонується оцінювати за трьома метриками: підвищення точності залишків (зменшення розбіжності між системними та фактичними даними), зменшення кількості квітів, що списуються/викидаються (30% квітів списуються, ціль на 3 місяці після впровадження системи - 20%), скорочення часу на зведення бухгалтерії та підготовку звітності (з 5 годин до 1 години впродовж 3 місяців після впровадження системи).

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Сформований проєкт створення CRM-системи спрямований на підвищення операційної ефективності мережі квіткових магазинів шляхом інтеграції ключових бізнес-процесів у

єдиному інформаційному середовищі. Запропонована система забезпечує централізоване управління замовленнями, облік клієнтів, контроль складських залишків та автоматизоване формування фінансової і управлінської звітності.

Інкрементний підхід до реалізації проєкту дозволяє поступово впроваджувати функціональність системи, починаючи з найбільш критичних для бізнесу модулів, що зменшує ризики впровадження та забезпечує можливість адаптації системи до реальних потреб користувачів. Важливою перевагою запропонованого рішення є підтримка контролю життєвого циклу замовлення — від моменту його створення до виконання та відображення у фінансовій звітності.

Очікується, що впровадження CRM-системи дозволить підвищити точність обліку товарних залишків, зменшити обсяг списання квіткової продукції, а також значно скоротити час, необхідний для підготовки бухгалтерської та управлінської звітності. Крім того, централізація даних сприятиме підвищенню прозорості операційної діяльності та якості управлінських рішень.

Таким чином, розроблений проєкт CRM-системи може розглядатися як ефективний інструмент цифровізації процесів управління роздрібною мережею квіткових магазинів та основа для подальшого розвитку аналітичних і інтеграційних можливостей інформаційної системи.

ДЖЕРЕЛА

1. Li, R., Seva, R., Chiu, A., (2025). Reducing Waste in Retail: A Mixed Strategy, Cost Optimization Model for Sustainable Dead Stock Management. Sustainability, 17(20), 9242. DOI: 10.3390/su17209242.
2. Project Management Institute, (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition. Project Management Institute.
3. Wang, T., Hu, K., Lim, S. F. W. T., Lim, Y. F., Yu, Y., (2022). How Retail System Complexity Drives Inventory Record Inaccuracy: Empirical Evidence from Cross-border E-commerce [онлайн]. SSRN. URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4275704(date of access: 03.03.2026) .



ЛІЛІЯ ГАРКУШКО
студентка 1 курсу магістратури за спеціальністю “Технології розробки ІТ проєктів” у Київському національному університеті імені Тараса Шевченка, Київ, Україна.
E-mail: lilly.garkushko@gmail.com
Науковий інтерес - розробка ІТ проєктів в області цифровізації та автоматизації бізнес процесів для підвищення операційної ефективності компаній.



ЛЮБОВ КУБЯВКА
к.т.н., доцент кафедри технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0005-5397-1585
E-mail: liubov.kubiavka@knu.ua
Викладач з 2015 р. Має понад 100 наукових праць. Серед наукових інтересів — бізнес-аналітика ІТ проєктів, технології управління життєвим циклом ІТ проєктів, реінжиніринг бізнес-процесів, Lean-менеджмент, прогнозна аналітика.

ІНТЕГРАЦІЯ FIGMA У ПРОЦЕС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: ЕТАП ПРОТОТИПУВАННЯ

Маргарита Гладка, Ольга Бондаренко

Анотація. *У роботі досліджено роль інструменту Figma як ключового елемента сучасного життєвого циклу розробки програмного забезпечення. Розглянуто методи переходу від статичного дизайну до інтерактивного прототипування, що дозволяє валідувати UX-рішення на ранніх етапах проєктування. Окрему увагу приділено оптимізації передачі макетів у розробку за допомогою функціоналу Dev Mode та використання дизайн-токенів. Це забезпечує значне скорочення витрат часу на верстку, покращує комунікацію всередині команди та мінімізує кількість помилок при реалізації інтерфейсу.*

Ключові слова: Figma; прототипування; розробка програмного забезпечення (ПЗ); UI/UX дизайн; інтерфейс, дизайн, Dev Mode.

I. ВСТУП

У сучасних умовах розробки програмного забезпечення (ПЗ) швидкість виходу продукту на ринок (Time-to-Market) та якість користувацького досвіду (UX) є визначальними факторами успіху. Традиційні методи проєктування інтерфейсів часто стикаються з проблемою розриву між дизайнерським баченням та технічною реалізацією [2]. Інтеграція інструменту Figma у життєвий цикл розробки, особливо на етапі прототипування, дозволяє створити єдине інформаційне середовище для всієї команди.

Актуальність даного дослідження зумовлена необхідністю оптимізації етапу прототипування як засобу ранньої валідації вимог. Figma надає можливості для створення високодеталізованих (High-fidelity) інтерактивних макетів, які не просто демонструють зовнішній вигляд, а й імітують реальну логіку роботи програми [1]. Це дозволяє виявити помилки в юзабіліті ще до написання першого рядка коду, що значно знижує вартість подальших виправлень [4].

Метою роботи є аналіз переваг використання Figma для побудови ефективного процесу взаємодії між дизайнерами та розробниками, а також дослідження інструментарію, що прискорює трансформацію прототипу у готовий програмний продукт.

II. ДАНІ ТА МЕТОДИ

У межах даного дослідження розглядається процес інтеграції інструментарію Figma у життєвий цикл розробки ПЗ з акцентом на створенні інтерактивних прототипів. Основними методами дослідження є системний аналіз компонентного підходу та експериментальне моделювання сценаріїв користувача [6].

Для реалізації якісного прототипування використовуються такі дані та інструменти:

1) Дизайн-системи та бібліотеки компонентів при використанні методології Atomic Design для створення перевикористовуваних елементів, що забезпечує консистентність інтерфейсу.
2) Прототипування високої точності (High-fidelity) у налаштуваннях інтерактивних зв'язків, анімацій переходу та логічних умов для імітації функціоналу продукту [3].
3) Інструменти розробника (Dev Mode) для аналізу специфікацій, отримання CSS-властивостей та використання Design Tokens для автоматизації передачі параметрів у код [5].

Процес побудови функціональної моделі взаємодії компонентів системи в межах прототипу можна представити у вигляді логічного циклу. Як показано на Рисунку 1, етап прототипування стає ітеративним процесом, що поєднує дизайн та технічну перевірку.

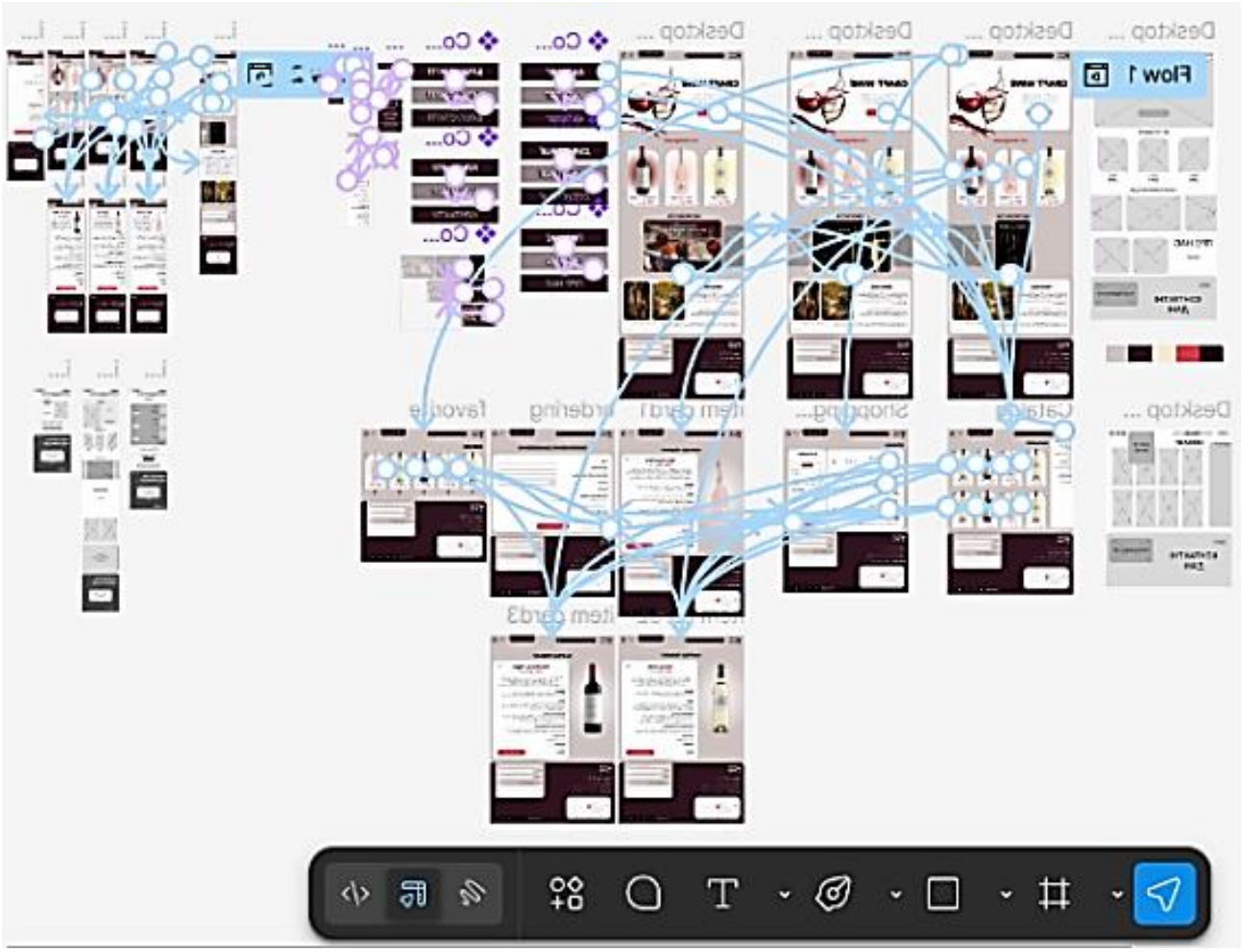


Рисунок 1. *Функціональна схема ітераційного прототипування у Figma*

Важливим аспектом методології є також використання плагінів для синхронізації даних, що дозволяє наповнювати прототипи реальним контентом (JSON, табличні дані) для максимально точного тестування UX-гіпотез.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Впровадження Figma у процес розробки дозволило трансформувати прототипування зі створення статичних зображень у розробку живих функціональних моделей продукту. Основним результатом інтеграції є радикальне скорочення часу на валідацію ідей завдяки можливості проведення коригувань у реальному часі без залучення дороговартісних ресурсів розробки.

Порівняння основних характеристик типів прототипів, що використовуються в межах дослідження, наведено в Таблиці 1.

Таблиця 1. *Порівняння кількісних та якісних метрик контенту*

Вид прототипу	Ступінь деталізації	Ключові переваги	Сфера застосування
Paper Prototype (паперовий)	Дуже низька (начерки від руки)	Миттєва візуалізація ідей, нульова вартість змін	Мозкові штурми, ранні концепт-тести
Wireframe (скелетний)	Низька (блоки, без графіки)	Чітка структура та навігація, відсутність відволікання на дизайн	Проєктування інформаційної архітектури
Mid-fidelity (середня точність)	Середня (монохром, базові шрифти)	Перевірка сценаріїв взаємодії (User Flows) без фінального візуалу	Узгодження функціональних вимог зі стейкхолдерами
High-fidelity (висока точність)	Висока (фінальна графіка, анімації)	Максимальна реалістичність, готовність до тестів на реальних користувачах	Презентації, фінальне UX-тестування, маркетинг
Functional/ Coded Prototype	Програмна (код на основі Figma)	100% відповідність технічним обмеженням, використання реальних даних	Перевірка складних алгоритмів та продуктивності

У ході аналізу було виявлено, що використання інтерактивних прототипів дозволяє стейкхолдерам отримати чітке уявлення про кінцевий продукт, що мінімізує кількість суттєвих змін на етапі написання коду. Це підтверджується впровадженням компонентного підходу: зміна одного майстер-компонента автоматично оновлює всі пов'язані екрани прототипу, забезпечуючи консистентність інтерфейсу [6].

Важливим технологічним результатом є використання режиму Dev Mode, який автоматизує процес передачі параметрів дизайну (колірні схеми, відступи, типографіка) безпосередньо розробникам у вигляді CSS, Swift або Kotlin коду [5]. Це усуває потребу в ручному створенні специфікацій.

Як показано на Рисунку 1 (див. розділ II), етап прототипування стає ітеративним процесом, що поєднує дизайн та технічну перевірку. Додатково, на Рисунку 2 продемонстровано взаємодію компонентів усередині Figma для створення складних сценаріїв.

Крім того, використання інструменту Variables дозволяє створювати умови (logic conditions), що імітують поведінку бази даних або авторизації. Це дає змогу проводити якісне тестування на користувачах ще до формування фінального технічного завдання.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Використання Figma як основного інструменту на етапі прототипування демонструє якісну зміну в парадигмі розробки ПЗ. Традиційний підхід, де дизайн був лише візуальною інструкцією, трансформується у створення динамічного середовища, що максимально наближене до фінального коду [2].

Важливим аспектом обговорення є концепція «дизайн-системи як коду». Завдяки впровадженню змінних (Variables) та режимів (Modes), прототип у Figma тепер здатний обробляти складну бізнес-логіку: від зміни мовних локалізацій до перемикання між темною та світлою темами на рівні системних токенів [3]. Це дозволяє розробникам отримувати не просто «картинку», а набір готових параметрів, що інтегруються у фронтенд-фреймворки

(React, Vue тощо) через API. Крім того, наявність функціоналу Dev Mode вирішує критичну проблему некоректної інтерпретації відступів, кольорів та анімацій, оскільки розробник бачить пряму специфікацію об'єктів [5].

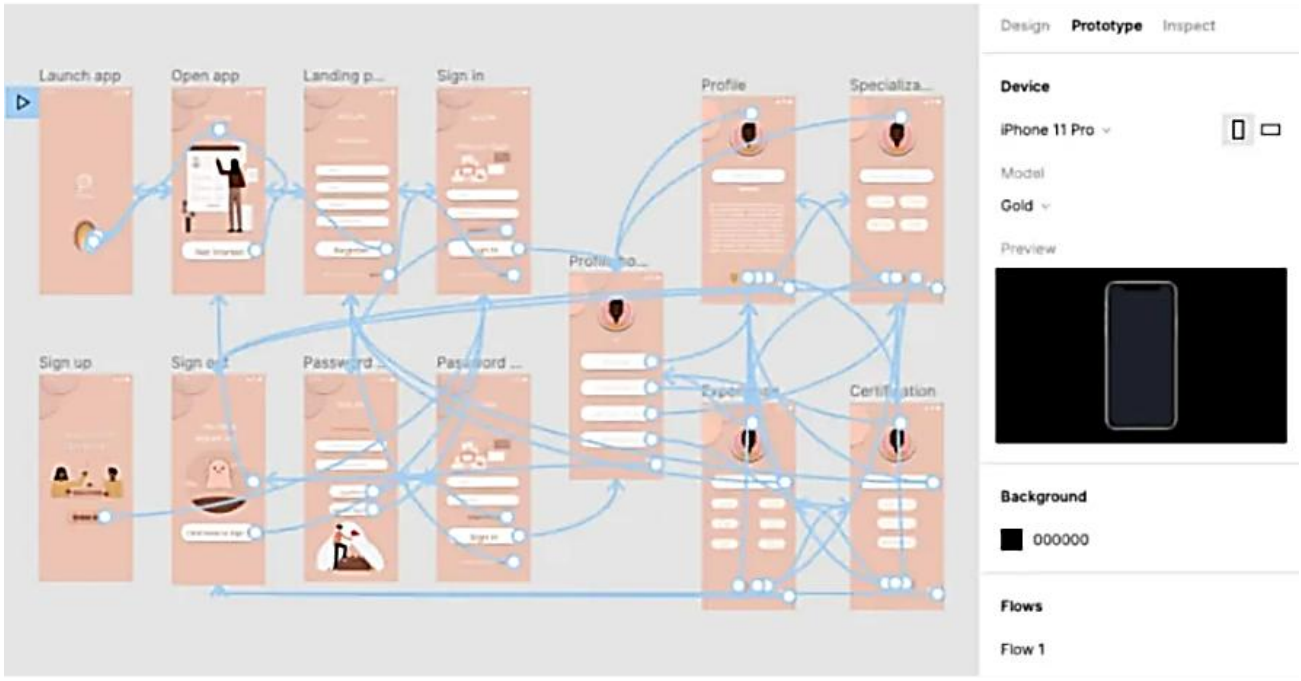


Рисунок 2. *Візуалізація інтерактивних зв'язків між екранами у прототипі Figma*

У результаті проведеного дослідження можна зробити висновок, що інтеграція Figma на етапі прототипування є стратегічно важливим кроком для сучасних IT-команд. Це забезпечує наступні переваги:

- економічна ефективність для валідації ідей через High-fidelity прототипи дозволяє уникнути витрат на розробку функцій, які можуть бути відхилені користувачами під час UX-тестування [1];
- підвищення якості продукту у ітераційному підході усередині Figma сприяє виявленню юзабіліті-дефектів на ранніх стадіях, що підвищує конверсію та задоволеність кінцевих користувачів [4];
- синергія команди, як хмарна природа інструменту створює єдиний простір для комунікації, де коментарі стейкхолдерів та технічні зауваження розробників прив'язані до конкретних елементів інтерфейсу [5].

Перспективним напрямком подальших розробок є автоматизація синхронізації між Figma та GitHub за допомогою спеціалізованих плагінів, що дозволить автоматично оновлювати стилі в репозиторії при зміні їх у дизайні. Також актуальним залишається питання використання генеративного ШІ для автоматичної побудови навігаційних зв'язків у складних багатоекранних системах.

ДЖЕРЕЛА

1. Staiano, F. (2022). Designing and Prototyping Interfaces with Figma: Learn essential UX/UI design principles by creating interactive prototypes for mobile, tablet, and desktop. Packt Publishing Ltd.

2. Putri, R. E., Fadly, Y., Purwanto, D., & Pardede, J. (2024). Prototype (desain UI UX) aplikasi perpustakaan digital dengan Figma. Penerbit Tahta Media.
3. Alda, M., Kurniawan, A. A., Ramadhani, V., & Ananda, M. R. (2026). Designing a Mobile Application Prototype for Accessing and Publishing Student Journals using Figma. Journal of Artificial Intelligence and Engineering Applications (JAIEA), 5(2), 3058-3063.
4. Pratama, M. O. D., & Suwarni, S. (2022). Pengembangan Prototipe Desain User Interface & User Experience (UI/UX) Pada Aplikasi OSS URINDO Menggunakan FIGMA. Jurnal Teknologi Informasi, 8(2), 155-166.
5. Huang, T. (2024). Fead: Figma-enhanced app design framework for improving UI/UX in educational app development. arXiv preprint arXiv:2412.06793.
6. Stewart, L. (2024). Evaluating the Alignment between Usability Requirements and Real-World Interface Design. Available at SSRN 5247130.
7. Олег Захарія, Наталія Кунанець, Юрій Жовнір. "ФОРМУВАННЯ ТЕХНІЧНОЇ ДОКУМЕНТАЦІЇ ІТ ПРОЄКТІВ В КОНТЕКСТІ РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ." (2025). INFORMATION SYSTEMS AND NETWORKS. Issue 18, part 1, 2025. https://doi.org/10.23939/sisn2025.18.
8. Ю.Г. Лобода, О.Г. Трофименко, С.Ю. Манаков , В.І. Гура. "Штучний інтелект у сучасній веброзробці та вебдизайні: багаторівнева класифікація та систематизація." *Informatics and Mathematical Methods in Simulation Vol.15 (2025), No.1, pp. 126-136.* DOI 10.15276/imms.v15.no1.126
9. Cherukuri B. Enhancing Web Application Performance with AI - Driven Optimization Techniques. International Journal of Science and Research (IJSR). 2021. Vol. 10. Issue 2. P. 1779-1788. https://www.ijsr.net/getabstract.php?paperid=SR21021103246. DOI: https://doi.org/10.21275/sr21021103246.



МАРГАРИТА ГЛАДКА
студентка 1 курсу бакалаврату технологій веброзробки та вебдизайну у Київському національному університеті імені Тараса Шевченка.
E-mail: margohladka@gmail.com
Серед наукових інтересів — технології вебдизайну, оптимізація користувацького досвіду (UX), а також алгоритми машинного навчання в задачах аналізу даних та автоматизації.



ОЛЬГА БОНДАРЕНКО
асистент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-0024-8789
E-mail: olha.bondarenko@knu.ua
Фахівець у галузі інформаційних систем, телекомунікацій та радіомовлення. Практичний досвід роботи у сфері телекомунікацій та медіаінфраструктури понад 8 років. Досвід викладання в університетах України понад 3 роки.
Наукові інтереси – інформаційно-комунікаційні системи, системи радіомоніторингу, мультисенсорні технології та IoT.

КІБЕРБЕЗПЕКА ТА НАДІЙНІСТЬ ЯК ВБУДОВАНІ ПРОЦЕСИ ГІБРИДНОГО УПРАВЛІННЯ IOT-ПРОЄКТАМИ В ЕНЕРГОСИСТЕМАХ

Дмитро Загородній, Ігор Пархомей

Анотація. *У роботі розглянуто підхід до інтеграції кібербезпеки та надійності як вбудованих процесів у гібридному управлінні IoT-проєктами в енергосистемах. Для формалізації вимог використано перелік кіберможливостей IoT-пристроїв, визначений у NISTIR 8259A (ідентифікація, конфігурація, захист даних, контроль доступу, безпечні оновлення, спостереження стану захисту). Запропоновано застосування критеріїв готовності на stage-gate переходах, а також кількісних показників кіберготовності CR і ризику Rj для підтримки управлінських рішень щодо переходу до пілоту та промислової експлуатації.*

Ключові слова: кібербезпека, надійність, критерії готовності, оцінювання ризиків, NISTIR 8259A

I. ВСТУП

Кібербезпека та надійність у проєктах розробки й упровадження IoT-рішень для енергосистем доцільно розглядати як наскрізні процеси, інтегровані в управління проєктом на всіх етапах життєвого циклу. Це зумовлено кіберфізичною природою енергетичної інфраструктури, де помилки ПЗ, конфігурацій пристроїв або мережевих політик можуть призводити до простоїв і зростання операційних ризиків. Додаткову складність формують конвергенція IT/OT, різнорідність пристроїв і постачальників, а також тривала експлуатація IoT-флоту з регулярними оновленнями та змінами налаштувань.

Традиційні стадійні підходи управління часто недостатньо гнучкі для роботи з невизначеністю вимог і швидкими ітераціями, тоді як суто гнучкі підходи не завжди забезпечують формалізований контроль, відповідальність і критерії переходу між критичними етапами (пілот, промислова експлуатація, масштабування). Тому актуальним є гібридний підхід, який поєднує stage-gate контроль для ключових рішень із ітеративною розробкою та валідацією для програмних компонентів та інтеграцій, доповнюючи їх вбудованими процедурами безпеки й надійності.

Метою роботи є обґрунтування підходу до інтеграції кібербезпеки та надійності як вбудованих процесів гібридного управління IoT-проєктами в енергосистемах. Передбачається подання вимог до безпеки й надійності у вигляді вимірюваних критеріїв готовності та їх перевірка на кожному контрольному переході, з акцентом на базові кіберможливості IoT-пристроїв (ідентифікація, керування конфігурацією, захист даних, контроль доступу, безпечні оновлення, моніторинг стану захисту) та їх верифікацію до пілоту і промислового розгортання. Очікуваний ефект полягає в підвищенні керованості ризиків, зменшенні переробок на інтеграції та зростанні надійності експлуатації IoT-рішень.

II. ДАНІ ТА МЕТОДИ

У роботі використано змішаний дизайн дослідження: аналіз нормативно-рекомендаційних джерел для формування вимог до кіберзахисту IoT-компонентів в OT-середовищі та розробку процесної моделі гібридного управління проєктами з оцінюванням через критерії готовності й метрики ризику. Базовий перелік кіберможливостей IoT-пристрою сформовано за NISTIR 8259A (ідентифікація, керування конфігурацією, захист даних, контроль доступу до інтерфейсів, безпечні оновлення ПЗ, спостереження стану кіберзахисту). Для індустріального контексту використано підхід

ISA/IEC 62443, зокрема логіку спільної відповідальності між зацікавленими сторонами життєвого циклу (asset owner, integrator, supplier/service) [1, 2].

Запропоновано гібридну модель "етапи + ітерації", у якій stage-gates визначають критичні переходи (концепт → пілот → промислова експлуатація → масштабування), а всередині етапів застосовуються ітерації розробки та інтеграції. Вимоги кібербезпеки й надійності включено до умов приймання на кожному gate у вигляді перевірюваних критеріїв готовності.

Для операціоналізації вимог застосовано матрицю відповідності "кіберможливість → артефакти → перевірка", наведено у Таблиці 1, яка забезпечує однозначну трасованість вимог до конкретних результатів проєкту та процедур верифікації [3].

Таблиця 1. *Відповідність кіберможливостей IoT-пристрою артефактам проєкту та перевіркам (за NISTIR 8259A)*

Кіберможливість	Артефакт(и) в проєкті	Перевірка перед gate-рішенням
Ідентифікація пристрою	Реєстр активів/пристроїв, правила ідентифікації	Перевірка унікальності ID, тест інвентаризації
Керування конфігурацією	Еталонні налаштування, правила внесення змін	Контрольована зміна + наявність журналу змін
Захист даних	Політики передавання/зберігання даних	Перевірка захисту даних під час передачі та зберігання
Контроль доступу до інтерфейсів	Матриця ролей/прав, правила автентифікації	Тест: доступ лише для авторизованих сутностей
Безпечні оновлення ПЗ	Процедура OTA/оновлення, правила відкату	Тест: оновлення проходить перевірки; перевірка відкату (за потреби)
Спостереження стану захисту	Набір security-подій/метрик, телеметрія	Перевірка наявності подій/метрик та їх доступності для моніторингу

Для кількісної оцінки "готовності" компонента/підсистеми застосовується інтегральний показник кіберготовності CR, що агрегує ступінь виконання вимог із вагами за критичністю активу та сценаріїв використання:

$$CR = \sum_{i=1}^{n} \omega_i * s_i, \sum_{i=1}^{n} \omega_i = 1, \quad (1)$$

де Si ∈{0,1} - виконання і-ї вимоги (1 - виконано, 0 - не виконано), ωi - вага (відносна важливість вимоги для заданого контексту впровадження).

Для підтримки рішень на контрольних переходах використовується оцінка ризику:

$$R_j = P_j * I_j, \quad (2)$$

де Rj - ризик j-ї загрози/відмови, Pj - оцінка ймовірності, Ij - оцінка впливу (з урахуванням наслідків для доступності, цілісності, конфіденційності та операційних показників).

Рішення про перехід через gate формалізується як виконання порогів CR ≥ CRmin та Rj ≤ Rmax для визначеного набору критичних ризиків. Це дозволяє включати безпеку й надійність у проєктні рішення щодо готовності до пілоту/експлуатації [3].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Сформовано набір критеріїв готовності для контрольних переходів у гібридному управлінні IoT-проєктами в енергосистемах, у якому кібербезпека та надійність представлені як формалізовані умови приймання рішення “перейти/повернути на доопрацювання/призупинити”. Вихідним результатом є стандартизований перелік перевірок для IoT-компонента, узгоджений із переліком кіберможливостей NISTIR 8259A (ідентифікація, керування конфігурацією, захист даних, контроль доступу, безпечні оновлення, спостереження стану захисту). Для промислового (OT) середовища додатково визначено відповідальні ролі за виконання перевірок і підготовку артефактів (власник активу, інтегратор, постачальник/сервіс), що відповідає логіці розподілу ролей у підходах, пов’язаних із екосистемою ISA/IEC 62443 [3].

Ключовим результатом формалізації стало введення кількісного показника кіберготовності CR, який використовується як пороговий індикатор у gate-рішеннях. Для демонстрації застосовності показника виконано ілюстративний приклад для шести груп вимог із Таблиці 1 (по одній на кожну кіберможливість NISTIR 8259A). Нехай значення виконання S_i дорівнюють: ідентифікація - 1, конфігурація - 1, захист даних - 0, контроль доступу - 1, оновлення - 0, спостереження стану - 1; ваги задані як

W = {0.1, 0.15, 0.2, 0.25, 0.2, 0.1} (більша вага надана контролю доступу та оновленням як типовим “точкам провалу” при експлуатації IoT-флоту). За формулою:

$$CR = \sum_{i=1}^{n} \omega_i * s_i \tag{3}$$

отримується CR = 0.1 + 0.15 + 0 + 0.25 + 0 + 0.1 = 0.6, що нижче умовного порогу CRmin = 0.8. отже перехід до промислової експлуатації потребує доопрацювання.

Недостатня готовність у прикладі зумовлена невиконанням вимог щодо захисту даних і безпечних оновлень, які в NISTIR 8259A визначені як окремі критичні кіберможливості, пов’язані зі зниженням ризиків компрометації даних та керуванням уразливостями під час експлуатації [3].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонований підхід дозволяє інтегрувати кібербезпеку та надійність у гібридне управління IoT-проєктами через чіткі критерії готовності на контрольних переходах, що зменшує ймовірність “перенесення” критичних дефектів на етап промислової експлуатації. Практичний ефект очікується у вигляді кращої керованості оновлень, доступів, конфігурацій і моніторингу стану захисту, оскільки ці елементи прямо відповідають ключовим кіберможливостям IoT-пристроїв, визначеним у NISTIR 8259A. Для енергетичного (OT) середовища додатковою перевагою є узгодження ролей і відповідальності учасників життєвого циклу, що відповідає принципу “people, processes and technology” та орієнтації ISA/IEC 62443 на безпеку протягом усього життєвого циклу систем[4, 5].

Обмеженням є залежність результатів оцінювання від експертного вибору ваг ω_i та порогів CR_{min}, а також від доступності даних для об’єктивної оцінки ймовірностей і впливів у ризик-моделі $R_j = P_j * I_j$. Подальші дослідження доцільно спрямувати на апробацію підходу на реальних кейсах енергетичних IoT-впроваджень з порівнянням показників до/після (час виходу на пілот, частка переробок, частота інцидентів/відмов) та уточненням набору критеріїв готовності для різних класів активів[6].

ДЖЕРЕЛА

1. International Society of Automation (ISA). (2024). ISA/IEC 62443 Series of Standards. International Society of Automation. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
2. ISA Global Cybersecurity Alliance (ISAGCA). (2021). Industrial Automation and Control System: Principal Roles and Responsibilities. ISA Global Cybersecurity Alliance. URL: https://gca.isa.org/hubfs/21-29%20-%20ISAGCA/ISAGCA-IACS%20Roles%20and%20Responsibilities.pdf
3. Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A). National Institute of Standards and Technology (NIST). URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259a.pdf
4. National Institute of Standards and Technology (NIST). (2020). NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline (Final). NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov/pubs/ir/8259/a/final
5. ISA Global Cybersecurity Alliance (ISAGCA). (2022). ISA/IEC 62443 Series of Standards. ISA Global Cybersecurity Alliance. URL: https://isagca.org/isa-iec-62443-standards
6. Wordvice. (2025). How to Write the Results/Findings Section in Research. Wordvice Blog. URL: https://blog.wordvice.com/writing-the-results-section-for-a-research-paper/
7. National Institute of Standards and Technology (NIST). (2021). IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog (NIST SP 800-213A). NIST Special Publication 800-213A. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf
8. Cisco. (2024). ISA/IEC-62443-3-3: What is it and how to comply? A Cybersecurity Framework to Protect Industrial Automation and Control Systems. Cisco White Paper. URL: https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html
9. ISA Global Cybersecurity Alliance (ISAGCA). (2023). IoT Security Maturity Model: ISA/IEC 62443 Mappings for Asset Owners, Product Suppliers and Service Providers. ISA Global Cybersecurity Alliance. URL: https://www.isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/SMM-62443-Asset-Owner-Product-Supplier-Service_20230809.pdf



ДМИТРО ЗАГОРОДНІЙ
студент 2 курсу аспірантури кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0007-8280-7201
E-mail: dimahome8@gmail.com
Отримав ступінь бакалавра комп'ютерної інженерії у Національному Університеті Біоресурсів і Природокористування (Київ, Україна) в 2022 році. Нині здобуває ступінь магістра на кафедрі інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка . Свою кар'єру почав в 2021 році в ДП "ІНФОТЕХ" на посаді Python Backend Developer. З 2022 року працює в ДП "ІЦПОПФУ" на посаді мережевого інженера.



ІГОР ПАРХОМЕЙ
д.т.н., професор, кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0002-9510-7657
E-mail: ihor.parkhomei@nnp.nau.edu.ua
Отримав ступінь магістра управління у Національній академії оборони України (Київ, Україна) в 2004 році. Доктор технічних наук з радіотехнічних пристроїв та засобів телекомунікацій (Державний університет телекомунікацій). Серед наукових інтересів - системи управління та радіоавтоматика.

АНАЛІТИКА ПОВЕДІНКИ КОРИСТУВАЧІВ У СИСТЕМАХ ВИПАДКОВИХ ВИНАГОРОД: МЕТОДИ ПРОГНОЗУВАННЯ УТРИМАННЯ ТА ВІДТОКУ КОРИСТУВАЧІВ

Любов Кубявка, Станіслав Ганчев

Анотація. *Досліджено проблему низького рівня утримання користувачів у мобільних іграх з механікою випадкових винагород (gacha). Метою роботи є обґрунтування методологічного підходу до прогнозування відтоку на основі глибокого аналізу ігрової телеметрії та системного A/B тестування механік. Запропоновано авторську систему специфічних метрик (зокрема показники pity-лічильників та темпи прогресії) та комплексний аналітичний підхід із застосуванням алгоритмів XGBoost, Random Forest та LSTM нейронних мереж.. Розроблено архітектуру аналітичного дашборду реального часу, що дозволяє здійснювати превентивний моніторинг ігрової економіки. Практична значущість дослідження полягає у створенні інструментарію для прийняття управлінських рішень на основі даних, що забезпечує оптимізацію маркетингових стратегій та подовження життєвого циклу користувачів у високонавантажених цифрових продуктах.*

Ключові слова: gacha-системи; утримання; відтік; прогнозна аналітика; IT-проєкт; live-service ігри.

I. ВСТУП

Індустрія ігор з механікою випадкових винагород (gacha) — Genshin Impact, Wuthering Waves тощо — демонструє мільярдні обороти, проте стикається з критично низьким показником утримання. За даними галузевих звітів (зокрема deltaDNA), понад 70% нових гравців залишають гру протягом першої доби. Враховуючи, що середня вартість залучення одного активного користувача (CAC) у мобільному геймінгу наразі становить від $5 до $15 залежно від регіону, такий рівень відтоку створює суттєві фінансові ризики.

Специфіка gacha-ігор полягає у монетизації через випадковість, що потребує тонкого балансування між мотивацією до покупки та фрустрацією гравця. Метою роботи є розробка методології ідентифікації факторів утримання та побудова прогнозних моделей для превентивного управління відтоком користувачів.Ця проблема посилюється в контексті моделі ігор з постійно оновлюваним контентом — з регулярними оновленнями, системами тимчасових подій та складною внутрішньоігровою економікою. Попри наявні дослідження у сфері аналітики відтоку [2–4], залишаються недостатньо вивченими: методологія ідентифікації критичних факторів утримання, специфічних для систем випадкових винагород; адаптація прогнозних моделей до ігор з циклічними оновленнями контенту; етичні аспекти A/B тестування ігрових механік. Метою роботи є обґрунтування методологічного підходу до аналітики поведінки користувачів у системах випадкових винагород для підвищення ефективності управління утриманням та зменшення відтоку

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На основі аналізу телеметричних даних ігор з механікою випадкових винагород визначено систему критичних метрик утримання, що включає чотири групи показників.

Перша група — метрики залученості: DAU (Daily Active Users — кількість унікальних активних користувачів на день), MAU (Monthly Active Users — кількість унікальних активних користувачів на місяць), а також показники утримання D1/D7/D30 (відсоток гравців, які повернулися до гри на 1-й, 7-й та 30-й день відповідно). Особливо критичним є показник D1, оскільки перші 24 години визначають довгострокову залученість гравця.

Друга група — метрики монетизації: ARPU (Average Revenue Per User — середній дохід з одного користувача), ARPPU (Average Revenue Per Paying User — середній дохід з одного платного користувача), LTV (Lifetime Value — сукупний дохід від користувача за весь час його перебування у грі), а також conversion rate (коефіцієнт конверсії — частка гравців, які перейшли від безкоштовної гри до здійснення платежів). Специфічною для систем випадкових винагород є метрика «кількість спроб до першої покупки», яка корелює з подальшою готовністю гравця до витрат.

Третя група — метрики взаємодії з механікою випадкових винагород: кількість безоплатних та оплачених спроб отримати персонажа, показник pity-лічильника (гарантії — механізм, що забезпечує отримання рідкісного предмета після певної кількості невдалих спроб), успішність отримання бажаних персонажів, рівень участі у тимчасових тематичних подіях. Ці метрики є унікальними індикаторами ризику відтоку, характерними саме для цього типу ігор.

Четверта група — метрики прогресії: рівень акаунта, ступінь проходження основного контенту, participation rate (рівень участі) у кінцевому ігровому контенті для досвідчених гравців.

На основі аналізу телеметричних даних ігрових сесій (на прикладі відкритих датасетів ігрової активності) визначено чотири групи критичних метрик:

1. Залученість: DAU/MAU, а також показники утримання D1, D7 та D30.
2. Монетизація: ARPU, ARPPU, LTV та швидкість конверсії у першу покупку.
3. Ігрова механіка: кількість спроб до отримання цілі, показники pity-лічильника (гарантованих виплат) та рівень участі у циклічних подіях.
4. Прогресія: рівень акаунта та темпи проходження основного контенту.

Для прогнозування ризику відтоку гравців запропоновано комплексний підхід, що комбінує кілька алгоритмів машинного навчання. Логістична регресія забезпечує базову бінарну класифікацію (відтік / не відтік) з інтерпретацією впливу окремих факторів через коефіцієнти шансів. Random Forest (метод випадкового лісу — алгоритм на основі ансамблю дерев рішень) ефективний для виявлення нелінійних залежностей і визначення важливості окремих показників (feature importance). XGBoost (градієнтний бустинг — метод послідовного навчання слабких моделей) демонструє високу точність на структурованих даних і рекомендується для промислових систем завдяки швидкості. LSTM (Long Short-Term Memory — нейронні мережі з довгою короткостроковою пам'яттю) застосовуються для аналізу часових рядів поведінки гравців з урахуванням сезонності циклів подій та ротації тематичних банерів, з яких дістаються персонажі або зброя. Комбінований підхід дозволяє досягти точності прогнозування понад 75–82%.

Розроблена методологія A/B тестування механік випадкових винагород базується на принципах справедливості та рівності між групами гравців. Тести не повинні створювати довгострокову нерівність: рекомендується тестувати зміни у безкоштовній ігровій валюті та інтерфейсі механіки випадкових винагород, але не в базових ігрових елементах. Сегментація здійснюється за стратами (новачки проти ветеранів), поведінкою витрат (безкоштовні гравці проти великих платників) та рівнем залученості. Мінімальна тривалість тесту — 2–3 повних цикли подій (2–6 тижнів) для врахування сезонності. Первинною метрикою успішності є D7 (утримання на сьомий день), вторинними — ARPU (середній дохід з користувача) та тривалість ігрових сесій.

Запропонована архітектура аналітичного дашборду реального часу включає чотири ключові компоненти: (1) візуалізацію кривої утримання для різних груп користувачів з деталізацією за атрибутами (джерело залучення, час реєстрації, перший отриманий персонаж); (2) автоматичні сповіщення про сегменти з підвищеним ризиком відтоку (поріг: понад 70% прогнозована ймовірність відходу) з рекомендаціями щодо кампаній утримання; (3) реал-тайм трекінг метрик активних A/B-експериментів зі статистичною значущістю та

довірчими інтервалами; (4) моніторинг внутрішньоігрової економіки (інфляція ігрової валюти, розподіл ресурсів, патерни витрат гравців) для уникнення дисбалансів.

III. ВИСНОВКИ

У роботі обґрунтовано методологічний підхід до аналітики поведінки користувачів у системах випадкових ігрових винагород на основі комбінації прогнозної аналітики та A/B тестування. Визначено специфічні метрики утримання та відтоку для механік випадкових винагород, що відрізняються від загальноігрових показників урахуванням pity-систем (механізмів гарантованих виграшів), ротації тематичних банерів та циклів подій.

Доведено, що комбінація прогнозної аналітики та стратегічного A/B тестування дозволяє ефективно керувати життєвим циклом користувача. Практична значущість полягає у можливості автоматизованого виявлення сегментів гравців з високим ризиком відходу (поріг >60% ймовірності) та впровадження персоналізованих кампаній з утримання. Це дозволяє оптимізувати маркетингові витрати та підвищити загальну рентабельність ігрових продуктів.

Практична значущість дослідження полягає у розробці архітектури аналітичного дашборду для менеджерів продукту, що забезпечує прийняття рішень на основі даних щодо балансування ігрової економіки та оптимізації кампаній утримання гравців.

Перспективи подальших досліджень: розробка рекомендаційних систем для персоналізованих пропозицій на основі прогнозованого ризику відтоку; дослідження впливу соціальних функцій на показники утримання; аналіз кросплатформенної поведінки користувачів (мобільні пристрої, ПК, консолі); вивчення довгострокових ефектів механік випадкових винагород на задоволення гравців та лояльність до бренду.

ДЖЕРЕЛА

1. Genshin Impact Revenue and Usage Statistics (2025). [Електронний ресурс]. — Режим доступу: https://www.businessofapps.com/data/genshin-impact-statistics/
2. Miloš Milošević, Nenad Živić, Igor Andjelković. Early churn prediction with personalized targeting in mobile social games (2017). [Електронний ресурс]. — Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0957417417303044
3. Canhui Chen, Zhixuan Fang. Gacha Game Analysis and Design.
4. Seungwook Kim, Daeyoung Choi, Eunjung Lee, Wonjong Rhee. Churn prediction of mobile and online casual games using play log data.



ЛЮБОВ КУБЯВКА
к.т.н., доцент кафедри технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0005-5397-1585
E-mail: liubov.kubiavka@knu.ua
Викладач з 2015 р. Має більше 100 наукових праць. Серед наукових інтересів — бізнес-аналітика ІТ проєктів, технології управління життєвим циклом ІТ проєктів, реінжиніринг бізнес-процесів, управління програмами інформатизації, цифровізації, командоутворення, Lean-менеджмент та прогнозна аналітика.



СТАНІСЛАВ ГАНЧЕВ
студент 1 курсу магістратури технологій управління у Київському національному університеті імені Тараса Шевченка.
E-mail: stas.hanchev@gmail.com
Наукові інтереси зосереджені у сфері аналітики поведінки користувачів у цифрових продуктах, прогнозному моделюванні відтоку користувачів на основі методів машинного навчання, а також в управлінні ІТ-проєктами у індустрії розробки ігор.

АВТОМАТИЗОВАНА СЕРІАЛІЗАЦІЯ (Е-АКЦИЗ) З ВИКОРИСТАННЯМ IOT-РІШЕНЬ

Дмитро Неделько, Володимир Дружинін

Анотація.. *Розглянуто концепцію автоматизованої серіалізації продукції з використанням IoT-технологій на прикладі української системи електронної акцизної марки («еАкциз»). Описано нанесення унікальних ідентифікаторів (DataMatrix-кодів) за допомогою сучасного обладнання (лазерне та термотрансферне маркування), відстеження транспортування й місцезнаходження продукції на складах, а також інформаційну інфраструктуру системи (сервер та базу даних) для обробки і збереження даних про кожну одиницю продукції. Розглянуто роль сканерів штрих-кодів у верифікації акцизних марок, а також необхідне друкуюче обладнання. На прикладі еАкциз показано, як інтеграція цих компонентів забезпечує прозорість ланцюга постачання і боротьбу з нелегальним обігом.*

Ключові слова: IoT, серіалізація, DataMatrix, сканування, трекінг, еАкциз, база даних, марка.

I. ВСТУП

Автоматизована серіалізація передбачає присвоєння кожній одиниці товару унікального ідентифікатора і відстеження її руху в реальному часі. Система еАкциз в Україні впроваджує саме такий підхід для підакцизних товарів (алкоголь, тютюн, рідини для електронних сигарет). Вона створена як єдиний цифровий сервіс контролю обігу таких товарів «від виробника або імпортера до точки продажу». Ефективна серіалізація ґрунтується на нанесенні на кожну упаковку товару електронної акцизної марки - двовимірного DataMatrix-коду з унікальним цифровим ідентифікатором. Подібна система відповідає європейським стандартам Track & Trace і забезпечує прозорість обігу продукції. З 1 січня 2026 року в Україні тестується система еАкциз: зокрема, введено обов’язок наносити на кожну пачку сигарет або пляшку марку DataMatrix із унікальним кодом.

II. МЕТА

Розробити комплексну систему маркування і відстеження продукції, що забезпечує прозорий ланцюг поставок і виключає нелегальний обіг.

Демонструвати функціонування інформаційної системи еАкциз, яка об’єднує маркування, збір даних і їх обробку для контролю платників акцизу і безпосередньо споживачів.

Показати переваги використання IoT у виробництві та логістиці продукції - моніторинг умов зберігання та геолокації пакунків.

Окреслити роль серверної інфраструктури та бази даних для фіксації кожної одиниці продукції і реєстрації подій обігу.

Навести можливість верифікувати легальність товару через мобільний додаток та контролювати переміщення вантажів у системі.

III. МЕТОДИ ТА КОМПОНЕНТИ СИСТЕМИ

Для нанесення електронної марки на продукцію можуть використовуватися промислові принтери-аплікатори або лазери. Ці системи наносять як DataMatrix-коди, так і текстові написи прямо на пакунок або етикетку для подання людині загальної інформації.

IoT-датчики для інтеграції автоматизованої серіалізації, верифікації та агрегації на виробництві. Сканери зчитування кодів для перевірки якості самого коду та нанесення.

На виробництві та складах використовуються промислові етикеткові принтери для друку DataMatrix-кодів на етикетках чи пакуванні. У логістиці та роздрібній торгівлі застосовуються сканери штрих-кодів (ручні), які зчитують коди з упаковок при прийманні, переміщенні чи продажі товару. На касах торговельних мереж модулі РРО/пРРО реєструють дані зчитаного коду - після сканування одиниця продукції виводиться з обігу і марка «спалюється». Функціонально сканування на різних етапах (виробництво, склад, транспорт, магазин) «дасть змогу відстежувати переміщення товару» і заносити ці події у систему. Крім того, продавцям потрібно забезпечити відображення коду еАкциз у фіскальних чеках.

На Рисунку 1 зображено серіалізацію на виробництві, який показує як відбувається процес від нанесення унікального ідентифікатора на продукт до нанесення унікального групового ідентифікатора на палету для подальшої логістики.

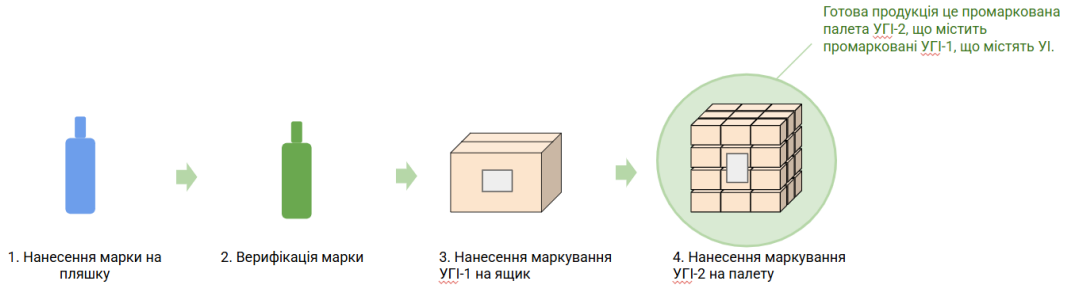


Рисунок 1. *Процес серіалізації на виробництві*

Хмарна платформа збирає і аналізує інформацію з усіх джерел: заявки на нові маркувальні коди, зчитування від IoT-датчиків, сканування кодів на різних етапах тощо. Сервер забезпечує валідацію та активацію кодів після сплати акцизу виробником/імпортером, фіксує кожну зміну статусу одиниці товару і інтегрується з іншими державними реєстрами (митниця, податкова, складські системи), що гарантує синхронність даних.

Ключовий компонент - надійна база даних, яка містить записи про кожен унікальний код продукції. Прикріпивши DataMatrix до упаковки і зареєструвавши його в системі, ми отримуємо можливість відстежувати кожну одиницю протягом всього ланцюга поставок. В базі даних зберігаються параметри товару (виробник, дата випуску тощо), історія проходження через митницю, перевізника, склад та інформація про продаж. На Рисунку 2 зображено схему що демострує всі процеси на виробництві та в логістиці, де Gateway - це хмарна платформа.

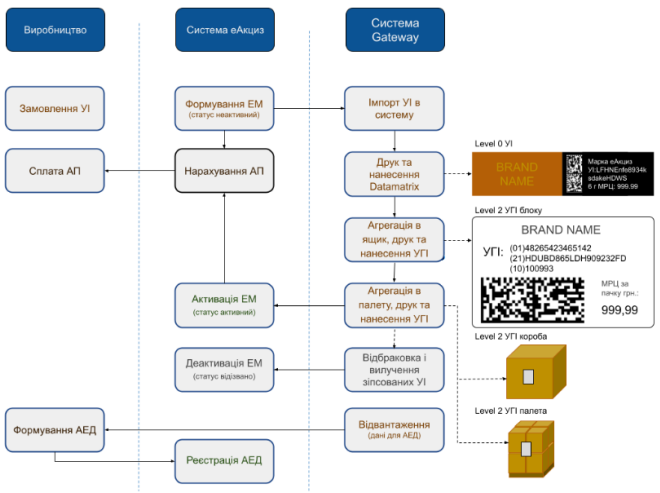


Рисунок 2. *Діаграма процесів*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Така інтеграція демонструє суттєві переваги: влада отримує можливість бачити «шлях товару від виробника до полиці магазину», внаслідок чого знижується обсяг нелегальної продукції на ринку. Запровадження унікального коду на кожній одиниці товару усуває «людський фактор» та корупційні ризики при контролі руху акцизних товарів. Система також автоматизує адміністрування податку (податок сплачено → марка активована) і дає інструментарій податковим органам для аудитів. Споживачі та бізнес отримують швидку перевірку легальності та історії товару, а держава - захищений і аналітично повний реєстр обігу продукції.

ДЖЕРЕЛА

1. Міністерство цифрової трансформації України. «еАкциз: створюємо систему чесного обігу». https://thedigital.gov.ua/news/technologies/eaktsiz-stvoryuemo-sistemu-chesnogo-obigu-tyutyunu-ta-alkogolyu-rezultati-vidryadzhennya-do-es
2. Державна податкова служба України. «Е-Акциз: затвердження порядку маркування електронними марками акцизного податку». https://dn.tax.gov.ua/media-ark/news-ark/946279.html
3. РБК-Україна. «З 1 січня почнуть тестувати «еАкциз»: що зміниться і для кого». https://www.rbc.ua/ukr/news/ukrayini-1-sichnya-pochnut-testuvati-eaktsiz-1767186164.html
4. WebChek. «еАкциз – рішення для інтеграції типових конфігурацій BAS». https://www.webchek.com.ua/eakciz_bas/
5. SystemGroup. «еАкциз: Яке обладнання та програми потрібні виробникам?». https://systemgroup.com.ua/uk/o-kompanii/article/eakcyz-yake-obladnannya-ta-programy-potribni-vyrobnykam-dystrybutoram-ta-riteyleram
6. Plasgad. «IoT Packaging for Logistics: Real-time data to boost your business». https://www.plasgad.com/iot/



ДМИТРО НЕДЕЛЬКО
Студент 1-го курсу магістратури, факультет інформаційних технологій, кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID: 0009-0009-7720-8647
E-mail: nedelkod@fit.knu.ua



ВОЛОДИМИР ДРУЖИНІН
Д.т.н., проф., завідувач кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@fit.knu.ua
Понад 100 наукових праць, серед яких 7 навчально-методичних посібники, 6 монографій, 7 публікацій у виданнях, включених до наукометричних баз даних Scopus та WoS. Індекс Гірша в Scopus – 4, у Google Scholar – 6.

ВИКОРИСТАННЯ МУЛЬТИМОДАЛЬНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ПРОТОТИПУВАННЯ ІНТЕРФЕЙСІВ КОРИСТУВАЧА

Юрій Поліщук, Сергій Грибков

Анотація. *Досліджено застосування мультимодальних великих мовних моделей у поєднанні з Model Context Protocol (MCP) для швидкого прототипування інтерфейсів користувача. Розглянуто pipeline із трьох MCP-інструментів — mobile-mcp для фіксації стану мобільного UI, agent-browser для аналізу веб-інтерфейсу та Pencil для AI-керованої генерації дизайну — оркестрованих AI-агентом Claude. Використання запропонованого підходу апробовано при створенні wireframes та повноцінної дизайн-системи для існуючого крос-платформного застосунку.*

Ключові слова: штучний інтелект; великі мовні моделі; прототипування інтерфейсів; Model Context Protocol; UI/UX дизайн.

I. ВСТУП

Прототипування інтерфейсів користувача є одним із найбільш трудомістких етапів розробки програмного забезпечення. Для невеликих команд та індивідуальних розробників створення якісних прототипів часто вимагає залучення дизайнерів або значних витрат часу на самостійне освоєння дизайн-інструментів.

Сучасні мультимодальні LLM (Large Language Model — велика мовна модель), такі як Claude від компанії Anthropic, GPT-5 від компанії OpenAI та Gemini від компанії Google, здатні аналізувати зображення інтерфейсів та генерувати код UI-компонентів [1]. Найпоширенішим підходом є парадигма «знімок екрана → код», тобто користувач надає моделі знімок існуючого інтерфейсу або створений від руки макет, а LLM генерує відповідний програмний код на основі візуального аналізу зображення. Однак цей підхід має суттєві обмеження – модель працює лише з пікселями растрового зображення та не має доступу до структури дизайну [2].

Компанія Anthropic у листопаді 2024 року представила відкритий стандарт Model Context Protocol (MCP), що змінює парадигму «знімок екрана → код» [3]. MCP стандартизує взаємодію AI-агентів із зовнішніми інструментами через архітектуру клієнт-сервер на основі JSON-RPC 2.0. Завдяки MCP, AI-агент може безпосередньо взаємодіяти з усіма іншими інструментами, що зараз використовуються людьми у професійній розробці. Прикладом одного з інструментів можна виділити програмний продукт Figma, що є один із найпопулярніших редакторів для створення макетів інтерфейсу користувача. У ньому інтерфейс будується з багаторазових векторних компонентів, об’єднаних дизайн-системою із токенами (кольори, типографіка, відступи), що гарантує узгодженість дизайну. Парадигма «знімок екрана → код» не здатна відтворити цю структурованість, адже AI кожен раз працює з окремим знімком, не маючи контексту загальної дизайн-системи.

Останнім часом спостерігається виникнення нової категорії ПЗ — AI-native, де AI-агент є не допоміжним доповненням, а повноправним користувачем системи нарівні з людиною. Прикладом такого інструменту у сфері дизайну є Pencil [6]. В ньому файли зберігаються у машиночитабельному JSON-форматі (.pen), а MCP-сервер є першокласним інтерфейсом роботи з інструментом. Завдяки цьому AI-агент може не лише аналізувати існуючі макети, а й самостійно створювати нові дизайн-артефакти — фрейми, компоненти, дизайн-токени — безпосередньо на векторному полотні, працюючи з повноцінною дизайн-системою.

II. ДАНІ ТА МЕТОДИ

В роботі проведено дослідження та аналіз вітчизняних та зарубіжних ресурсів присвячених застосування мультимодальних великих мовних моделей у поєднанні з Model Context Protocol (MCP) для швидкого прототипування інтерфейсів користувача. Розглянуто pipeline із трьох MCP-інструментів — mobile-mcp для фіксації стану мобільного UI, agent-browser для аналізу веб-інтерфейсу та Pencil для AI-керованої генерації дизайну — оркестрованих AI-агентом Claude.

У межах емпіричного етапу дослідження здійснено перевірку ефективності запропонованих інструментальних засобів шляхом їх практичного впровадження у процес проєктування користувацького інтерфейсу існуючого кросплатформного програмного продукту. Об'єктом апробації виступав діючий програмний застосунок, що функціонує на декількох програмно-апаратних платформах, а предметом — методи та засоби підтримки розроблення каркасних моделей інтерфейсу (wireframes) і формування цілісної дизайн-системи. Апробація передбачала поетапне застосування запропонованих інструментальних рішень:

1. структуризацію функціональних вимог і сценаріїв взаємодії користувача;
2. розроблення каркасних моделей інтерфейсу з урахуванням принципів модульності та повторного використання компонентів;
3. формалізацію візуально-стильових і компонентних рішень у вигляді систематизованої дизайн-системи, що включає набір UI-компонентів, патернів взаємодії, типографічних і колірних токенів;
4. інтеграцію сформованої дизайн-системи у процес подальшої розробки інтерфейсів.

Оцінювання результативності здійснювалося за сукупністю критеріїв, зокрема: узгодженість інтерфейсних рішень між платформами, рівень повторного використання компонентів, зниження трудомісткості внесення змін, а також відповідність принципам масштабованості та підтримуваності. Отримані результати дозволили підтвердити практичну придатність запропонованих інструментальних засобів і їх доцільність для застосування в умовах розроблення та еволюційного розвитку кросплатформних програмних систем.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У даній роботі запропоновано трьохетапний підхід до прототипування UI із використанням екосистеми MCP-серверів, оркестрованих AI-агентом Claude Code. Об'єктом експерименту став існуючий крос-платформний мобільний застосунок для моніторингу діабету 1 типу, побудований на React Native.

Перший етап — повністю автономна фіксація поточного стану інтерфейсу існуючого застосунку. AI-агент самостійно, без участі людини, використовує два MCP-сервери: mobile-mcp [4] для взаємодії з мобільним пристроєм (отримання знімків екранів та дерева доступності через нативні інтерфейси Android/iOS) та agent-browser [5] для аналізу веб-версії застосунку. Агент автономно обходить екрани, фіксує їхній стан та формує повний контекст існуючого інтерфейсу.

Другий етап — автономна генерація початкових wireframes. AI-агент, маючи зібраний контекст, самостійно використовує MCP-сервер Pencil [6] для створення wireframe-екранів. Через операцію «batch_design» агент створює структуровані фрейми з компонентами, макетами та стилями, працюючи безпосередньо з дизайн-системою інструменту.

Третій етап — ітеративне оновлення дизайну. Через вбудований AI-чат Pencil з моделлю Claude Opus було надано текстовий запит для створення покращеної дизайн-системи. AI-агент автономно оновив дизайн-токени, створив нові компоненти, перебудував мобільні екрани та створив планшетні й десктопні варіанти.

На перших двох етапах AI-агент працював повністю автономно, без втручання людини. На першому етапі він самостійно обходив застосунок через mobile-mcp та agent-browser, створюючи знімки всіх екранів та збираючи дерево доступності з семантичною інформацією про елементи UI. На другому етапі агент через Pencil MCP автономно згенерував початкові wireframes для всіх основних екранів (Рисунок 1), працюючи зі структурованим JSON-форматом .pen файлів. Повна автономність агента на цих етапах значно пришвидшила процес отримання початкового прототипу.

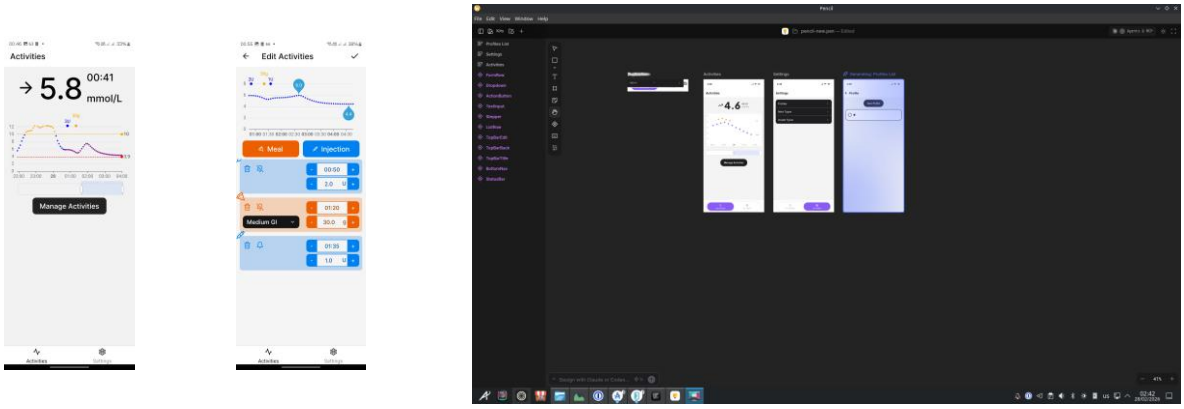


Рисунок 1. *Існуючий застосунок (ліворуч) та згенеровані wireframes у Pencil (праворуч)*

На третьому етапі AI-агент виконав повний редизайн, автономно пройшовши шість фаз: оновлення дизайн-токенів, оновлення стилів існуючих компонентів, створення 7 нових компонентів, перебудову 10 мобільних екранів, створення 10 планшетних та 10 десктопних екранів, і фінальне оновлення дизайн-системи (Рисунок 2). Загальний час генерації склав менше 30 хвилин.

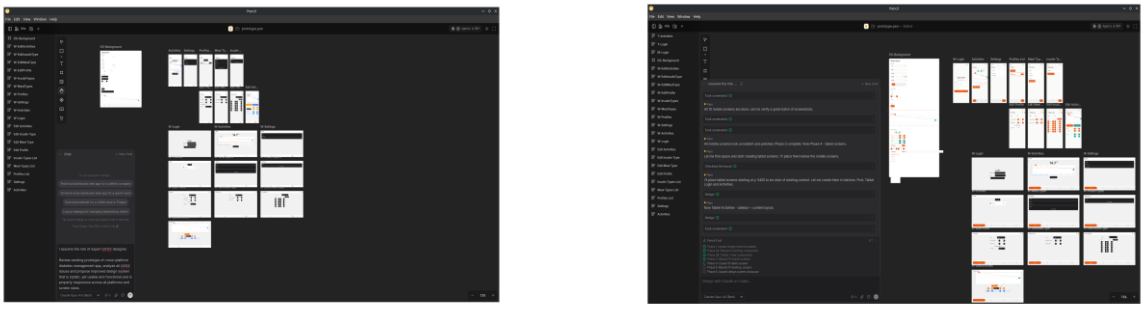


Рисунок 2. *Огляд wireframe-екранів (ліворуч) та процес автономного редизайну (праворуч)*

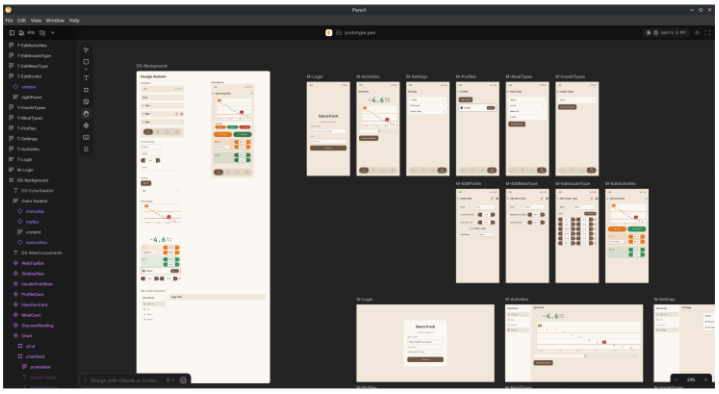


Рисунок 3. *Фінальний дизайн із дизайн-системою та адаптивними екранами*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонований підхід має кілька переваг порівняно з традиційними методами AI-генерації UI. По-перше, AI працює зі структурованими артефактами (JSON), а не інтерпретує растрові зображення, що забезпечує точність та відтворюваність. По-друге, екосистема MCP-серверів дозволяє з'єднувати різнорідні інструменти в єдиний автоматизований pipeline. По-третє, .pen файли зберігаються у Git-репозиторії поряд із кодом, забезпечуючи версіонування дизайну. Більше того, завдяки тому ж MCP, готовий макет може бути безпосередньо імплементований AI-агентом у коді застосунку, замикаючи цикл від дизайну до реалізації.

Серед обмежень — залежність якості від формулювання текстових запитів, можливі візуальні артефакти та обмежений вибір MCP-сумісних дизайн-інструментів. Згенерований дизайн потребує подальшого ручного коригування та професійної доробки. На даному етапі ці інструменти не можуть замінити людину, проте вони стануть чудовим доповненням для пришвидшення рутинних трудомістких задач прототипування. Водночас MCP вже прийнятий OpenAI, Google DeepMind та переданий до Linux Foundation, що свідчить про його становлення як універсального стандарту інтеграції AI-агентів із зовнішніми інструментами.

ДЖЕРЕЛА

1. Park S., Song Y., Lee S., Kim J., Seo J. (2025) Leveraging Multimodal LLM for Inspirational User Interface Search. Proceedings of the CHI Conference on Human Factors in Computing Systems. DOI: 10.1145/3706598.3714213.
2. Yuan M. et al. (2025) Towards Human-AI Synergy in UI Design: Supporting Iterative Generation with LLMs. ACM Transactions on Computer-Human Interaction. DOI: 10.1145/3773035.
3. Anthropic (2024) Model Context Protocol. URL: https://modelcontextprotocol.io/
4. mobile-next (2025) Mobile MCP: Mobile Device Automation via MCP. URL: https://github.com/mobile-next/mobile-mcp
5. Vercel Labs (2025) Agent Browser: Browser Automation CLI for AI Agents. URL: https://github.com/vercel-labs/agent-browser
6. Pencil (2026) Pencil — Design on Canvas, Land in Code. URL: https://pencil.dev/



ЮРІЙ ПОЛІЩУК
здобувач ступеня доктора філософії, за спеціальністю F3 Комп'ютерні науки, кафедри Інформаційних технологій, штучного інтелекту і кібербезпеки Національного університету харчових технологій, Київ, Україна.
ORCID: 0009-0008-2654-1637
E-mail: yuriipolishchuk1@gmail.com
Наукові інтереси — крос-платформна розробка мобільних застосунків, математичне моделювання біологічних процесів, штучний інтелект.



СЕРГІЙ ГРИБКОВ
д.т.н, професор, зав. кафедри Інформаційних технологій, штучного інтелекту і кібербезпеки Національного університету харчових технологій, Київ, Україна.
ORCID: 0000-0002-2552-2839
E-mail: sergio_nuft@nuft.edu.ua
У 2021 році захистив докторську дисертацію в Інституту проблем математичних машин і систем НАН України на тему «Інформаційні технології прийняття рішень на основі модифікованих евристичних і еволюційних методів та алгоритмів для харчових підприємств». У 2023 році отримав звання професора кафедри інформаційних технологій, штучного інтелекту і кібербезпеки Національного університету харчових технологій.
Наукові інтереси — розробка систем підтримки прийняття рішень, мови програмування, розробка баз та сховищ даних, інтелектуальний аналіз даних, методи оптимізації системи.

МАСШТАБОВАНІ AGILE-ФРЕЙМВОРКИ ЯК ІНСТРУМЕНТ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ В УМОВАХ ВІЙНИ В УКРАЇНІ

Олена Фендьо, Микола Пирог

Анотація. *У роботі досліджено можливості застосування масштабованих Agile-фреймворків (LeSS, Nexus, SAFe) в управлінні проєктами українських ІТ-компаній у кризових умовах війни. Визначено, що сучасний бізнес працює у складних умовах, які характеризується постійними змінами зовнішнього і внутрішнього середовища, а також зростанням вимог до результатів проєктної діяльності. Збільшення кількості і складності проєктів, підвищення вимог до їх результатів зумовлює необхідність використання інноваційних підходів до управління. У цьому контексті масштабовані Agile-фреймворки розглядаються як інструмент підвищення гнучкості, прозорості та стійкості організаційних процесів.*

Ключові слова: ІТ-проєкти, Agile, Large-Scale Scrum (LeSS), Nexus, Scaled Agile Framework (SAFe).

I. ВСТУП

Повномасштабна війна в Україні створила безпрецедентні виклики для бізнесу: перебої в енергопостачанні, мобілізація працівників, релокація виробництв, зниження внутрішнього споживання. В ІТ-сфері, окрім іншого, має місце вимушене переведення діяльності в онлайн формат, робота з розподіленими командами. Попри це, більшість компаній демонструють високий рівень стійкості та адаптивності. За таких умов особливо актуальним стає використання масштабованих Agile методологій управління проєктами (фреймворки LeSS, Nexus, SAFe), які дозволяють координувати роботу великих команд, забезпечувати прозорість комунікацій між командами та швидко реагувати на зміни.

II. ДАНІ ТА МЕТОДИ

В якості даних використано результати опитування українських підприємств (2025 р.), яке проводила ГО «Інститут економічних досліджень та політичних консультацій» за підтримки Міжнародного фонду «Відродження» [1].

Зокрема, 44-й випуск щомісячного опитування «Український бізнес під час війни» репрезентував результати відповідей 485-ти суб'єктів підприємницької діяльності, яке відображає сучасний стан бізнесу в Україні. Визначено, що станом на грудень 2025 р. 76% компаній працюють у повному обсязі, але під впливом таких негативних факторів, як обмеження через повітряні тривоги (45%), відключення електро- то теплопостачання, кадрові втрати внаслідок призову або виїзду співробітників (62%), вимушене переведення діяльності в онлайн-формат (40%) [1]. Додатково враховано дані економічних досліджень Інституту економічних досліджень та політичних консультацій (2025 р.), які аналізують вплив війни на економічну активність [2].

Методи дослідження: порівняльний аналіз сучасних практик управління ІТ-проєктами, зокрема масштабованих Agile-фреймворків, у кризових умовах в Україні.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У грудні 2025 р. темпи відновлення ділової активності в Україні перервали тенденцію до сповільнення, а значення індексу відновлення ділової активності (Рисунок 1), хоча й незначним чином, проте збільшилось із нуля до 0,03.

У відсотковому розподілі частка тих, у кого ситуація погіршилась, суттєво не змінилась у порівнянні з попередніми роками, і в грудні 2025 р. становить 17,4% (була 17,5%). Водночас, збільшилась частка тих, у кого ситуація стала кращою, ніж була рік тому, (із 17,7% до 20,2%) [1, с. 11].

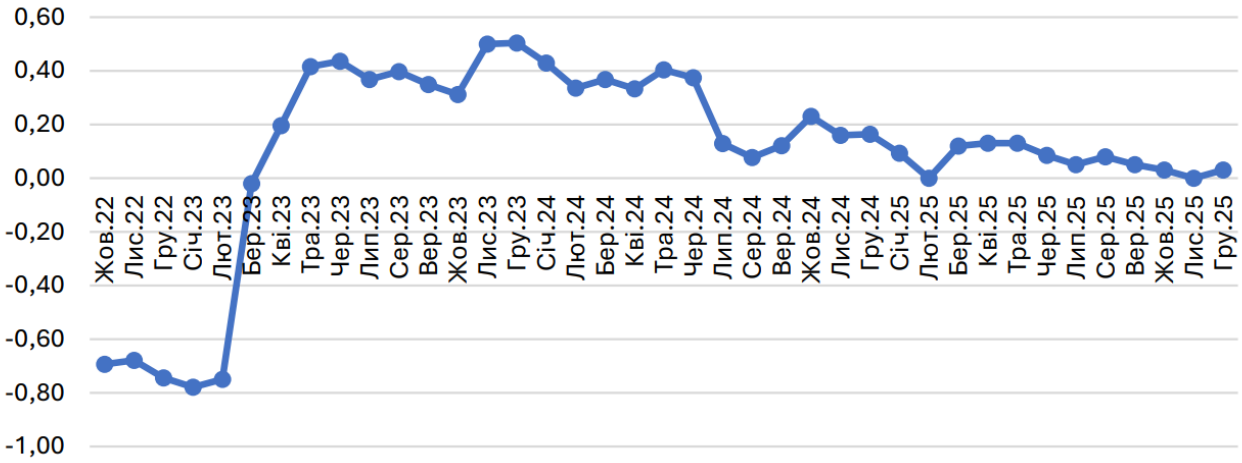


Рисунок 1. *Індекс відновлення ділової активності в Україні з 2022 по 2025 рр. [1, с. 11]*

Індекс поточної фінансово-економічної ситуації в Україні у грудні 2025 р. становив 0,03 (був 0,02 в листопаді та жовтні). У відсотковому розподілі істотних змін не відбулось. Частка тих, хто позитивно оцінює фінансово-економічну ситуацію на підприємстві, становила 11,8% (була 10,4%). Частка опитаних, що дають негативні оцінки, також суттєво не змінилась та становить 12,7% (була 12,6%) [1, с. 11-12].

За такої складної фінансово-економічної ситуації в Україні, коли планування та реалізація ІТ-проєктів стають більш масштабними та непрогнозованими, компанії постійно досліджують та вивчають фреймворки, які забезпечать початкову бізнес-цінність програмного продукту, збережуть час і витрати, а також знизять ризики доставки готового інкременту. У поєднанні зі швидкими змінами в технологіях та ринковими інноваціями, популярність та явна перевага масштабованих Agile-фреймворків стають очевидними.

На сьогодні існує низка Agile фреймворків, які добре себе зарекомендували для створення програмного забезпечення (далі – ПЗ), зокрема Scrum, Kanban, eXtreme Programming (XP), оскільки вони чітко зосереджені на адаптивності до змін та ітеративному створенні ПЗ для замовника. Проте, найбільшим їх обмеженням є використання для команд невеликого розміру (команди розміром 7±2 особи) і застосовувати їх у масштабах великої компанії з десятками ІТ-команд складно і нераціонально.

На відміну від них, масштабовані Agile фреймворки (LeSS, Nexus, SAFe) дозволяють вирішити ці проблеми і забезпечити гнучкість у розробленні ІТ-проєктів у масштабі, адже вони встановлюють рекомендації, методи, процеси, ролі та артефакти, які забезпечують скоординованість та легкість управління роботою сотень та тисяч ІТ-фахівців, розташованих у різних географічних регіонах.

Разом з тим необхідно зазначити, що перед початком впровадження масштабованих Agile-фреймворків ІТ-компаніям необхідно врахувати низку ключових факторів масштабування: розмір компанії та її організаційна структура; система управління та рівень зрілості процесів; корпоративна культура та дисципліна; технічний ландшафт та ступінь його гнучкості; рівень розподілу ролей у компанії; як бізнес оцінює створювану цінність [3].

З огляду на вищезазначене, проведемо порівняльний аналіз фреймворків LeSS, Nexus та SAFe за низкою визначених критеріїв.

Такий аналіз дозволить не лише ідентифікувати сильні та слабкі сторони кожного з фреймворків, але й співставити їх із потребами та особливостями управління великими за обсягом ІТ-проєктами (Таблиця 1).

Таблиця 1. *Порівняння масштабованих Agile-фреймворків*

Критерій	**LeSS** [3]		**Nexus** [4]	**SAFe** [5]
	Basic LeSS	**LeSS Huge**		
Масштаб ІТ-проєкту	• Великі і середні проєкти із залученням від 10 до 6000 розробників і більше	• Масштабні проєкти із залученням до 100 розробників	• Для проєктів корпоративного рівня, що охоплюють сотні команд	•
Ядро фреймворку	• один Product Owner, • один Scrum Master для 1-3 команд; • команди LeSS	• один Product Owner; • Scrum Master; • координаційні механізми для багатьох LeSS команд	• один Product Owner; • Scrum Master; • однин або кілька членів від кожної scrum-команди	• один Product Owner, • один Scrum Master для 2-3 команд; • ScrumXP команда; • Program Increment Planning
Кількість scrum-команд	від 2 до 8 команд	більше 8 команд	від 3 до 9 команд, що спільно працюють над досягнення Product Goal	десятки команд, організованих у Agile Release Trains (ART)
Кількість розробників у scrum-команді	від 10 до 50 розробників	від 50 до 6000 розробників і більше	5-9 розробників	5-9 розробників у кожній команді
Артефакти	• один Product Backlog; • окремий Sprint Backlog для кожної команди; • один потенційно відвантажений Increment	• масштабований Product Backlog; • багаторівневі Sprint Backlogs; • інтегрований Increment	• один загальний Product Backlog, який використо-вують усі команди; • Nexus Sprint Backlog; • Integrated Increment	• Portfolio Backlog; • Program Backlog; • Team Backlog; • Solution Increment
Події	• Sprint Planning; • Daily Scrum; • Sprint Review Sprint; • Retrospective	• багаторівневе Sprint Planning; • багатокомандні Review та Retrospective	• Sprint; • Nexus Sprint Planning; • Nexus Daily Scrum; • Nexus Sprint Review; • Nexus Sprint Retrospective	• Iteration Planning; • Daily Stand-up; • System Demo; • Inspect & Adapt
Масштабованість	Висока	Дуже висока	Помірна	Низька – середня (залежно від контексту)
Пристосування до змін	Помірне	Помірне	Низьке	Високе
Технічна складність	Помірна	Висока	Помірна	Низька
Географічна розподіле-ність	Помірна	Висока	Помірна	Помірна

Дана Таблиця 1 є лише невеликою складовою порівняльного аналізу масштабованих Agile-фреймворків, які можуть використовуватись ІТ-компаніями для розроблення ПЗ.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

В умовах війни масштабовані Agile-фреймворки стають не лише інструментом управління проєктами, а й засобом підтримки організаційної стійкості компаній. Їх застосування дозволяє бізнесу зберігати конкурентоспроможність, швидко адаптуватися до змін та підтримувати командну взаємодію. Фреймворки LeSS та Nexus забезпечують прозорість комунікацій між командами, що критично важливо при втраті частини персоналу через мобілізацію. Використання SAFe дозволяє інтегрувати стратегічне планування з оперативними діями, що підвищує стійкість бізнесу. Перспективним напрямом є інтеграція цифрових технологій управління IT-проєктами з Agile методологіями, що може стати основою для післявоєнної відбудови та розвитку українського бізнесу.

ДЖЕРЕЛА

1. Institute for Economic Research and Policy Consulting (2025) Ukrainian business during the war. Monthly enterprise survey. Issue 44, December 2025, 54 p. URL: http://www.ier.com.ua/files/Projects/2025/NRES/2025_NRES_December_UKR_FINAL_.pdf.
2. European Business Association (2026) Four years of full-scale war: How business operates in Ukraine. URL: https://eba.com.ua/chotyry-roky-velykoyi-vijny-yak-pratsyuye-biznes-v-ukrayini/.
3. Almeida, F. and Espinheira, E. (2021) Large-Scale Agile Frameworks: A Comparative Review. Journal of Applied Sciences, Management and Engineering Technology, 2(1), 14–27.
4. Scrum.org (2021) Nexus Guide: The official guide to scaling Scrum with Nexus. URL: https://www.scrum.org/resources/nexus-guide
5. Yeman, R.J. and Malaiya, Y.K. (2023) Comparison of Agile Scaling Frameworks. In: Proceedings of the International Conference on Information Systems Security (ICISS 2023), 11–13 August 2023, 51–57.



ОЛЕНА ФЕНДЬО
к.т.н., доцент кафедри прикладних інформаційних систем факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-9197-6399
E-mail: olena1.fendyo@knu.ua
У 2003 році закінчила магістратуру факультету комп'ютерних технологій ТДТУ імені Івана Пулюя за спеціальністю «Комп'ютерно-інтегровані технологічні процеси і виробництва». У 2011 році захистила дисертацію за спеціальністю 05.05.17. У 2022 році присвоєно вчене звання доцента кафедри технологій управління. Науково-педагогічний стаж роботи – 13 років. Автор понад 50 публікацій у вітчизняних і закордонних фахових виданнях. Коло наукових інтересів: інформаційні технології, управління проєктами.



МИКОЛА ПИРОГ
асистент кафедри прикладних інформаційних систем факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-2588-6066
E-mail: m.pyroh@knu.ua
Закінчив Приватний вищий навчальний заклад «Європейський університет» за спеціальністю «Інформаційні управляючі системи та технології». Сферою наукової діяльності є дослідження питання ІКТ в освіті, впровадження гнучких методологій в освітній процес.

Section

Network and Internet Technology

Секція

Мережеві та інтернет-технології

TIME-WEIGHTED PAGERANK FOR MEASURING STRUCTURAL EMBEDDEDNESS IN LARGE-SCALE BIBLIOGRAPHIC COUPLING NETWORKS

Zhanel Rymkhanova

Abstract. *Evaluating structural embeddedness in scholarly networks is hindered by temporal bias inherent in growing scientific systems. Traditional PageRank-based centrality measures systematically favor older publications, thereby underestimating recently influential work. This study proposes a Time-Weighted PageRank (TWPR) framework for large-scale bibliographic coupling networks and extends it with citation velocity normalization (TWPR-CI). Using 159,847 publications from OpenAlex (2010–2025), we compare PR, TWPR, and TWPR-CI at work and author levels. Results reveal moderate overlap between PR and TWPR-CI and demonstrate systematic elevation of recent high-impact publications, confirming that temporal weighting significantly alters structural embeddedness assessment.*

Keywords: PageRank; bibliographic coupling; structural embeddedness; citation velocity; network centrality; bibliometrics.

I. INTRODUCTION

Assessing scientific impact and centrality remains a central challenge in scientometrics. Traditional citation-based metrics, including total citation counts and the h-index, have long dominated this field. However, these approaches inadequately capture temporal dynamics of scientific influence and changes in centrality indicators. Recent studies have begun incorporating temporal dynamics through time-oriented citation metrics; however, most approaches treat time as an external adjustment factor rather than an internal component of the network structure.

Time-weighted centrality has been primarily validated in citation networks, where directionality and influence propagation are intrinsic structural properties [1, 2]. However, coupling networks lack directionality and instead encode intellectual similarity, which fundamentally alters the interpretation of centrality scores. To the best of our knowledge, time-weighted centrality has not been systematically evaluated in large-scale bibliographic coupling networks. PageRank estimates are important for evaluating collaboration among researchers and for the formation of scientific communities [5, 6, 7]. The aim of this study is to investigate how incorporating temporal decay and citation velocity dynamics changes the assessment of structural embeddedness in bibliographic coupling networks, and to determine whether time-weighted modifications of PageRank reflect a distinct structural dimension compared to the classical approach. The specific objectives are: (1) to construct a large-scale bibliographic coupling network based on OpenAlex publications (2010–2025) using link filtering procedures; (2) to implement and compute three centrality measures — classical PageRank (PR), Time-Weighted PageRank (TWPR), and Time-Weighted PageRank with Citation Intensity (TWPR-CI); and (3) to quantitatively evaluate the structural correspondence between PR, TWPR, and TWPR-CI across research clusters. This study makes three distinct contributions. First, it extends time-weighted centrality modeling to undirected bibliographic coupling networks, where centrality reflects structural embeddedness rather than prestige. Second, it introduces a hybrid formulation integrating temporal decay and citation velocity into a unified structural framework. Third, it empirically demonstrates that temporal weighting reconfigures thematic network cores in large-scale scholarly systems.

II. DATA AND METHODS

Let G = (P, E, W) be an undirected weighted bibliographic coupling network, where P represents scientific publications, E is the set of coupling edges, and w_{ij} denotes the number of shared references between publications i and j. To incorporate temporal dynamics, we define a time-weighted adjacency matrix with elements w_{ij}:

$$w_{ij} = w_{ij} \cdot e^{-\lambda(T-max(t_j,t_i))} , \quad (1)$$

where T is the reference year (e.g., 2025), y_i is the publication year of node i, and λ is the temporal decay parameter. The selected decay parameter λ = 0.15 corresponds to an approximate half-life of scholarly relevance of 4.6 years, aligning with observed citation aging patterns in dynamic research domains [4]. The TWPR is then defined as the stationary distribution of a random walk on the time-weighted network:

$$r = \alpha \cdot \hat{0}^b \cdot r + (1-\alpha) \cdot v , \quad (2)$$

where r is the ranking vector, α is the damping factor (α = 0.85), $\hat{O}^b$ is the normalized transition matrix derived from the time-weighted adjacency matrix A^b, and v is the teleportation vector. The transition matrix is row-stochastic after normalization by node strength, ensuring convergence of the iterative ranking process [3]. Convergence was achieved when the L1-norm difference between successive rank vectors fell below 10^{-6}, typically within 40–50 iterations. To integrate citation velocity, the TWPR score is multiplied by the ratio c_i / ē_y, where c_i is the citation count of publication i and ē_y is the average citation count for publications from the same year, yielding the TWPR-CI score [1, 2].

Data were collected from OpenAlex [8] and our sampling strategy targeted 10,000 articles per year from 2010 through 2025, yielding 160,000 publications total. We restricted sampling to works classified as ‘article’ type, excluding conference papers, reviews, and books to maintain consistency in citation practices. The final preprocessed dataset contained 159,847 works with complete metadata, 2,354,309 citation edges, and 646,515 authorships linking to 509,676 unique authors and 29,134 institutions. Distribution by publication year closely approximated the target of 10,000 per year, with 99.89% of citations pointing outside the sampled dataset. Bibliographic coupling networks were constructed using a shared-reference approach. For each cited work, all citing works within the dataset were identified and pairwise connections generated between them. After filtering, the network contained 159,847 nodes and 88,708 edges, exhibiting clear community structure with modularity 0.73 and mean degree 23.1.

III. RESULTS AND ANALYSIS

The coupling network evolution across temporal snapshots reveals progressive growth in both nodes and edges. Average degree increased from 0.06 in 2010 to 1.11 in 2025, demonstrating growing intellectual connectivity. The network’s modularity of 0.73 confirms strong community structure, validating the clustering approach for within-community metric comparisons.

As shown in Figure 1, correlation analysis at work level reveals complex relationships between metrics. PR and TWPR exhibit high positive correlation (r = 0.89), indicating substantial agreement in identifying influential publications, though with notable exceptions. PR and TWPR-CI show moderate correlation (r = 0.52), suggesting TWPR-CI captures different influence dimensions. TWPR and TWPR-CI demonstrate strong correlation (r = 0.84), expected given TWPR-CI’s multiplicative dependence on TWPR. Notably, CI shows weak correlation with

network-based metrics ($r < 0.3$), confirming that citation counts and network position measure distinct influence aspects.

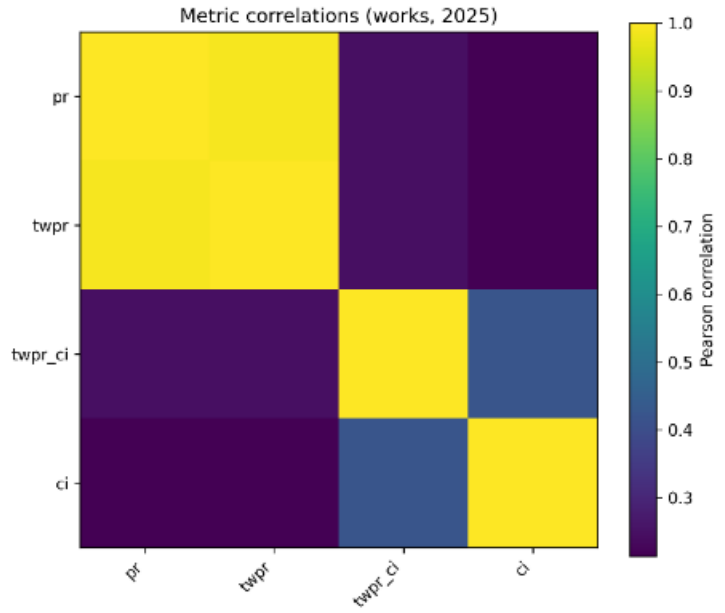


Figure 1. *Correlation analysis at publications level*

These patterns persist in author-level aggregations (Figure 2), with PR_sum and TWPR_sum highly correlated ($r = 0.91$) but TWPR-CI_sum showing greater independence ($r = 0.61$ with PR_sum). The correlation structure validates our multi-metric approach, demonstrating that time-weighted variants provide complementary rather than redundant information.

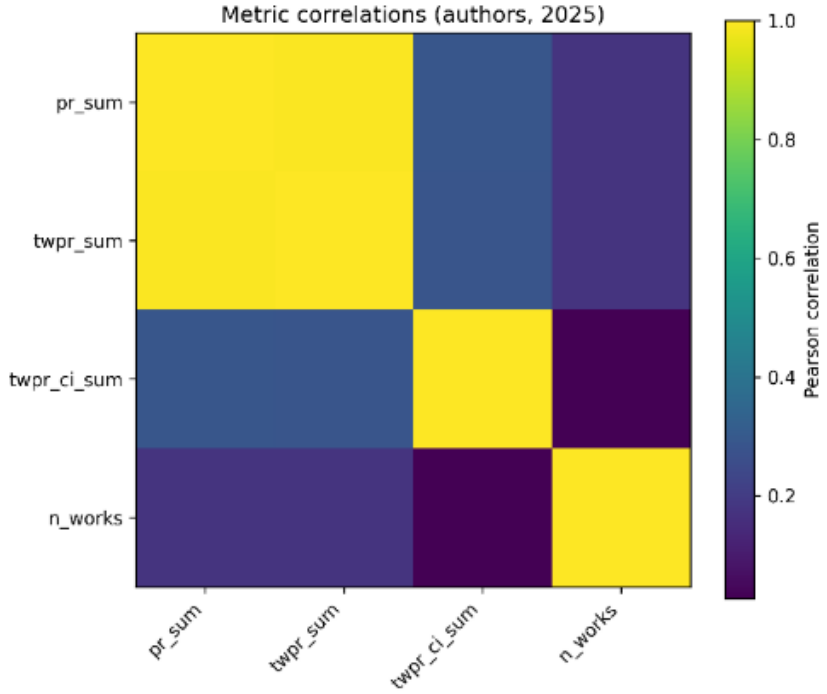


Figure 2. *Correlation analysis at authors' level*

Figure 3 displays histograms of overlap frequencies across clusters. The PR vs. TWPR distribution is concentrated in the 8–10 range, confirming minimal reordering. In contrast, PR vs.

TWPR-CI exhibits a wider distribution with a pronounced left tail, indicating the presence of clusters where the hybrid metric substantially reshapes the top-ranked publications. TWPR vs. TWPR-CI occupies an intermediate position.

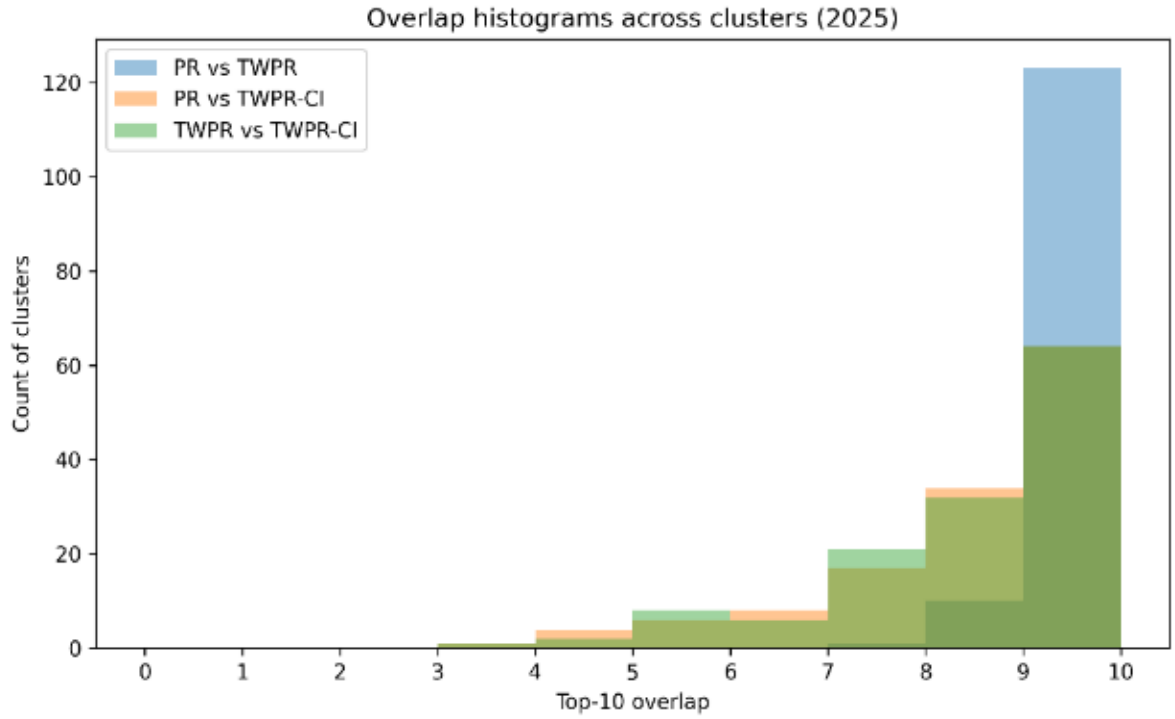


Figure 3. *Overlap histograms across clusters (2025)*

Rank-shift analysis between PR and TWPR-CI demonstrates substantial reordering across the full set of publications. Cluster-level case study analysis across three representative thematic communities further illustrates these findings. Cluster 0 (computer vision, n = 45) exhibits pronounced ranking divergence: the top-5 PR publications average publication year 2022.0 with mean citation count 48.2, whereas the top-5 TWPR-CI publications average year 2020.8 with substantially higher mean citations (266.4). This contrast illustrates that PR emphasizes current topological position within the research front, whereas TWPR-CI captures dynamic structural embeddedness by integrating temporal weighting with citation intensity. Cluster 2 (graphene materials, n = 34) displays substantially lower divergence. The PR top-5 and TWPR-CI top-5 share four out of five publications, with both groups centered around 2011–2012. This cluster represents a mature research domain in which foundational works retain both high structural centrality and sustained citation impact. Cluster 1 (microbiome analysis, n = 34) demonstrates moderate divergence: TWPR-CI slightly favors recent publications exhibiting higher citation velocity, suggesting that dynamic thematic integration plays a stronger role than cumulative legacy positioning in this rapidly evolving field.

IV. DISCUSSION AND CONCLUSION

This study demonstrates that temporal weighting systematically reconfigures the assessment of structural embeddedness in bibliographic coupling networks. The moderate overlap between traditional PageRank and TWPR-CI rankings (mean 6.2/10 within clusters) indicates that these metrics capture partially distinct structural dimensions rather than redundant information. The divergence observed is not stochastic variation but reflects differences between cumulative structural integration captured by PR and dynamic structural embeddedness captured by TWPR-CI,

which incorporates temporal proximity and citation velocity. The asymmetric rank-shift patterns further confirm this structural differentiation. TWPR-CI systematically elevates publications exhibiting strong current thematic integration and sustained citation intensity, particularly in rapidly evolving research fronts. Cluster-level analysis shows that this divergence is context-dependent: mature domains with stable foundational literature demonstrate high structural alignment between metrics, whereas emerging or methodologically dynamic fields display stronger reordering effects.

In conclusion, time-weighted PageRank variants reveal a dual nature of embeddedness in thematic scholarly networks: classical PageRank captures cumulative, historically consolidated integration, whereas TWPR-CI identifies dynamic structural embeddedness reflecting current thematic centrality and citation intensity. The obtained results support the inclusion of time-sensitive structural indicators in bibliometric analysis and research evaluation systems, where both historical consolidation and current intellectual integration are essential.

REFERENCES

1. A. Kuchanskyi, A. Biloshchytskyi, Y. Andrashko, S. Biloshchytska, and A. Faizullin, "The scientific productivity of collective subjects based on the time-weighted PageRank method with citation intensity," Publications, vol. 10, no. 4, Art. no. 40, 2022. doi: 10.3390/publications10040040
2. A. Biloshchytskyi, O. Kuchanskyi, A. Mukhatayev, Y. Andrashko, S. Toxanov, A. Faizullin, and K. Kassenov, "Application of time-weighted PageRank method with citation intensity for assessing the recent publication productivity and partners selection in R&D collaboration," Publications, vol. 12, no. 4, Art. no. 48, 2024. doi: 10.3390/publications12040048
3. X. B. Han, S. Wang, and C. Yu, "PageRank of gluing networks and corresponding Markov chains," Mathematics, vol. 13, no. 13, Art. no. 2080, 2025.
4. F. Hu et al., "The aging effect in evolving scientific citation networks," Scientometrics, vol. 126, pp. 4297–4309, 2021.
5. A. Biloshchytskyi, O. Kuchanskyi, Y. Andrashko, A. Mukhatayev, S. Toxanov, A. Faizullin, and N. Yurchenko, "Revealing the closeness of publication ties in scientific cooperation taking into account scientific productivity based on the time-weighted PageRank method with citation intensity," East.-Eur. J. Enterp. Technol., vol. 5, pp. 63–70, 2024. doi: 10.15587/1729-4061.2024.312884
6. H. Xu, A. Kuchansky, and M. Gladka, "Devising an individually oriented method for selection of scientific activity subjects for implementing scientific projects based on scientometric analysis," East.-Eur. J. Enterp. Technol., vol. 6, no. 3, pp. 93–100, 2021. doi: 10.15587/1729-4061.2021.248040
7. O. Kuchanskyi, Y. Andrashko, A. Biloshchytskyi, A. Mukhatayev, S. Biloshchytska, and F. Numanova, "Resilience of scientific collaboration networks in young universities based on bibliometric and network analysis," Data, vol. 10, no. 11, Art. no. 184, 2025. doi: 10.3390/data10110184
8. OpenAlex, "OpenAlex: An open catalog of the global research system." [Online]. Available: https://openalex.org



ZHANEL RYMKHANOVA
Master's student, School of AI & Data Science, Astana IT University, Astana, Kazakhstan
ORCID: 0009-0005-2929-449X
E-mail: 242774@astanait.edu.kz
Master's student in AI & Data Science at Astana IT University. Her research focuses on scientometric analysis, bibliographic coupling networks, and time-weighted centrality methods for evaluating structural embeddedness in scholarly networks.

INTEGRATED METHOD OF LOW-DETECTION REDUNDANCY MONITORING IN WIRELESS SENSOR NETWORKS

Mykhaylo Sharapov, Yurii Kravchenko, Andrii Sobchuk

Abstract. *Wireless sensor networks operating under sustained destabilizing influence require redundancy monitoring with minimal external observability. This paper proposes an integrated low-detection monitoring method that combines an SIR-type dynamic state model with pseudo-chaotic diagnostic execution. The SIR model serves as an internal estimator of redundancy sufficiency and enables event-driven diagnostic activation based on state-space analysis. Once triggered, diagnostics are embedded into pseudo-chaotic traffic patterns, significantly reducing detectability. The framework provides a mathematically grounded approach to covert redundancy monitoring while preserving informational completeness under resource and adversarial constraints.*

Keywords: Functional stability of wireless sensor networks; redundancy monitoring; low-detection diagnostics; covert monitoring; SIR model; pseudo-chaotic signals.

I. INTRODUCTION

Wireless sensor networks (WSNs) are increasingly deployed in environments characterized by sustained destabilizing influence, including hostile interference, partial node compromise, and resource-constrained operation. In such conditions, maintaining functional availability is inseparably linked to the timely detection of redundancy degradation. Classical diagnostic procedures, however, rely on the explicit probing, polling, or test traffic, which inevitably increases observability and may itself become a trigger for targeted disruption. Consequently, the problem of low-detectability redundancy monitoring emerges as a critical scientific and practical challenge for the resilient WSN operation. Existing research on WSN redundancy monitoring predominantly focuses on improving fault detection accuracy, reducing energy consumption, or optimizing diagnostic scheduling. Epidemic models, including SIR-type formulations, are typically used for descriptive analysis and forecasting of fault propagation and state evolution; however, despite the fact that SIR models have long transcended their epidemiological origins and are widely applied in technical and socio-technical systems, they are still rarely integrated into operational monitoring loops [1,2]. Conversely, covert or pseudo-chaotic communication methods are primarily studied as standalone concealment techniques, without being embedded into adaptive decision-making frameworks [3]. As a result, prior research lacks an integrated method that jointly determines when diagnostics should be activated and how they should be executed in a minimally detectable manner.

The purpose of this study is to develop and validate an integrated method for redundancy monitoring in WSNs that combines an SIR-based state model with pseudo-chaotic covert diagnostics. The method aims to minimize external observability of monitoring activity while preserving sufficient informational completeness for reliable redundancy assessment and ensuring efficient use of network resources through event-driven, state-dependent diagnostic activation.

II. DATA AND METHODS

The proposed method combines two complementary mechanisms with distinct functional roles. The first mechanism is an SIR-type model that describes the evolution of node states and provides a decision criterion for initiating diagnostics. The second mechanism is a pseudo-chaotic monitoring procedure that enables covert execution of diagnostics once activation is required. Their integration ensures that explicit diagnostic actions are both resource-conscious and masked within normal network dynamics.

Schematic representation of the cycle mechanisms interaction is provided by Figure 1.

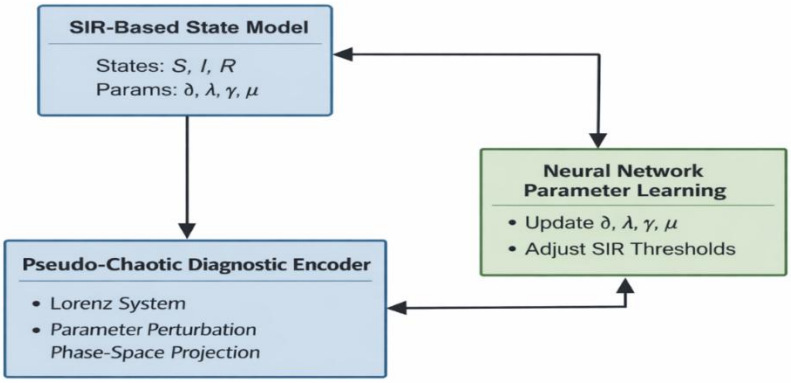


Figure 1. *Schematic representation of the interaction between the method's mechanisms*

In the adopted SIR formulation, nodes of the WSN are classified into three abstract states: operational (S), degraded or at-risk (I), and functionally lost (R). Transitions between these states are governed by parameters reflecting failure rates, recovery or compensation effects, and redundancy exhaustion. Unlike classical epidemic interpretations, the SIR model here serves as an internal estimator of redundancy sufficiency rather than a literal failure spread description.

The SIR subsystem continuously evaluates the network state using observable and covertly collected indicators. The decision mechanism exploits phase-plane analysis of the SIR dynamics, monitoring the trajectory of the system in the S–I plane and its proximity to critical regions associated with accelerated degradation [4]. When the inferred state enters such a region or when the proportion of nodes in the at-risk class exceeds a dynamically adjusted threshold, the model signals the necessity of executing explicit diagnostics. In this way, diagnostics are not periodic but event-driven, reducing unnecessary exposure and limiting predictability.

Once diagnostics are triggered, the monitoring traffic is embedded into pseudo-chaotic signal patterns generated by a deterministic chaotic system. These patterns are practically indistinguishable from background noise or benign traffic fluctuations for an external observer. The Lorenz system [5] is employed as a generator of such pseudo-chaotic trajectories, ensuring reproducibility at legitimate nodes while maintaining apparent randomness.

Diagnostic queries and responses are modulated onto chaotic trajectories through parameter perturbation and phase-space projection. Each node responds with a fragment of diagnostic information mapped onto the chaotic signal, avoiding explicit diagnostic packets. This significantly lowers the probability of detection and classification by adversarial monitoring systems.

Due to asynchronous node operation and energy-aware scheduling, pseudo-chaotic responses arrive with non-uniform delays. The method explicitly accounts for these lags by introducing time-shifted interpretation windows in the reconstruction of diagnostic data. This prevents misclassification of delayed responses as node failures.

Collected pseudo-chaotic signals are aligned using lag compensation functions derived from network timing statistics. The reconstructed diagnostic state is then mapped back into redundancy metrics, such as effective node availability and redundancy margin. To adapt the SIR model to changing operational conditions, a neural network can be introduced as a parameter estimator. The network learns updated values of the transition parameters δ, λ, γ, and μ based on reconstructed diagnostic reports obtained through the pseudo-chaotic channel. The neural network operates in a closed feedback loop: diagnostic outcomes refine SIR parameters, and updated SIR dynamics adjust future diagnostic activation thresholds. This allows the system to adapt to evolving attack strategies, environmental changes, and aging effects without explicit reconfiguration. The complete operational cycle consists of continuous low-visibility observation, SIR-based risk evaluation, covert diagnostic activation, lag-aware data reconstruction, and adaptive parameter learning. Each cycle reinforces the system's ability to balance informational accuracy against detectability.

III. RESULTS AND ANALYSIS

Proposed method formalizes the use of an SIR-type dynamic model as an internal estimator of redundancy sufficiency in a wireless sensor network. Unlike classical reliability or epidemic interpretations, the SIR formulation is reinterpreted as a state-space abstraction that captures the balance between operational capacity, degradation processes, and irreversible loss. This formalization establishes explicit conditions under which diagnostic intervention is justified, thereby providing a mathematically grounded alternative to periodic or heuristic monitoring strategies. Second, we are proposing a framework for covert diagnostic execution based on pseudo-chaotic signal generation. The use of deterministic chaotic systems enables diagnostic information to be embedded into traffic patterns that are statistically consistent with normal network dynamics. This result demonstrates that diagnostic observability can be reduced without suppressing diagnostic functionality, provided that information encoding and decoding are synchronized through shared system dynamics.

A natural direction for further research concerns the practical realization and validation of adaptive feedback mechanisms within the proposed framework. In particular, the incorporation of neural network–based learning into the SIR–pseudo-chaotic diagnostic model represents a promising extension that has a promising potential to be fully explored [6]. Future work will focus on developing neural network architectures capable of learning and updating the SIR transition parameters δ, λ, γ, and μ using diagnostic information reconstructed from the pseudo-chaotic channel. Such learning would enable the monitoring system to adjust its internal state model in response to changing operational conditions, including evolving destabilizing influences, environmental variability, and long-term network aging effects.

Another important research task is the systematic evaluation of closed-loop stability and convergence when adaptive learning is introduced. The interaction between reconstructed diagnostic states, neural parameter updates, and SIR-based diagnostic activation thresholds requires formal analysis to ensure that adaptation improves monitoring accuracy without introducing oscillatory or unstable behaviour. Addressing these issues will be essential for transitioning the proposed framework from a conceptual and methodological contribution to a fully operational adaptive monitoring system.

IV. DISCUSSION AND CONCLUSION

The study presents an integrated method for low-detection redundancy monitoring in wireless sensor networks, combining SIR-based decision modelling with pseudo-chaotic covert diagnostics. The resulting mathematical framework provides a rigorous theoretical basis for selecting both the timing and the manner of recovery and diagnostic actions in wireless sensor networks operating under persistent destabilizing conditions. The proposed approach offers a consistent and extensible methodological foundation for low-detection redundancy monitoring, explicitly linking state estimation with covert execution mechanisms. The achieved formalizations and integration mechanisms meet the stated purpose of the study by enabling informed decisions on when to initiate recovery, how to perform it in a low-observability manner, and how to support adaptive model evolution within a single coherent framework.

ACKNOWLEDGMENT

The study was conducted within the framework of scientific research work No. 25BP064-01: Methods and means of intelligently ensuring the functional stability of the reconnaissance system and autonomous navigation of the combat line using UAVs.

REFERENCES

1. Ginters E., Eroles M. A. P., Matvejevs A. (2024) Usability of classic SIR and diffusion models for assessing malware spread in the early stages of infectious diseases. In 2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University, 1–8.
2. Teng Y., Wei W. (2024) Review on the application of the SIR model in predicting urban traffic congestion: Successes and future directions. In Proceedings of the 2024 5th International Conference on Urban Construction and Management Engineering (ICUCME 2024), 242, 4.
3. Zhai H., Paris B. P. (2022) Practical Methods for Joint Time and Carrier Synchronization in LPI/LPD Communications. In MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM), 431-436.
4. Wang J. (2021) Dynamics and bifurcation analysis of a state-dependent impulsive SIS model. Advances in Difference Equations, 287, 1–19, https://doi.org/10.1186/s13662-021-03436-3.
5. Pichkur V., Kapustyan O., Sobchuk V. (2023) Stability and attractors of evolutionary equations, https://www.researchgate.net/publication/375547080_Stability_and_Attractors_of_Evolutionary_Equations.
6. Grimm V., Heinlein A., Klawonn A., Lanser M., Weber J. (2021) Estimating the time-dependent contact rate of SIR and SEIR models in mathematical epidemiology using physics-informed neural networks. Electronic transactions on numerical analysis, 56. 1-27. 10.1553/etna_vol56s1.



MYKHAYLO SHARAPOV
Postgraduate student, Department of Information Systems and Technology, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0009-0007-8225-0677
E-mail: sharapovm@fit.knu.ua
Obtained a Specialist degree in Accounting and Auditing from the National Academy of Management in 1998 and a Bachelor's degree in Information Technologies from the National Aviation University in 2021. PhD student at Taras Shevchenko National University of Kyiv. Research interests include redundancy monitoring in wireless sensor networks.



YURII KRAVCHENKO
Professor, Head of the Networking and Internet Technologies Department, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0000-0002-0281-4396
E-mail: yurii.kravchenko@knu.ua
With more than 30 years of teaching and research experience, he has published over 200 scientific works, including 2 monographs, 11 textbooks and teaching manuals, and 35 articles in peer-reviewed Ukrainian journals. His h-index is 17 in Scopus and 18 in Google Scholar. He has supervised 5 Doctors of Sciences, 8 Candidates of Sciences, and 2 PhD holders.
Research interests include telecommunication systems, functional stability of complex systems, and artificial intelligence.



ANDRII SOBCHUK
Associate professor, Department of Cybernetic Security Systems and Technologies, State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-3250-3799
E-mail: anri.sobchuk@gmail.com
Obtained a PhD from Taras Shevchenko National University of Kyiv (Kyiv, Ukraine) in 2020. Author of more than 50 scientific publications. Research interests include functional stability of complex technical systems, protection of enterprise information resources, computer networks, and industrial informatics.

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ IOT-ПРИСТРОЇВ

Олексій Бичков, Володимир Петрівський, Денис Штома

Анотація. *У роботі проведено порівняльний аналіз методів машинного навчання для виявлення аномалій у мережевому трафіку пристроїв Інтернету речей. На наборі даних IoT-23 досліджено ефективність алгоритмів Random Forest, Isolation Forest та автоенкодера. Результати демонструють, що Random Forest забезпечує найвищу точність (99,2%), тоді як автоенкодер є перспективним для виявлення невідомих атак без розмічених даних.*

Ключові слова: машинне навчання, Інтернет речей, виявлення аномалій, мережевий трафік, кібербезпека.

I. ВСТУП

На сьогоднішній день, стрімке поширення пристроїв Інтернету речей (далі – IoT) створює нові виклики для кібербезпеки. За даними IoT Analytics, кількість підключених IoT-пристроїв у 2024 році досягла 18,8 мільярда, а до 2030 року прогнозується зростання до 40 мільярдів [1]. Така експоненційна динаміка обумовлена активною цифровізацією промисловості, розвитком концепції Industry 4.0, впровадженням «розумних» міст, систем енергоменеджменту, телемедицини та побутових IoT-рішень.

Водночас більшість IoT-пристроїв характеризуються обмеженими обчислювальними ресурсами, низьким обсягом пам’яті, енергозалежністю та спрощеними операційними системами. Це нівелює впровадження традиційних засобів кіберзахисту, зокрема складних криптографічних протоколів, багаторівневих IDS/IPS або постійного сигнатурного оновлення антивірусних баз.

Загрози для IoT-мереж також демонструють зростальну тенденцію. За звітом SonicWall 2025, кількість атак шкідливого програмного забезпечення на IoT-пристрої збільшилась на 124% протягом року [2].

Основними векторами атак залишаються ботнети, експлуатація відкритих портів, слабка автентифікація та вразливості прошивок. У цьому контексті класичні сигнатурні методи виявлення виявляються недостатньо ефективними, оскільки не здатні оперативно реагувати на нові або модифіковані типи атак. Альтернативою виступають підходи на основі машинного навчання (далі – МН), які дозволяють виявляти аномальні патерни поведінки мережевого трафіку без необхідності постійного оновлення сигнатурних баз [3].

Метою даного дослідження є проведення порівняльного аналізу ефективності алгоритмів Random Forest, Isolation Forest та автоенкодера на реальному наборі даних IoT-трафіку.

II. ДАНІ ТА МЕТОДИ

У межах даного дослідження було використано набір даних IoT-23, створений лабораторією Stratosphere Research Lab Чеського технічного університету в Празі [4]. Датасет містить понад 325 млн записів мережевих з’єднань (Zeek/Bro flows), зібраних у 23 сценаріях, серед яких 20 сценаріїв відображають активність реального шкідливого програмного забезпечення (Mirai, Torii, Gagfyt, Okiru та ін.), а 3 – легітимний трафік пристроїв Philips HUE, Amazon Echo та Somfy Smart Door Lock. Кожен запис містить 21 ознаку, що описує характеристики мережевого з’єднання: тривалість, кількість переданих байтів, протокол, напрямок трафіку, кількість пакетів тощо.

Перед навчанням моделей було здійснено попередню обробку даних, що включала очищення від пропусків, кодування категоріальних ознак, нормалізацію числових параметрів та балансування вибірки. Дані поділено на навчальну (70%) та тестову (30%) вибірки. Для можливості забезпечення коректності порівняння моделей було застосовано однакові критерії оцінювання: Accuracy, Precision, Recall та F1-міру. Автоенкодер навчався виключно на нормальному трафіку, що відповідає концепції напівконтрольованого навчання для виявлення аномалій.

Застосовано три підходи.

По-перше, Random Forest (далі – RF) – ансамблевий метод класифікації, що формує сукупність рішень на основі множини дерев рішень і забезпечує високу узагальнювальну здатність [3].

По-друге, Isolation Forest (далі – IF) – алгоритм, орієнтований на ізоляцію аномальних спостережень шляхом випадкового розбиття простору ознак.

По-третє, автоенкодер (далі – AE) – нейромережева модель, що стискає вхідні дані у латентне представлення та відтворює їх; аномалії визначаються за перевищенням порогового значення помилки реконструкції [5].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Як показано в Таблиці 1 – RF продемонстрував найкращі результати з точністю 99,2%, а також найвищі значення Precision (0,988), Recall (0,991) та F1-міри (0,989). Це вказує не лише про загальну високу коректність класифікації, але й про збалансованість моделі щодо мінімізації як хибнопозитивних, так і хибнонегативних спрацювань.

Таблиця 1. *Порівняння методів виявлення аномалій на IoT-23*

Метод	Accuracy	Precision	Recall	F1
Random Forest	0,992	0,988	0,991	0,989
Isolation Forest	0,951	0,942	0,935	0,938
Автоенкодер	0,976	0,971	0,968	0,969

Отримані результати узгоджуються з висновками іншого дослідження, де було зафіксовано точність RF на рівні 99,16–100% на датасеті IoT-23 [6]. Висока ефективність RF пояснюється здатністю ансамблевих методів агрегувати рішення великої кількості дерев рішень, що дозволяє враховувати складні нелінійні взаємозв'язки між ознаками мережевого трафіку. Крім того, механізм випадкової підвибірки ознак і об'єктів зменшує ризик перенавчання та підвищує узагальнювальну здатність моделі при роботі з високорозмірними даними.

AE показав точність 97,6% (F1 = 0,969), що відповідає діапазону 95,8–99,3%, зафіксованому у дослідженні Bachar, Khiat та El Guemmat [7]. Хоча показники дещо поступаються RF, слід зауважити, що AE має вагому перевагу з точки зору застосування концепції виявлення аномалій. Оскільки модель навчається виключно на нормальному трафіку, вона формує латентне представлення типової поведінки системи. А тому будь-які суттєві відхилення, що призводять до зростання помилки реконструкції, інтерпретуються як потенційні аномалії.

Визначений підхід є особливо цінним в умовах появи нових або модифікованих типів атак, для яких відсутні попередньо розмічені приклади. Водночас ефективність автоенкодера значною мірою залежить від коректного вибору архітектури мережі, розміру латентного простору та порогового значення аномальності.

IF продемонстрував найнижчу точність 95,1% (F1 = 0,938), що підтверджує його чутливість до налаштування гіперпараметрів, зокрема кількості дерев та розміру підвибірки [6]. Алгоритм ґрунтується на припущенні, що аномалії легше ізолювати в просторі ознак шляхом випадкових розбиттів. Водночас, у випадку складних, багатовимірних і частково перекривних розподілів, характерних для IoT-трафіку, таке припущення не завжди реалізується належним чином. Незважаючи на це, IF залишається перспективним інструментом для попереднього скринінгу даних або використання у складі гібридних систем, де його швидкість та відсутність потреби в розмічених даних можуть компенсувати дещо нижчу точність.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати у даному дослідженні підтверджують високу ефективність методів машинного навчання для виявлення аномалій у мережевому трафіку IoT-пристроїв. Тим не менш, інтерпретація отриманих показників потребує врахування низки факторів.

По-перше, RF є алгоритмом контрольованого навчання, що потребує наявності якісно розмічених даних.

У реальних умовах експлуатації IoT-мереж процес формування повного та достовірного набору міток є складним і ресурсомістким. По-друге, датасет IoT-23, хоча й репрезентативний, не відображає повною мірою усю різноманітність сучасних IoT-середовищ.

AE має вагому перевагу – здатність виявляти нові, раніше невідомі типи атак без необхідності попереднього маркування шкідливого трафіку. Це особливо актуально в умовах швидкої еволюції ботнетів та експлойтів. Однак нейромережеві моделі потребують більшого обчислювального ресурсу, що обмежує їх використання безпосередньо на граничних (edge) пристроях.

Перспективним рішенням є перенесення складних обчислень на edge-шлюзи або використання оптимізованих легковагових архітектур.

IF, навіть не зважаючи на нижчі показники, залишається привабливим завдяки невисокій обчислювальній складності та можливості роботи без міток класів. Його доцільно використовувати як первинний фільтр або компонент гібридної системи.

Перспективним напрямом подальших досліджень є розроблення гібридних моделей (наприклад, AE+IF або RF+AE), які синтезують в собі переваги контрольованого й неконтрольованого навчання та здатні підвищити F1-міру до 0,98–0,99 [7].

Додатково актуальним є впровадження федеративного навчання, що дозволяє здійснювати розподілене тренування моделей без передачі сирих даних, підвищуючи рівень конфіденційності.

Таким чином, результати дослідження підтверджують доцільність застосування методів машинного навчання для забезпечення кібербезпеки IoT-мереж. Оптимальний вибір моделі залежить від наявності розмічених даних, обчислювальних ресурсів та вимог до здатності виявляти нові типи атак.

ДЖЕРЕЛА

1. IoT Analytics. (2024). State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. https://iot-analytics.com/number-connected-iot-devices/

2. SonicWall. (2025). 2025 SonicWall annual cyber threat report. https://www.sonicwall.com/threat-report/
3. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293
4. Garcia, S., Parmisano, A., & Erquiaga, M. J. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0). Zenodo. https://doi.org/10.5281/zenodo.4743746
5. Chatterjee, A., & Ahmed, B. S. (2022). IoT anomaly detection methods and applications: A survey. Internet of Things, 19, 100568. https://doi.org/10.1016/j.iot.2022.100568
6.Krzysztoń, E., Rojek, I., & Mikołajewski, D. (2024). A comparative analysis of anomaly detection methods in IoT networks. Applied Sciences, 14(24), 11545. https://doi.org/10.3390/app142411545
7. Bachar, A., Khiat, A., & El Guemmat, K. (2026). Enhancing anomaly detection in IoT networks using hybrid autoencoder and Isolation Forest. Engineering, Technology & Applied Science Research, 16(1), 31123–31129. https://doi.org/10.48084/etasr.15288



ОЛЕКСІЙ БИЧКОВ
Професор, завідувач кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка
E-mail: oleksiibychkov@knu.ua
ORCID: 0000-0002-9378-9535



ВОЛОДИМИР ПЕТРІВСЬКИЙ
Доктор філософії (PhD), Асистент кафедри програмних систем і технологій. Київського національного університету імені Тараса Шевченка;
e-mail: volodymyr.petrivskyi@knu.ua
ORCID: 0000-0001-9298-8244



ДЕНИС ШТОМА
Студент 3 курсу ФІТ Київського національного університету імені Тараса Шевченка.
E-mail: denys.shtoma@knu.ua
ORCID: 0009-0009-8942-3088
Наукові інтереси: кібербезпека IoT-систем, машинне навчання, аналіз мережевих аномалій

КОНВЕРГЕНЦІЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ: CPU, GPU, NPU, CXL

Андрій Бондарчук, Віталій Залива, Микола Лисенко

Анотація. *У роботі розглянуто сучасний стан та перспективи розвитку гетерогенних обчислювальних архітектур. Проаналізовано еволюцію ролі центрального процесора від простого виконавця обчислень до оркестратора потоків даних між спеціалізованими прискорювачами. Досліджено особливості чиплетної архітектури, технології CXL 3.0 для об'єднання пам'яті, а також апаратні рішення для прискорення AI-завдань. Окрему увагу приділено програмним стекам, що забезпечують безшовну інтеграцію гетерогенних компонентів. Визначено три ключові вектори подальшого розвитку: інтеграція на рівні кристала, масштабування до рівня дата-центру та інтелектуальна оркестрація обчислювальних ресурсів.*

Ключові слова: гетерогенні архітектури, обчислювальні системи, процесор, оркестрація обчислень.

I. ВСТУП

Ера, коли продуктивність визначалася лише тактовою частотою або кількістю ядер, завершилася. З уповільненням дії закону Мура, подальший прогрес забезпечується не мініатюризацією, а інтелектуальною інтеграцією спеціалізованих обчислювальних блоків. Сьогодні ми переходимо від простого набору мікросхем у сервері до створення єдиного обчислювального організму, де CPU, GPU, NPU та нова пам'ять на базі CXL працюють як одне ціле.

Актуальність дослідження гетерогенних архітектур зумовлена необхідністю подолання фундаментальних обмежень, з якими зіткнулася напівпровідникова індустрія. Подальше нарощування продуктивності за рахунок збільшення кількості ядер або тактової частоти більше не є ефективним через фізичні обмеження та енергоспоживання. Натомість, чиплетна архітектура та технології об'єднаної пам'яті відкривають нові можливості для масштабування обчислювальних систем. Метою даної роботи є аналіз сучасного стану та перспектив розвитку гетерогенних архітектур, дослідження ролі CPU як оркестратора обчислювальних потоків, а також визначення ключових напрямів подальшої еволюції обчислювальних систем, від інтеграції на рівні кристала до масштабування на рівні цілого дата-центру.

II. ДАНІ ТА МЕТОДИ

Провідні виробники, такі як AMD та Intel, повністю перейшли на chiplet архітектуру, яка стала основою проєктування сучасних гетерогенних систем. Цей підхід дозволяє поєднувати в одному корпусі обчислювальні ядра, виконані за різними техпроцесами, та спеціалізовані прискорювачі, що забезпечує гнучкість конфігурацій та оптимізацію вартості виробництва. Замість монолітного кристала, чиплетна архітектура використовує набір менших чипів (чиплетів), з'єднаних високошвидкісними інтерфейсами, такими як Infinity Fabric від AMD або Embedded Multi-Die Interconnect Bridge (EMIB) від Intel. Це дає змогу комбінувати обчислювальні ядра, графічні процесори, контролери пам'яті та блоки введення-виведення, оптимізуючи кожен компонент під конкретне завдання та технологічний процес.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На рисунку 1 схематично зображено взаємодію трьох ключових обчислювальних компонентів сучасної гетерогенної системи: центрального процесора (CPU), графічного процесора (GPU) та нейронного процесора (NPU). Схема ілюструє еволюцію ролі CPU від простого виконавця обчислень до оркестратора, який розподіляє потоки даних між спеціалізованими прискорювачами. GPU відповідає за паралельні обчислення та матричні

операції, тоді як NPU, інтегрований у систему через шину даних, спеціалізується на виконанні завдань штучного інтелекту з високою енергоефективністю. Така архітектурна організація дозволяє досягти оптимального балансу між продуктивністю, енергоспоживанням та гнучкістю системи, передаючи кожен тип навантаження на найбільш придатний для нього обчислювальний блок. [1]

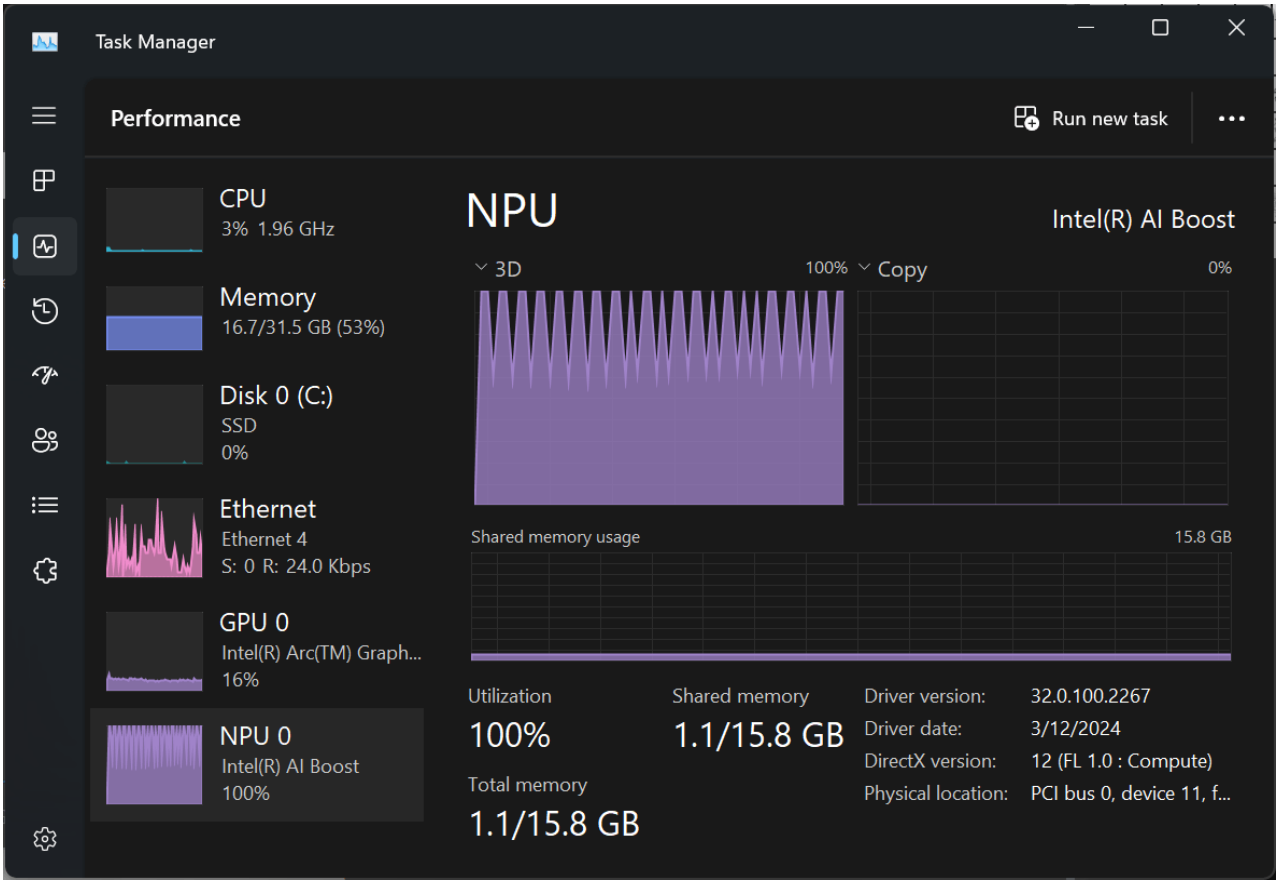


Рисунок 1. *Взаємодія CPU, GPU та NPU в гетерогенній обчислювальній структурі.*

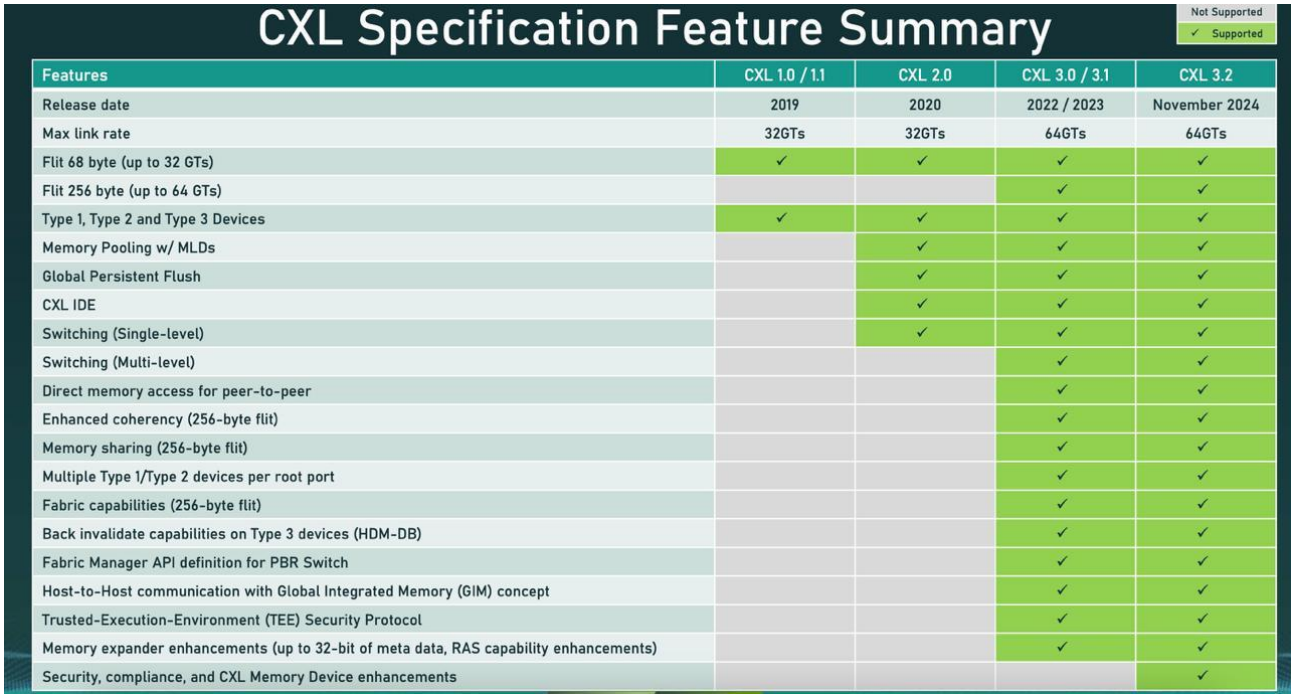
Ключова зміна 2026 року це поява так званого "шару конвергенції CPU-NPU". Процесор більше не є просто "обчислювачем", він стає оркестратором потоку даних для AI-завдань. Аналіз Alibaba Cloud показує, що вузькі місця при обслуговуванні великих мовних моделей LLM тепер припадають не на саме множення матриць (де працюють GPU/NPU), а на етапи попередньої обробки: токенізацію та керування KV-кешем [2]. Тому нові серверні процесори інтегрують апаратні блоки саме для цих завдань. Результат — зменшення затримок на 22% без жодних змін у коді.

Технологія CXL (Compute Express Link) 3.0 стає стандартом де-факто. Вона руйнує традиційну межу між "пам'яттю процесора" та "пам'яттю прискорювача". CXL дозволяє створювати об'єднані пули пам'яті, до яких мають прямий доступ усі гетерогенні компоненти, що критично важливо для роботи з надвеликими моделями. [3]

Головним обмежувачем продуктивності стає не флопс, а пропускна здатність пам'яті. Вирішенням цієї проблеми є перехід до HBM (High Bandwidth Memory) , що фізично наближає пам'ять до обчислювальних блоків .

Найкраще ефективність гетерогенних систем демонструє техніка "PD-Separation" (розділення фаз передзаповнення та декодування), реалізована China Telecom. Вони довели, що фази роботи LLM мають різні вимоги до ресурсів. Динамічно розподіляючи

ці фази між різними типами прискорювачів, вдалося знизити вартість інференції на 42% . Це яскравий приклад того, як архітектура підлаштовується під задачу, а не навпаки.



CXL Specification Feature Summary

Not Supported
✓ Supported

Features	CXL 1.0 / 1.1	CXL 2.0	CXL 3.0 / 3.1	CXL 3.2
Release date	2019	2020	2022 / 2023	November 2024
Max link rate	32GTs	32GTs	64GTs	64GTs
Flit 68 byte (up to 32 GTs)	✓	✓	✓	✓
Flit 256 byte (up to 64 GTs)			✓	✓
Type 1, Type 2 and Type 3 Devices	✓	✓	✓	✓
Memory Pooling w/ MLDs		✓	✓	✓
Global Persistent Flush		✓	✓	✓
CXL IDE		✓	✓	✓
Switching (Single-level)		✓	✓	✓
Switching (Multi-level)			✓	✓
Direct memory access for peer-to-peer			✓	✓
Enhanced coherency (256-byte flit)			✓	✓
Memory sharing (256-byte flit)			✓	✓
Multiple Type 1/Type 2 devices per root port			✓	✓
Fabric capabilities (256-byte flit)			✓	✓
Back invalidate capabilities on Type 3 devices (HDM-DB)			✓	✓
Fabric Manager API definition for PBR Switch			✓	✓
Host-to-Host communication with Global Integrated Memory (GIM) concept			✓	✓
Trusted-Execution-Environment (TEE) Security Protocol			✓	✓
Memory expander enhancements (up to 32-bit of meta data, RAS capability enhancements)			✓	✓
Security, compliance, and CXL Memory Device enhancements				✓

Рисунок 2. *Еволюція CXL*

Жодна складна архітектура не працюватиме без інтелектуального програмного забезпечення. У 2026 році ми спостерігаємо розквіт програмних стеків, які виконують роль "перекладача" між застосунком та різнорідним "залізом". Платформи, наприклад Huawei CANN, дозволяють розробникам писати код на Python, не замислюючись, чи виконується він на CPU, GPU чи NPU [4]. Це забезпечує безшовну інтеграцію та ефективність на рівні 90% від спеціалізованих кластерів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведений аналіз сучасного стану розвитку гетерогенних обчислювальних архітектур засвідчує фундаментальну зміну парадигми проєктування обчислювальних систем. На зміну гонці тактових частот та кількості ядер приходить ера інтелектуальної інтеграції спеціалізованих обчислювальних блоків, об'єднаних у єдиний організм за допомогою чиплетних технологій та інтерфейсів типу CXL. Ключовим висновком є трансформація ролі центрального процесора, який з простого виконавця обчислень перетворюється на оркестратора, що керує потоками даних між CPU, GPU, NPU та іншими прискорювачами. Такий підхід дозволяє досягти значного підвищення продуктивності без нарощування енергоспоживання. Водночас, досвід впровадження NPU показує, що апаратна потужність є необхідною, але недостатньою умовою успіху.

Визначено три ключові вектори подальшого розвитку гетерогенних архітектур. Перший вектор, від "підключення" до "злиття", передбачає подальшу інтеграцію обчислювальних блоків на рівні кристала та упаковки, де роль CPU як центрального елемента не лише зберігатиметься, а й зростатиме через необхідність координації дедалі складніших гетерогенних систем. Другий вектор, від "пристрою" до "системи" , полягає в масштабуванні гетерогенності від окремого чипа до рівня цілого дата-центру, де обчислювальним ресурсом стає вся мережа, утворюючи єдиний "розподілений комп'ютер" з

об'єднаною пам'яттю та обчислювальними потужностями. Третій вектор, від "керування" до "оркестрації", спрямований на розвиток інтелектуальних програмних середовищ, здатних у реальному часі адаптувати архітектуру системи до профілю навантаження, динамічно розподіляючи завдання між прискорювачами з урахуванням їхньої енергоефективності, тепловиділення та доступних бібліотек. Саме цей вектор, як показує приклад техніки PD-Separation від China Telecom [5], здатен забезпечити найбільший приріст економічної ефективності, знижуючи вартість інференції великих мовних моделей на десятки відсотків.

ДЖЕРЕЛА

1. Prieto, P., & Abad, P. (2025). Edge Deployment of Small Language Models, a comprehensive comparison of CPU, GPU and NPU backends. arXiv preprint arXiv:2511.22334.
2. Miao, R., Zhu, L., Ma, S., Qian, K., Zhuang, S., Li, B., ... & Liu, H. H. (2022, August). From luna to solar: the evolutions of the compute-to-storage networks in alibaba cloud. In Proceedings of the ACM SIGCOMM 2022 Conference (pp. 753-766).
3. Das Sharma, D., Blankenship, R., & Berger, D. (2024). An introduction to the compute express link (cxl) interconnect. ACM Computing Surveys, 56(11), 1-37.
4. Shi, K., Liu, Q., Zheng, Z., & Xiao, L. (2023, October). Efficient implementation for composite CNN-based HSI classification algorithm with Huawei ascend framework. In 2023 13th Workshop on Hyperspectral Imaging and Signal Processing: Evolution in Remote Sensing (WHISPERS) (pp. 1-5). IEEE.
5. Wang, L., Gao, D., & Wang, Y. (2025, December). HBM Direct-KV Cache Processing in Compute-in-Memory Architectures: Decoupling for Accelerated LLM Inference. In 2025 IEEE 7th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (Vol. 7, pp. 756-762). IEEE.
6. Сторчак, К. П., Тушич, А. М., & Бондарчук, А. П. (2018). Кластерний аналіз даних із використанням штучних нейронних мереж. Зв'язок, (6), 36-38.



АНДРІЙ БОНДАРЧУК
д.т.н., професор, завідувач кафедри комп'ютерних наук, Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5124-5102
E-mail:a.bondarchuk@kubg.edu.ua
Наукові інтереси: управління , ідентифікація, відеоаналітика, паралельні обчислення



ВІТАЛІЙ ЗАЛИВА
phd, доцент кафедри інженерії програмного забезпечення, Державний університет інформаційно-комунікаційних технологій , Київ, Україна
ORCID: 0009-0002-0857-2209
E-mail: neapolvet@gmail.com
Наукові інтереси: комп'ютерні системи, адаптивні інтерфейси.



МИКОЛА ЛИСЕНКО
аспірант кафедри інформаційних систем та технологій, Державний університет інформаційно-комунікаційних технологій , Київ, Україна
ORCID: 0009-0000-3734-8332
E-mail: lysenkon@ukr.net
Наукові інтереси: машинне навчання, інформаційні системи, аналітика даних.

МОДЕЛЮВАННЯ ТА ЕКВАЛІЗАЦІЯ ШВИДКІСНИХ PAM4 СИГНАЛІВ

Назар Гаврись, Євгеній Коновал

Анотація. *В даній роботі представлено нове рішення з обробки сигналів в рамках участі у конкурсі IMC Challenge під патронатом компанії Huawei. Ми зосередилися на двох ключових проблемах: моделюванні швидкісних сигналів та їх еквалізації. Перше завдання передбачало відновлення аналогових форм сигналів із цифрових PAM4-символів, тоді як друге полягало в точній еквалізації та детектуванні символів у шумних середовищах. Ми застосували методи цифрової обробки сигналів, регуляризоване розкладання Холецького та адаптивне порогування для досягнення стійких рішень із високою точністю.*

Ключові слова: PAM4, обробка сигналів, еквалізація, розкладання Холецького, швидкісний зв'язок.

I. ВСТУП

Конкурс IMC, спонсорований компанією Huawei, — це міжнародний конкурс, у межах якого учасники розв'язують реальні проблеми в галузі швидкісного зв'язку та обробки сигналів. Наше дослідження зосередилося на двох конкретних завданнях: Задача A: моделювання швидкісних сигналів та Задача B: еквалізація швидкісних сигналів. Обидва завдання пов'язані з PAM4 (імпульсною амплітудною модуляцією з чотирма рівнями) — форматом модуляції, який став ключовим у проєктуванні сучасних систем передавання даних [1].

Задача A передбачала розроблення моделі, здатної відновлювати аналогові форми сигналів із цифрових послідовностей PAM4-символів. Складність полягала в наявності міжсимвольної інтерференції (ISI), шуму та інших спотворень, що виникають під час передавання сигналу. Задача B зосереджувалася на приймальній стороні, де завданням було виділення PAM4-символів із шумних аналогових сигналів, що потребувало визначення оптимальної фази дискретизації та застосування адаптивних методів еквалізації [2].

II. ДАНІ ТА МЕТОДИ

Модуляція PAM4 використовує чотири дискретні рівні амплітуди (−3, −1, +1, +3), кодуючи два біти на кожен символ. Це підвищує спектральну ефективність порівняно з двійковою модуляцією, однак зменшує стійкість до шуму та ISI.

Для Задачі A відновлення аналогової форми сигналу формулюється як система регуляризованих лінійних регресійних моделей. Регуляризовані нормальні рівняння розв'язуються за допомогою розкладання Холецького:

$$(X^{\mathrm{T}}X + \lambda I)w = X^{\mathrm{T}}y \qquad (1)$$

де:

- $\boldsymbol{X^T}$ – транспонована матриця ознак
- $\boldsymbol{X}$ — матриця ознак (вікно цифрових символів)
- y — вектор аналогових відліків (цільові значення)
- λI — регуляризація (ridge-регресія)
- w — набір коефіцієнтів фільтра

Параметр регуляризації λ було визначено як $\lambda = \kappa \cdot tr(X^{\mathrm{T}}X)$, з $\kappa = 10^{-6}$, де $tr(X^{\mathrm{T}}X)$ — це сума квадратів усіх елементів матриці X. Такий підхід забезпечує числову стабільність та оберненість матриці шляхом додавання штрафного члена, пропорційного енергії матриці автокореляції [3].

Для Задачі B наш підхід складався з трьох етапів: вибору фази дискретизації шляхом максимізації міжквартильного розмаху (IQR), медіанної нормалізації та адаптивного оцінювання порогів на основі квантильних методів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Для Задачі A середньоквадратична помилка (RMS) між відновленою формою сигналу та еталонним сигналом становила 0,616. На рисунку 1 наведено діаграму ока, побудовану за першими 50 символами відновленого сигналу. Діаграма демонструє частково відкриті «ока», що свідчить про наявність ISI та шуму, проте їхній вплив не є критичним.

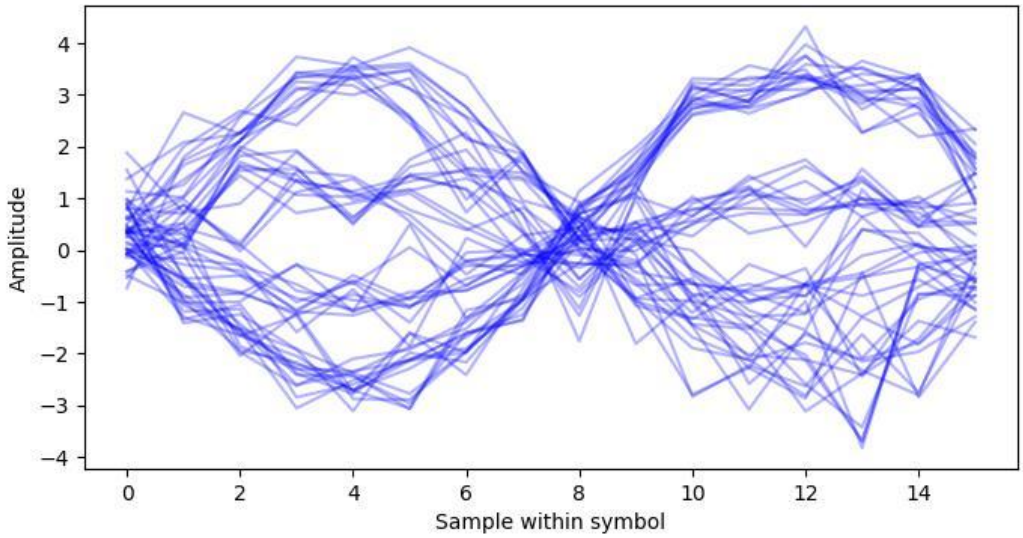


Рисунок 1. *Діаграма ока відновленої форми сигналу (Задача A)*

На рисунку 2 наведено гістограму відновлених символів. В ідеальному випадку спостерігаються чотири чітко виражені піки, що відповідають рівням PAM4 (−3, −1, +1, +3). У відновленій формі сигналу піки недостатньо добре розділені, що відображає вплив шуму.

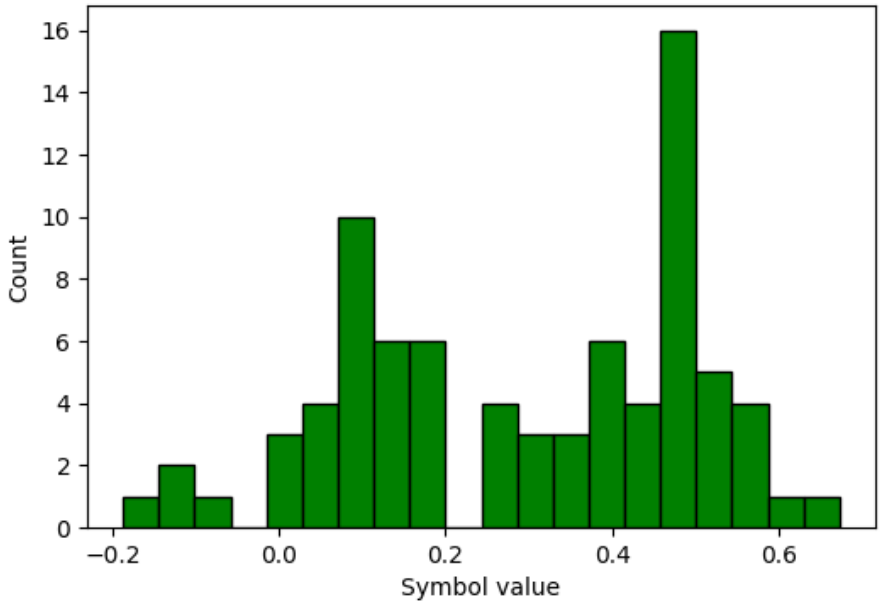


Рисунок 2. *Гістограма відновлених символів (Задача A)*

Для Задачі В було досягнуто коефіцієнт символьної помилки (SER) на рівні 27,6 %. На рисунку 3 наведено діаграму ока прийнятого сигналу, яка не демонструє чітко відкритих «вікон», що свідчить про значний вплив ISI та шуму.

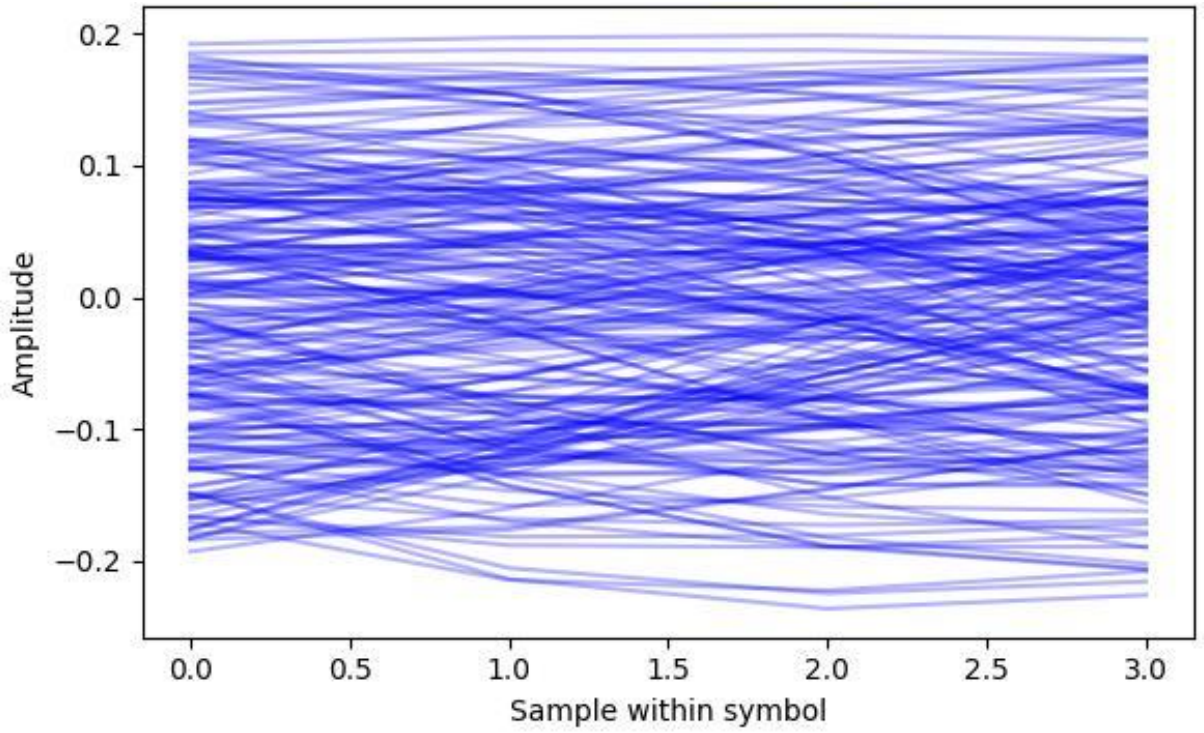


Рисунок 3. *Діаграма ока прийнятого сигналу (Задача В)*

На рисунку 4 наведено гістограму детектованих символів із порогами прийняття рішення. Замість чотирьох чітко виражених піків значення розподілені в перекривних діапазонах, що призводить до частих помилок класифікації.

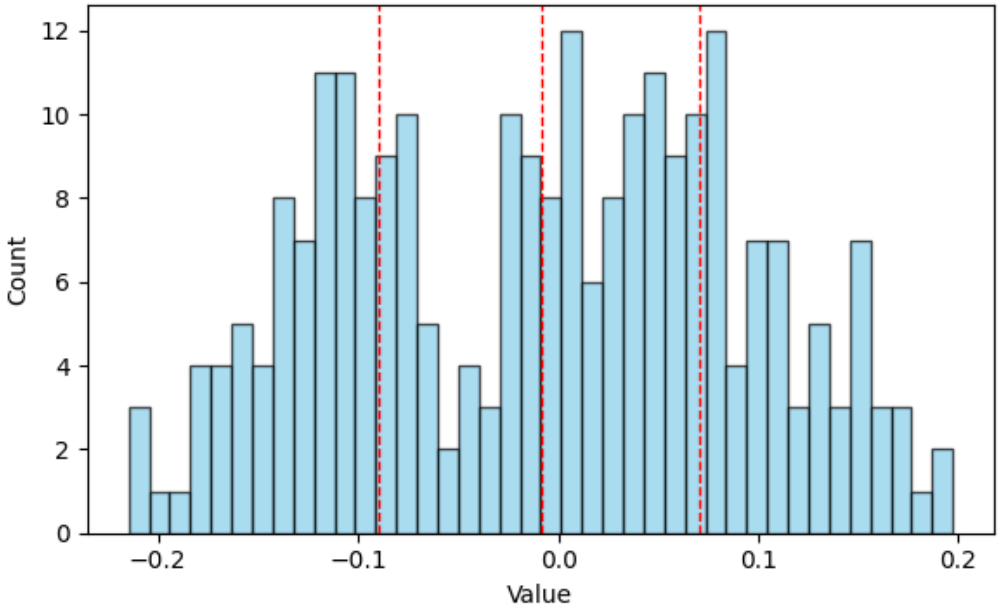


Рисунок 4. *Гістограма детектованих символів із порогами (Задача В)*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Застосований метод для Задачі А забезпечує відтворення загальної часової структури та основних статистичних характеристик PAM4-сигналу, зокрема амплітудного розподілу рівнів. Водночас через вплив каналу з пам'яттю, що спричиняє міжсимвольну інтерференцію, а також через наявність шуму та обмежену довжину фільтра, повне розділення рівнів символів не досягається. Середньоквадратична помилка використовується як кількісна метрика відхилення від еталонного аналогового сигналу та дозволяє об'єктивно оцінити якість відновлення.

Для Задачі В отримані результати демонструють обмеження базового методу. Хоча він відтворює окремі статистичні характеристики сигналу, проте не забезпечує точного відновлення символів в умовах реального шуму та спотворень каналу. Для зменшення коефіцієнта символьної помилки (SER) доцільно розглянути ефективніші методи, такі як адаптивна еквалізація, еквалізація зі зворотним зв'язком або кластеризаційне оцінювання рівнів [4].

ДЖЕРЕЛА

1. Miller B. PAM4: pulse amplitude modulation explained. Semiconductor Engineering. URL: https://semiengineering.com/pam4-pulse-amplitude-modulation-explained/ (дата доступу: 28.02.2026).
2.50G PAM4 technical white paper. Huawei Carrier. URL: https://carrier.huawei.com/~/media/CNBGV2/download/products/networks/50G-PAM4-Technical-White-Paper.pdf (date of access: 28.02.2026).
3. J. Nicholas. Analysis of the cholesky decomposition of a semi-definite matrix. MIMS EPrints. URL: https://eprints.maths.manchester.ac.uk/1193/1/high90c.pdf (дата доступу: 28.02.2026).
4. A PAM4 transceiver design scheme with threshold adaptive and tap adaptive. SpringerLink. URL: https://link.springer.com/content/pdf/10.1186/s13634-023-01033-y.pdf (дата доступу: 28.02.2026).
5. IMC Challenge sponsored by Huawei 2025. URL: https://www.huawei.com/minisite/imc-challenge/en/ (дата доступу: 28.02.2026)



НАЗАР ГАВРИСЬ
Студент, факультет інформаційних технологій та математики, Київський столичний університет імені Бориса Грінченка, Україна
ORCID: 0009-0000-3183-7047
E-mail:nahavrys.fitm23@kubg.edu.ua
Наукові інтереси: обробка сигналів, швидкісні системи зв'язку.



ЄВГЕНІЙ КОНОВАЛ
Студент, факультет інформаційних технологій та математики, Київський столичний університет імені Бориса Грінченка, Україна
ORCID: 0009-0007-5063-7957
E-mail: yykonoval.fitm23@kubg.edu.ua
Наукові інтереси: цифрова обробка сигналів, алгоритми еквалізації.

ІНТЕЛЕКТУАЛІЗАЦІЯ КЕРУВАННЯ ВІРТУАЛЬНИМИ МЕРЕЖЕВИМИ ФУНКЦІЯМИ В АРХІТЕКТУРАХ SDN/KDN ДЛЯ ВИСОКОНАВАНТАЖЕНИХ СЕРВІСІВ

Дмитро Кульчицький

Анотація. *У роботі розглянуто підходи до інтелектуалізації керування віртуальними мережевими функціями в архітектурах SDN та KDN для високонавантажених сервісів. Проаналізовано інтеграцію NFV, централізованого SDN-керування та аналітичного шару KDN. Окреслено можливості застосування нечіткої логіки для оцінювання стану мережі, оптимізації ресурсів і масштабування сервісів. Показано, що інтелектуальні моделі сприяють підвищенню адаптивності інфраструктури та покращенню якості обслуговування.*

Ключові слова: SDN, KDN, NFV, віртуальні мережеві функції, інтелектуальне керування, QoS.

I. ВСТУП

Стрімка цифровізація суспільства, поширення хмарних платформ, розвиток фінтех-сервісів, систем електронних платежів, платформ дистанційної взаємодії та інших критично важливих інформаційних систем зумовлюють постійне зростання вимог до мережевої інфраструктури. Для сучасних високонавантажених сервісів важливими є не лише достатня пропускна здатність мережі, а й здатність системи забезпечувати низьку затримку, надійність, доступність та адаптивність до швидких змін середовища. У таких умовах традиційні методи побудови та адміністрування мереж уже не повною мірою відповідають потребам динамічних цифрових платформ.

У цій роботі розглянуто особливості інтелектуалізації керування віртуальними мережевими функціями в архітектурах SDN/KDN, а також окреслено можливості використання нечіткої логіки та аналітичних моделей для підтримки стабільності високонавантажених сервісів.

II. ДАНІ ТА МЕТОДИ

Методологічною основою дослідження є аналіз підходів до побудови SDN і NFV інфраструктур, вивчення концепції KDN та узагальнення сучасних методів інтелектуального керування мережевими функціями. У роботі розглянуто високонавантажене сервісне середовище, в якому мережеві сервіси реалізуються як ланцюги віртуальних мережевих функцій, зокрема балансувальників навантаження, міжмережевих екранів, систем моніторингу, шлюзів безпеки та маршрутизувальних модулів.

Запропонований підхід орієнтований на інтегральне оцінювання стану сервісного ланцюга. Це означає, що об’єктом аналізу є не окрема віртуальна мережна функція ізольовано, а вся послідовність взаємопов’язаних компонентів, від яких залежить робота конкретного цифрового сервісу. Такий підхід дозволяє виявляти вузькі місця, що виникають в окремих сегментах інфраструктури, та ухвалювати керувальні рішення з урахуванням їх впливу на загальну продуктивність і якість обслуговування.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз показує, що інтелектуалізація керування в архітектурах SDN/KDN принципово змінює логіку функціонування мережевої інфраструктури. У традиційних системах мережеве керування часто реалізується реактивно, тобто після перевищення заздалегідь установленого порогу завантаження або затримки. Такий підхід у високонавантажених середовищах виявляється недостатнім, оскільки деградація сервісу може розвиватися швидше, ніж система встигне відреагувати. Натомість інтелектуальна модель дозволяє враховувати сукупність параметрів і виявляти ризикові тенденції ще до переходу мережі в критичний стан.

У межах проведеного узагальнення було виділено типові стани мережевого середовища, відповідні їм індикатори, рівні ризику та рекомендовані керувальні дії, що наведено в Таблиці 1.

Таблиця 1. *Відповідність станів мережевого середовища*

Стан мережевого середовища	Характерні індикатори	Рівень ризику	Рекомендована керувальна дія
Стабільний	Низька затримка, рівномірне навантаження, мінімальні втрати пакетів	Низький	Підтримання поточної конфігурації, постійний моніторинг телеметрії
Зростаюче навантаження	Підвищення кількості сесій, локальне зростання затримки, збільшення використання CPU/RAM	Помірний	Превентивний перерозподіл трафіку, підготовка до масштабування
Ризик деградації	Нестабільна затримка, перевантаження окремих VNF, зростання втрат пакетів	Високий	Горизонтальне або вертикальне масштабування VNF, зміна маршрутів обробки трафіку
Критичний стан	Критична затримка, різке зростання навантаження, суттєве погіршення QoS	Критичний	Міграція VNF, пріоритизація критичного трафіку, тимчасове обмеження другорядних сервісів

Як видно з Таблиці 1, найбільш ефективним є підхід, за якого керування ґрунтується не на одному ізольованому показнику, а на інтегральній оцінці стану мережевого середовища. Наприклад, незначне зростання затримки саме по собі ще не завжди означає критичну ситуацію. Однак якщо воно супроводжується різким збільшенням кількості активних сесій, перевантаженням окремих вузлів і зростанням втрат пакетів, це вже свідчить про високий ризик деградації сервісу. У такому випадку система повинна не чекати повного виходу за порогові значення, а реагувати завчасно.

Аналіз показує, що застосування аналітичного шару KDN у поєднанні з NFV-оркестрацією відкриває можливість як для реактивного, так і для проактивного керування. У реактивному режимі система реагує на вже наявні зміни стану інфраструктури. У проактивному режимі вона здатна виявляти тренди, прогнозувати можливе погіршення

якості обслуговування та ініціювати керувальні дії заздалегідь. Для високонавантажених фінтех-сервісів, систем обробки транзакцій, хмарних платформ і сервісів реального часу це має принципове значення, оскільки забезпечує підтримку безперервності роботи та зменшує ризик критичних відмов.

Серед основних переваг інтелектуалізованого підходу:

- підвищення адаптивності мережі до динамічних навантажень;
- скорочення часу реакції на пікові стани;
- зменшення ризику перевантаження окремих VNF;
- ефективніше використання обчислювальних ресурсів;
- покращення якості обслуговування критичних сервісів.

Таким чином, результати аналізу підтверджують, що поєднання SDN, NFV та KDN створює основу для формування адаптивної мережевої інфраструктури нового покоління, здатної ефективно підтримувати стабільність і продуктивність високонавантажених сервісів.

IV. ВИСНОВКИ

У результаті дослідження встановлено, що інтелектуалізація керування віртуальними мережевими функціями в архітектурах SDN/KDN є перспективним напрямом розвитку мережевих технологій, оскільки поєднання програмно-конфігурованого керування, NFV та аналітичного шару знань забезпечує перехід до адаптивного прийняття рішень і підвищує ефективність використання ресурсів. Інтегральна оцінка стану мережевого середовища дозволяє своєчасно виявляти ризики деградації сервісів, ініціювати масштабування або перерозподіл ресурсів і підтримувати необхідний рівень якості обслуговування, що особливо важливо для високонавантажених систем; подальші дослідження доцільно спрямувати на розроблення когнітивних моделей прийняття рішень та їх експериментальну перевірку в середовищах SDN/NFV.

ДЖЕРЕЛА

1. Kreutz D., Ramos F. M. V., Verissimo P., Rothenberg C. E., Azodolmolky S., Uhlig S. Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE. 2015. Vol. 103, No. 1. P. 14–76.
2. Mestres A., Rodriguez-Natal A., Carner J. et al. Knowledge-Defined Networking. ACM SIGCOMM Computer Communication Review. 2017. Vol. 47, No. 3. P. 2–10.
3. ETSI. Network Functions Virtualisation (NFV): An Introduction, Benefits, Enablers, Challenges and Call for Action. ETSI White Paper. 2012.



ДМИТРО КУЛЬЧИЦЬКИЙ
Аспірант кафедри інформаційних систем та технологій у Київському національному університеті імені Тараса Шевченка.
ORCID : 0009-0009-4060-315X
E-mail: dima01062009@gmail.com
Серед наукових інтересів — Прикладне програмування, IoT системи.

ВИКОРИСТАННЯ ЦИФРОВИХ ПЛАТФОРМ ДЛЯ АНАЛІЗУ ЗОВНІШНЬОПОЛІТИЧНИХ КОМУНІКАЦІЙ: КЕЙС ПУБЛІКАЦІЙ МЗС КНР У СОЦМЕРЕЖІ X ЩОДО КИТАЙСЬКО-ЯПОНСЬКИХ ВІДНОСИН (ГРУДЕНЬ 2025 Р.)

Анна Кушнір, Галина Кучаковська

Анотація. *У тезах досліджено використання цифрових платформ для аналізу зовнішньополітичних комунікацій на прикладі публікацій Міністерства закордонних справ КНР у соціальній мережі X щодо китайсько-японських відносин у грудні 2025 року. Розглянуто трансформацію дипломатичної комунікації під впливом соціальних мереж, зокрема розвиток публічної дипломатії та явища Twiplomacy. Проаналізовано зміст офіційних повідомлень китайської сторони у контексті загострення регіональної безпеки, питання Тайваню та історичних наративів. Встановлено, що цифрові платформи виступають інструментом оперативного реагування, формування міжнародного іміджу та впливу на глобальну громадську думку, що робить їх невід'ємною складовою сучасних дипломатичних практик.*

Ключові слова: цифрова дипломатія; Twiplomacy; соціальні мережі; зовнішньополітична комунікація; Китай-Японія.

I. ВСТУП

Поява соціальних мереж трансформувало дипломатичну практику та методи міждержавної комунікації. Наразі такі платформи як Instagram, YouTube або X (Twitter) використовуються для реалізації публічної дипломатії, поширення наративів та демонстрації позицій акторів міжнародних відносин поза межами прес-конференцій. В останній час саме за цим принципом проявлялись аспекти комплексних відносин між КНР та Японією – двох держав-лідерів Індо-Тихоокеанського регіону. Загострення китайсько-японських відносин можливо прослідкувати на основі публікацій МЗС КНР у соцмережі X.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Термін «соціальна мережа» був започаткований британським соціологом, представником Манчестерської школи Джеймсом Барнсом у 1954, що означав тісні взаємовідносини між двома і більше людьми [2]. Однак на тлі появи Інтернету, сучасне привичне поняття соціальної мережі – це платформа, що допомагає людям здійснювати зв'язок між собою та групуванню за специфічними інтересами внезалженості від індивідуальних можливостей, уподобань чи місця проживання [2].

Враховуючи дипломатичну природу прикладів цієї роботи, то варто зазначити, що дипломатична комунікація – це процес обміну інформацією та взаємодії між державами, міжнародними організаціями й іншими суб'єктами міжнародних відносин, спрямований на встановлення, підтримку та розвиток мирних і взаємовигідних відносин [1, с. 2].

Об'єднавши обидва виміри комунікацій, то можливо підкреслити, що соцмережі стали каналами для оперативного реагування та поширення офіційних заяв, коментарів тощо у реальному часі. З усіх платформ, Twitter став вагомою платформою для реалізації дипломатії: ще у 2018 р. близько 79,6% політичних діячів із 26 країн Європи були залучені до Twiplomacy [1, с. 3].

У грудні ця соцмережа продовжувала існувати як канал міждержавної комунікації, що можливо побачити на прикладі китайсько-японських відносин, зокрема повідомлень китайської сторони.

Як реакцію на ремарки прем'єр-міністерки Японії Такаїчі щодо можливої ескалації ситуації навколо Тайваню, 4 грудня 2025 р. прес-секретар КНР МЗС Лін Цзяня опублікував: "Ми закликаємо японську сторону задуматися над своїми помилками та виправити їх, а також відкликати помилкові заяви прем'єр-міністра Такаїчі щодо Тайваню. Факти та зобов'язання Японії чітко викладені в історичних документах. «Без змін у позиції» — це далеко не адекватна і, безумовно, неприйнятна відповідь Китаю" [6].

Інше повідомлення від 8 грудня 2025 р., коли Японія підняла винищувачі у відповідь на маневри російських та китайських бомбардувальників [3] між японськими островами Окінава та Міяко: «Інцидент стався через навмисне вторгнення японських літаків у зони навчань і тренувань Китаю, а також через їхню близьку розвідку і перешкоджання нормальній військовій діяльності Китаю. Проте японська сторона звинуватила в цьому Китай і спробувала ввести в оману світову громадськість, безпідставно звинуативши Китай у «радіолокаційному освітленні». Китай засуджує і виступає проти цих безпідставних звинувачень і висловив японській стороні рішучий протест.» [7]

Інші публікації також обертаються навколо теми Тайваню, спільного історичного минулого між ним, КНР та Японією, а ще зміни японської оборонної та безпекової політики: «Китайський народ... має відповідальність підтримувати... зобов'язання перешкоджати амбіціям Японії озброїтися і навіть відродити мілітаризм» [5]; «Японські мілітаристи під час Другої світової війни вели загарбницькі війни та чинили нелюдські злочини, створивши найпохмурішу сторінку в історії людства. Незважаючи на поразку, Японія так і не змогла повністю викорінити лихо мілітаризму в країні.» [4]

III. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Підбиваючи підсумки, розвиток соціальних мереж суттєво трансформував методи ведення дипломатичної комунікації, перевівши значну частину взаємодії держав у відкритий цифровий простір. Соціальні платформи стали не лише каналом інформування, а й інструментом формування наративів, стратегічного впливу та демонстрації позиції держави в режимі реального часу. Саме в цьому контексті сформувалося явище Twiplomacy − використання мікроблогінгових сервісів для здійснення дипломатичної діяльності.

Аналіз публікацій МЗС КНР у мережі X у грудні 2025 року свідчить, що цифрова дипломатія активно застосовується для реагування на політичні заяви, військові інциденти та історичні суперечності у китайсько-японських відносинах. Повідомлення китайської сторони виконують одразу кілька функцій: офіційне спростування або засудження дій опонента, мобілізацію внутрішньої та міжнародної підтримки, а також формування бажаної інтерпретації подій для світової аудиторії.

Особливістю таких комунікацій є поєднання дипломатичного дискурсу з елементами інформаційного протиборства. Звернення до історичної пам'яті, питання Тайваню та безпекової політики Японії демонструють використання цифрових платформ як інструменту стратегічної комунікації, що виходить за межі традиційної дипломатії.

Отже, цифрові платформи стали невід'ємною складовою сучасних міжнародних відносин, забезпечуючи швидкість, публічність і глобальне охоплення дипломатичних меседжів. Подальші дослідження можуть бути спрямовані на порівняльний аналіз цифрової дипломатії різних держав, вивчення її ефективності та впливу на формування міжнародної громадської думки й прийняття зовнішньополітичних рішень

ДЖЕРЕЛА

1. Бойко, А. (2025) Вплив соціальних мереж на дипломатичну комунікацію. Матеріали Всеукраїнської науково-практичної конференції. https://conf.ztu.edu.ua/wp-content/uploads/2025/02/576.pdf
2. Соціальні мережі: Поняття, історія виникнення. (б. д.). https://zounb.zp.ua/resourse/zaporizkyy-kray/zaporizhzhya-bibliotechne/fahova-osvita/socialni-merezhi-piv.
3. Японія підняла винищувачі у відповідь на маневри російських та китайських бомбардувальників. (б. д.). https://www.ukrinform.ua/rubric-world/4067933-aponia-pidnala-vinisuvaci-u-vidpovid-na-manevri-rosijskih-ta-kitajskih-bombarduvalnikiv.html.
4. Lin Jian 林剑 (@SpoxCHN_LinJian). Пост у X (Twitter) від 22.12.2025. (б. д.). https://x.com/SpoxCHN_LinJian/status/2003112979102085605?s=20
5. Lin Jian 林剑 (@SpoxCHN_LinJian). Пост у X (Twitter) від 09.12.2025 (б. д.). https://x.com/SpoxCHN_LinJian/status/1998409058953658826?s=20
6. Lin Jian 林剑 (@SpoxCHN_LinJian). Пост у X (Twitter) від 04.12.2025. (б. д.). https://x.com/SpoxCHN_LinJian/status/1996593109468352595?s=20
7. Lin Jian 林剑 (@SpoxCHN_LinJian). Пост у X (Twitter) від 08.12.2025. (б. д.). https://x.com/SpoxCHN_LinJian/status/1998032137174536663?s=20



АННА КУШНІР
студентка ІІІ курсу бакалаврату суспільних комунікацій, кафедра міжнародних відносин, Факультет права та міжнародних відносин, Київський столичний університет імені Бориса Грінченка
E-mail: aokushnir.fpmv24@kubg.edu.ua
Студентка ІІІ курсу бакалаврату спеціальності «Суспільні комунікації» кафедри міжнародних відносин Факультету права та міжнародних відносин Київський столичний університет імені Бориса Грінченка. Наукові інтереси охоплюють проблематику зовнішньополітичних комунікацій, використання інформаційно-комунікаційних технологій у сфері суспільних комунікацій, а також інтеграцію соціальних мереж у професійну діяльність фахівця з суспільних комунікацій. Бере участь у наукових і освітніх заходах, пов'язаних із дослідженням сучасних цифрових практик комунікації.



ГАЛИНА КУЧАКОВСЬКА
кандидат педагогічних наук, старший викладач кафедри комп'ютерних наук, факультет інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка,
ORCID: 0000-0002-4555-896X
E-mail: h.kuchakovska@kubg.edu.ua
отримала ступінь магістра соціальної інформатики у Київському столичному університеті імені Бориса Грінченка (Київ, Україна) в 2011 році. Захистила дисертацію на здобуття кандиада педагогічних наук у 2025 році в Інституті цифровізації освіти НАН України. Серед наукових інтересів — ІКТ в освіті, використання ШІ технологій в освітньому процесі, шляхи впровадження соціальних мереж в процес навчання студентів ЗВО. Автор понад 30 наукових праць, деякі з яких індексуються в міжнародних науково-метричних базах Scopus та Web of Science.

МЕТОДИ ТА АЛГОРИТМИ КООРДИНАЦІЇ РОЗПОДІЛЕНИХ МУЛЬТИАГЕНТНИХ СИСТЕМ У СЕРЕДОВИЩАХ З ОБМЕЖЕНОЮ НАВІГАЦІЄЮ

Сергій Шевченко

Анотація. *У цій роботі розглядається розробка децентралізованої мультиагентної системи рою безпілотних літальних апаратів, здатної функціонувати без GPS та централізованої інфраструктури. Запропонована архітектура базується на локальній mesh-комунікації, алгоритмах консенсусу та розподіленому механізмі розподілу задач між агентами. Рішення забезпечує узгоджену координацію дронів в автономних місіях, зокрема у задачах пошуку і рятування та моніторингу в умовах обмеженого зв'язку.*

Ключові слова: IoT, мультиагентні системи, рій безпілотних літальних апаратів, децентралізоване керування, mesh-мережі, алгоритми консенсусу, розподіл задач, автономні системи.

I. ВСТУП

Сучасний розвиток автономних безпілотних літальних апаратів сприяє активному впровадженню мультиагентних систем, здатних виконувати складні завдання у кооперації. Ройові підходи дозволяють підвищити гнучкість, масштабованість та відмовостійкість у порівнянні з одиночними платформами, що особливо актуально для задач моніторингу, пошуку і рятування та роботи у небезпечних середовищах. Водночас більшість існуючих рішень залежать від супутникової навігації та централізованих серверів керування, що обмежує їх застосування в умовах втрати GPS-сигналу або мережевої інфраструктури. Такі обмеження створюють ризики втрати координації, зниження надійності та повної зупинки місії у разі відмови центрального вузла. У зв'язку з цим особливої ваги набуває розробка децентралізованих механізмів координації, які забезпечують узгоджену поведінку агентів на основі локальної взаємодії. Метою даного дослідження є проєктування та аналіз архітектури рою автономних дронів, що функціонує без GPS і централізованого керування та використовує розподілені алгоритми для досягнення спільних цілей.

II. ДАНІ ТА МЕТОДИ

Запропонована система реалізує архітектуру рою автономних агентів, у якій кожен безпілотний літальний апарат виступає як самостійний обчислювальний та комунікаційний вузол. Дрони обмінюються службовою інформацією про власний стан і параметри місії через локальну mesh-мережу, що забезпечує прямі зв'язки між сусідніми агентами без використання централізованого сервера.Для узгодження спільної поведінки застосовуються розподілені алгоритми консенсусу, які забезпечують поступове вирівнювання станів агентів на основі локальної взаємодії. Розподіл задач між дронами реалізується через децентралізований механізм обміну оцінками та прийняття рішень, що дозволяє визначати виконавця без центрального координатора. Така методологія забезпечує масштабованість, відмовостійкість і автономність функціонування рою в умовах обмеженого зв'язку.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У ході експериментального моделювання було досліджено поведінку рою автономних агентів у конфігураціях з різною кількістю вузлів та за умов контрольованої деградації

мережі. Система продемонструвала стабільне формування узгоджених рішень щодо розподілу задач без використання централізованого координатора. За базового інтервалу керуючого циклу 250 мс середня затримка між публікацією задачі та прийняттям рішення про її призначення перебувала в межах приблизно однієї секунди, що відповідає моделі одновіконного аукціону з фіксованим часовим вікном узгодження. Навіть при збільшенні кількості агентів від 5 до 20 зберігалася передбачуваність часу прийняття рішення, а зростання затримки мало помірний характер. Перевірка коректності розподілу задач показала, що за відсутності втрат пакетів система стабільно обирає агента з мінімальною обчисленою вартістю виконання задачі, що підтверджує узгодженість локальних оцінок і глобального результату. У серіях повторних запусків не спостерігалося конфліктного призначення однієї задачі кільком агентам. За моделювання втрат керуючих повідомлень на рівні 5% усі сценарії завершувалися коректним призначенням, хоча час узгодження незначно зростав. При 10% втрат більшість задач узгоджувалася в межах першого вікна прийняття рішень, а в окремих випадках було необхідне додаткове коло обміну повідомленнями, що призводило до затримки приблизно на один цикл керування. При цьому явищ розходження або «роздвоєного» рішення не зафіксовано.

У всіх досліджених конфігураціях система демонструвала стійку збіжність без ознак нестабільності. Отримані результати свідчать про відмовостійкість, масштабованість та придатність запропонованої децентралізованої архітектури для застосування в умовах обмеженого або деградованого зв’язку.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована децентралізована архітектура рою автономних безпілотних літальних апаратів підтвердила свою ефективність у забезпеченні узгодженої колективної поведінки без використання GPS та централізованих вузлів керування. Наукова цінність роботи полягає у демонстрації практичної реалізації алгоритмів консенсусу та розподілу задач у середовищі з деградованим зв’язком, а практична — у можливості застосування підходу для пошуково-рятувальних операцій, моніторингу та автономних місій у складних умовах.

Децентралізований підхід забезпечує відмовостійкість, усуває єдину точку відмови та підвищує масштабованість системи зі зростанням кількості агентів. Подальші дослідження можуть бути спрямовані на інтеграцію сенсорних підсистем локалізації, розширення механізмів динамічного перепризначення задач та вдосконалення адаптивності рою в умовах високої мобільності й змінного середовища.

ДЖЕРЕЛА

1. Olfati-Saber, R., Fax, J. A., Murray, R. M. Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE, 2007.
2. Ren, W., Beard, R. W. Consensus seeking in multi-agent systems under dynamically changing interaction topologies. IEEE Transactions on Automatic Control, 2005.



СЕРГІЙ ШЕВЧЕНКО
Студент, Кафедра інформаційних систем та технологій, КНУ ім. Т.Г.Шевченка, Київ, Україна
E-mail: s.v.shewchenko@knu.ua
Здобуває ступінь магістра комп’ютерних наук у Київському національному університеті імені Тараса Шевченка (Київ, Україна). Серед наукових інтересів — системи комп’ютерного моніторингу та контролю.

Section

Security of information systems and networks

Секція

Безпека інформаційних систем та мереж

RISK-BASED MODEL FOR CRYPTOGRAPHIC MFA SELECTION

Daulet Zhumat

Abstract. *Modern web and cloud services increasingly rely on identity as the main security boundary. While multi-factor authentication (MFA) is widely deployed, different MFA classes provide very different resistance to phishing, adversary-in-the-middle attacks, and social engineering. This short paper compares three representative MFA classes - one-time codes, push confirmations enhanced with explicit user intent, and public-key credentials - and proposes a lightweight selection model. The proposed contribution is a simple 0-2 scoring rubric and a decision-tree recommendation that helps choose stronger cryptography-based MFA for higher-risk accounts while keeping practical fallback options.*

Keywords: multi-factor authentication; cryptography-based authentication; phishing resistance; cloud access; risk-based model.

I. INTRODUCTION

Identity-based attacks are still one of the most common problems in cloud systems. Even today, phishing attacks and session interception remain effective, and attackers often try to capture user credentials or authentication sessions instead of breaking technical defenses directly. Recent research confirms that phishing techniques continue to evolve and remain a major security risk for online services [9], [3].

Because of this, many organizations use multi-factor authentication (MFA). However, it is important to understand that not all MFA methods provide the same level of protection. Some mechanisms only add a second step for the user, while others use cryptographic verification and are much harder to bypass. According to NIST guidance, stronger authentication methods should rely on cryptographic proof of possession and authenticators that cannot be copied or exported, which improves resistance to phishing attacks [1].

In this paper, we focus on three MFA classes that are widely used in web and cloud applications today:

- time-based one-time passwords (TOTP),
- push authentication with number matching or explicit confirmation,
- public-key authentication implemented through WebAuthn and passkeys [2], [5].

The goal of this work is not to build a complex theoretical model, but to give a short and practical comparison that shows how these approaches differ in security and usability. We also try to explain in simple terms when each method is more suitable.

II. DATA AND METHODS

To make the comparison clear, we evaluate the three MFA classes using six criteria that reflect both security strength and real-world usage:

- resistance to phishing attacks,
- resistance to session relay or adversary-in-the-middle attacks,
- protection against accidental approval or notification fatigue,
- behaviour when the user device or session is compromised,
- user convenience and effort required,
- complexity of deployment and recovery.

Each criterion is scored from 0 to 2, where 0 means weak protection, 1 means partial protection, 2 means strong protection. This approach is based on modern authentication standards and recent studies discussing WebAuthn, FIDO authentication models, and security properties of

different MFA systems [2], [5], [6]. Research on usability and authentication workflows was also considered, since adoption problems often determine which methods organizations actually use in practice [7]. The goal of this method is not to produce exact numeric measurements, but to provide a simple structured comparison that can be easily explained and applied.

III. RESULTS AND ANALYSIS

The comparison shows clear differences between the three authentication approaches.

Table 1. *Security comparison of MFA classes across evaluation criteria*

MFA class	Phishing	Relay	Fatigue	Compromised device	Usability	Deployment	Total
TOTP codes	0	0	2	0	1	2	5
Push + number matching	1	1	2	0	2	2	8
WebAuthn / Passkeys	2	2	2	1	2	1	10

Table 2. *Practical interpretation of MFA comparison results*

MFA class	Key strengths	Main limitations
TOTP codes	Simple, widely supported, easy rollout	Vulnerable to phishing and session relay
Push + number matching	Reduces approval mistakes, good usability	Still depends on session/device integrity
WebAuthn / Passkeys	Strongest phishing resistance, origin binding	Deployment and recovery may be harder

As shown in Tables 1 and 2, the three MFA approaches differ in both security properties and practical deployment aspects. TOTP codes are simple and widely supported, which explains why they are still common in many systems. However, they provide limited protection against phishing. Since the user types the code manually into the website, attackers can capture and reuse it in real time if the login page is fake or intercepted. Studies on authentication security note that OTP-based MFA does not fully protect against relay attacks [1].

Push authentication with number matching improves security compared to simple push approval. It requires the user to confirm a number or context, which reduces the risk of accidental approval and makes automated push-spam attacks less effective. Research on modern authentication workflows shows that this kind of intent verification improves usability and decreases user mistakes [7]. At the same time, the method still depends on the security of the active session, so it cannot fully eliminate relay attacks if the session itself is compromised.

WebAuthn and passkey authentication provide the strongest protection among the compared options. These systems rely on asymmetric cryptography and bind credentials to the website origin. This means that credentials cannot be reused on a fake site, which directly addresses the main weakness of OTP-based methods. Analyses of WebAuthn and FIDO implementations confirm that public-key authentication significantly improves phishing resistance compared to traditional MFA approaches [5], [6]. This also corresponds to the NIST definition of higher-assurance authentication mechanisms [2].

From the usability side, OTP methods remain the easiest to deploy, push authentication offers a compromise between usability and security, and WebAuthn provides the strongest protection but may require more preparation for rollout and recovery procedures. A simplified decision model for selecting MFA in cloud systems is shown in Figure 1.

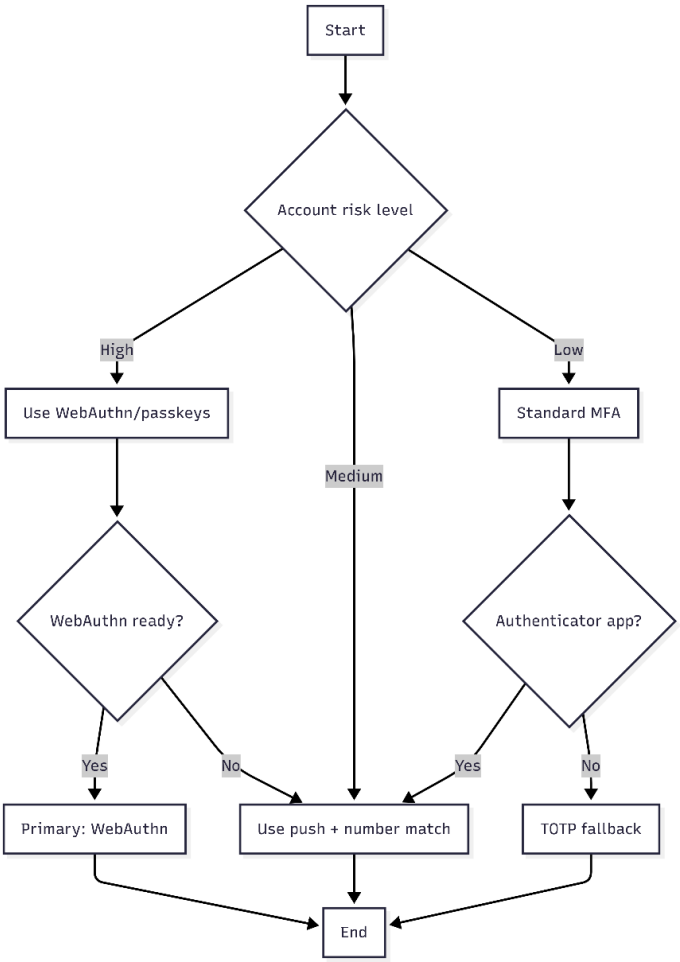


Figure 1. *Decision tree for selecting MFA in cloud applications*

IV. DISCUSSION AND CONCLUSION

The results of this comparison indicate that multi-factor authentication should not be viewed as a single standardized security measure. Instead, different MFA mechanisms demonstrate varying levels of effectiveness depending on the threat model, system sensitivity, and deployment context. Modern cloud environments require authentication approaches that not only increase the number of verification steps but also address specific technical risks such as phishing, session interception, and credential reuse.

Public-key authentication mechanisms, including WebAuthn and passkeys, provide the highest level of technical protection among the compared approaches. Their reliance on asymmetric cryptography and origin-bound credentials makes credential replay significantly more difficult and directly reduces the effectiveness of phishing attacks. Because of these properties, such mechanisms are particularly appropriate for privileged user roles, financial infrastructures, administrative panels, and other services where the potential impact of account compromise is high [3], [5].

Push authentication enhanced with number matching can be considered a practical intermediate solution between basic MFA and fully phishing-resistant authentication. By introducing an explicit confirmation step, this method reduces the probability of accidental approvals and mitigates the impact of push-fatigue attacks. At the same time, it remains relatively simple to deploy in existing organizational environments, which explains why it is often used as a transitional solution in many systems [7].

TOTP-based authentication continues to be widely adopted due to its simplicity, low implementation cost, and compatibility with legacy systems. However, the comparison shows that

such mechanisms should primarily be treated as baseline protection rather than as a complete defense against modern identity-based threats. In environments where higher levels of assurance are required, organizations should gradually transition toward stronger cryptographic authentication mechanisms instead of relying exclusively on code-based verification.

Overall, the findings suggest that selecting an appropriate MFA approach should be guided by both the criticality of the protected resources and the technical readiness of the organization. A structured comparison framework, even a simplified one, can help decision-makers better understand the trade-offs between usability, deployment effort, and security strength. Such an approach also improves transparency in authentication policy decisions and helps justify why different user groups may require different authentication mechanisms within the same system. In addition, the proposed model can serve as a practical starting point for further refinement and empirical validation in real organizational environments. Future research may expand this comparison by incorporating quantitative measurements, user studies, or long-term deployment data. Such extensions would allow a deeper evaluation of how cryptographic MFA mechanisms perform under evolving threat conditions and large-scale cloud adoption.

REFERENCES

1. NIST (2023) Digital Identity Guidelines — Authentication and Lifecycle Management National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.SP.800-63B-4
2. W3C (2021) Web Authentication: An API for accessing Public Key Credentials (WebAuthn) Level 2. World Wide Web Consortium. URL: https://www.w3.org/TR/webauthn-2/
3. Eric B. Blancaflor, Jacob O. Duldulao, John Vincent E. Espeño, Geoff Stephen M. Patag, Ma. Theresa Menor, Grace Lorraine Intal (2025). Advanced Phishing Techniques: Analyzing Adversary-in-the-Middle and Browser-in-the-Browser Attacks in modern cybersecurity. URL: https://cit.iict.bas.bg/CIT-2025/v-25-1/10341-Volume25_Issue_1-04_paper.pdf
4. Manuel Barbosa, Alexandra Boldyreva, Shan Chen, and Bogdan Warinschi (2021). Provable Security Analysis of FIDO2. URL: https://eprint.iacr.org/2020/756.pdf
5. Rivera-Dourado, M., Gestal, M., Pazos, A., & Vázquez-Naya, J. M. (2021). An Analysis of the Current Implementations Based on the WebAuthn and FIDO Authentication Standards. Engineering Proceedings, 7(1), 56. https://doi.org/10.3390/engproc2021007056
6. Jubur, Mohammed, "On the Security and Usability of New Paradigms of Web Authentication" (2021). https://digitalcommons.library.uab.edu/etd-collection/816
7 . Käsemodel, M., Winterhalter, V., Heisel, F., Alt, F., Pfleging, B. (2026). BlueTOTP: Designing Phishing-Resistant and User-Friendly Two-Factor Authentication. https://doi.org/10.1007/978-3-032-05005-2_31
8 .Shirvanian M., Agrawal S. (2021). 2D-2FA: A New Dimension in Two-Factor Authentication. ACSAC Conference. https://dl.acm.org/doi/epdf/10.1145/3485832.3485910
9. Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, Jari Porras, Mitigation Strategies against the Phishing Attacks: A Systematic Literature Review, Computers & Security (2023), https://doi.org/10.1016/j.cose.2023.103387



DAULET ZHUMAT
2nd year student of M.S degree in secure software engineering at Astana IT University
ORCID: 0009-0002-3488-0360
E-mail: daukabai97@gmail.com
Received the B.S degree in oil and gas industry at Almaty, Kazakh-British Technical University in 2024. Currently pursuing M.S degree in secure software engineering at Astana, Astana IT University.

АДАПТИВНІ МЕХАНІЗМИ ПРЕВЕНТИВНОГО ВИЯВЛЕННЯ АНОМАЛІЙ У РОБОТІ ЯДРА LINUX НА ОСНОВІ ТЕХНОЛОГІЇ EBPF

Міхал Аг, Мирослава Гладка

Анотація. *У роботі досліджено підходи до забезпечення безпеки інформаційних систем через призму програмованої обсервабельності ядра Linux. Розглянуто використання технології eBPF (Extended Berkeley Packet Filter) для моніторингу системних викликів у реальному часі без внесення змін у вихідний код ядра. Запропоновано модель виявлення експлуатації вразливостей нульового дня (0-day) шляхом аналізу нетипових послідовностей kprobes та tracepoints, що дозволяє мінімізувати накладні витрати на безпеку при високій швидкодії.*

Ключові слова: кібербезпека, ядро Linux, eBPF, виявлення вторгнень, системні виклики.

I. ВСТУП

У сучасних умовах гібридних загроз традиційні засоби захисту (антивіруси, базові IDS) часто виявляються неефективними проти цілеспрямованих атак (APT), що використовують легітимні інструменти адміністрування.

Особливої актуальності набуває безпека систем на базі Linux, які складають основу хмарних інфраструктур та IoT-мереж. Проблема полягає у тому, що стандартні механізми логування (наприклад, auditd) створюють значне навантаження на CPU при детальному моніторингу.

Метою роботи є розробка архітектури безпеки, яка працює безпосередньо в kernel-space, забезпечуючи максимальну видимість процесів з мінімальною затримкою.

II. ДАНІ ТА МЕТОДИ

Для дослідження обрано технологію eBPF, яка дозволяє запускати перевірений пісочницею (sandbox) код у контексті ядра.

Методика базується на перехопленні системних викликів (syscalls), таких як execve(), memfd_create() та ptrace(), які найчастіше використовуються для підвищення привілеїв та закріплення в системі. Як показано на Рисунку 1, процес моніторингу включає завантаження eBPF-програми, її верифікацію та прикріплення до відповідних точок трасування (hooks).

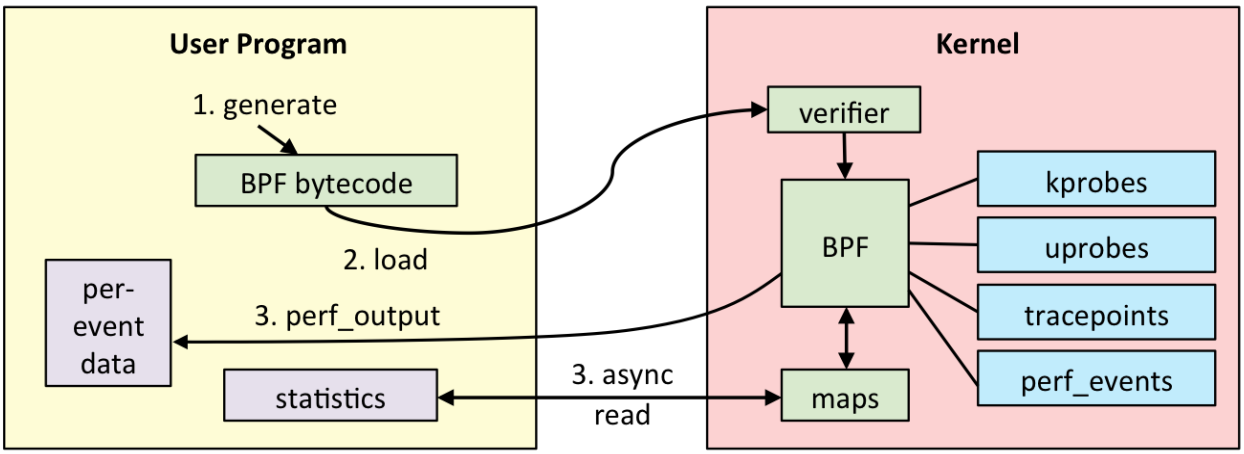


Рисунок 1. *Схема функціонування eBPF-фільтрів у контексті безпеки ядра*

Для кількісного аналізу ефективності ми використовуємо формулу оцінки накладних витрат (overhead) при обробці одного перехопленого пакету:

$$O = \frac{T_{ebpf} - T_{native}}{T_{native}} \times 100\% \quad (1)$$

де T_ebpf - час виконання запиту з активним моніторингом,
T_native - час виконання запиту в штатних умовах.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У ході експериментів було порівняно продуктивність eBPF-рішень (на кшталт Tetragon або Falco) із класичним auditd. Результати наведено в Таблиці 1.

Таблиця 1. *Порівняння засобів моніторингу системних подій*

Параметр	**Auditd**	**eBPF**
Навантаження на CPU (%)	12-15%	1.5-3%
Можливість блокування (inline)	Обмежена	Повна (через LSM hooks)
Стійкість до обходу (bypass)	Низька	Висока

Аналіз показав, що eBPF дозволяє виявляти аномалії, такі як спроба виконання коду з анонімної пам'яті (fileless malware), що є критичним для захисту сучасних систем.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведене дослідження підтверджує, що впровадження низькорівневої обсервабельності на базі eBPF дозволяє фундаментально змінити парадигму забезпечення безпеки Linux-систем - від реактивного логування до превентивного виявлення та блокування загроз у реальному часі. На відміну від класичних інструментів моніторингу, які працюють на рівні користувача, запропонований підхід забезпечує глибоку видимість операцій ядра без необхідності внесення змін у його вихідний код або перекомпіляції модулів.

Однією з ключових переваг є використання eBPF Maps як високопродуктивного механізму передачі структурованих даних між простором ядра (kernel-space) та прикладним ПЗ (user-space). Це дозволяє виносити складні обчислення та кореляційний аналіз аномалій за межі критичних шляхів виконання ядра, що гарантує стабільність системи та нівелює ризики виникнення критичних помилок (Kernel Panic). Верифікатор байт-коду (Verifier) виступає додатковим рівнем безпеки, гарантуючи, що завантажені програми моніторингу не призведуть до зациклення або несанкціонованого доступу до пам'яті.

Результати порівняльного аналізу (див. Таблицю 1) демонструють значну перевагу eBPF над стандартним підсистемами аудиту (наприклад, auditd), особливо в умовах високого мережевого навантаження. Зниження накладних витрат на CPU з 12-15% до 1.5-3% відкриває можливості для розгортання повноцінних систем виявлення вторгнень (IDS) навіть на пристроях з обмеженими ресурсами (Edge-computing та IoT).

Перспективи подальших досліджень полягають у розробці та інтеграції компактних моделей машинного навчання безпосередньо в eBPF-байткод. Це дозволить реалізувати інтелектуальну фільтрацію трафіку та системних подій на рівні L2/L3 моделей OSI без затримок, пов'язаних із копіюванням даних у простір користувача. Такий підхід дозволить

автоматично ідентифікувати складні патерни атак, такі як повільне сканування портів або експлуатація вразливостей нульового дня, безпосередньо в момент їх виникнення.

ДЖЕРЕЛА

1. Grehan D., Moore A. (2021) Linux Observability with BPF. O'Reilly Media.
2. Rice L. (2023) Learning eBPF: Programming the Linux Kernel for Observability and Networking. O'Reilly Media.
3. Huang, K., Payer, M., Qian, Z., Sampson, J., Tan, G. and Jaeger, T. 2025, 'Sok: Challenges and paths toward memory safety for ebpf', in 2025 IEEE Symposium on Security and Privacy (SP), IEEE, pp. 848-866.
4. Lim, S. Y., Prasad, T., Han, X. and Pasquier, T. (2024) ‘Safebpf: Hardware-assisted defense-in-depth for ebpf kernel extensions’, in Proceedings of the 2024 on Cloud Computing Security Workshop. [Online]. New York, NY, USA: Association for Computing Machinery. pp. 80–94.
5. Hadi, H. J., Adnan, M., Cao, Y., Hussain, F. B., Ahmad, N., Alshara, M. A. and Javed, Y. (2024) ‘ikern: Advanced intrusion detection and prevention at the kernel level using ebpf’, Technologies, 12(8), p. 122.
6. Anand, N., Saifulla, M. A. and Aakula, P. K. (2023) ‘High-performance intrusion detection system using eBPF with machine learning algorithms’, in 2023 7th International Conference on Computing Methodologies and Communication (ICCMC). IEEE, pp. 263–269.
7. Хрущак, С. В., О. Р. Бойко, and М. Ю. Терьохіна. "Безпековий моніторинг інформаційних систем за допомогою eBPF." Наука і техніка сьогодні. (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка») 2024.№ 4 (32). С. 1251-1262. DOI: https://doi. org/10.52058/2786-6025-2024-4 (32).



МІХАЛ АГ
студент 1 курсу бакалаврату технологій веброзробки та вебдизайну у Київському національному університеті імені Тараса Шевченка.
E-mail: mihal_ag@knu.ua
Наукові інтереси охоплюють сферу кібербезпеки Linux-систем, проєктування низькорівневих механізмів обсервабельності за допомогою eBPF та методології тестування на проникнення (pentesting). Спеціалізується на розробці високопродуктивних архітектур вебзастосунків на базі JavaScript/TypeScript та дослідженні інтелектуальних методів аналізу системних викликів для превентивного виявлення аномалій у критичній інфраструктурі.



МИРОСЛАВА ГЛАДКА
к.т.н., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-5233-2021
E-mail: myroslava.gladka@knu.ua
Досвід практичної роботи понад 10 років. Коло наукових інтересів: управління проєктами, моделювання та інжиніринг бізнес-процесів.

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА РАДІОТЕХНІЧНОГО МОНІТОРИНГУ

Віталій Андрійчук, Юлій Бойко, Леся Карпова

Анотація. *Розглянуто систему радіотехнічного моніторингу для виявлення малорозмірних БПЛА на дальностях до 2,5 км. Обґрунтовано структурну побудову та параметри антенної підсистеми з електронним скануванням. Використано фазокодований сигнал із кодом Баркера для підвищення завадостійкості та покращення співвідношення сигнал/шум. На основі радіолокаційного рівняння оцінено залежність дальності виявлення від ефективної площі розсіювання цілі. Результати моделювання підтверджують енергетичну достатність і практичну реалізованість запропонованої системи.*

Ключові слова: радіотехнічний моніторинг, антена, радіолокаційне рівняння, дальність виявлення, система, БПЛА.

I. ВСТУП

Сучасний розвиток безпілотних літальних апаратів (БПЛА) зумовлює необхідність створення ефективних систем контролю повітряного простору на малих та середніх дальностях. Активне використання БПЛА у цивільній, комерційній та військовій сферах підвищує ризики несанкціонованого проникнення у зони обмеженого доступу, що потребує впровадження технічних засобів своєчасного виявлення та локалізації таких об’єктів. Особливо актуальними є системи, здатні функціонувати в умовах складної радіоелектронної обстановки, міської забудови та наявності інтенсивних завад [1, 2].

Особливої актуальності набувають системи радіотехнічного моніторингу, які дозволяють здійснювати виявлення, аналіз та ідентифікацію радіооб’єктів як у пасивному, так і в активному режимах функціонування. Пасивний режим забезпечує контроль каналів керування та телеметрії, тоді як активний режим дозволяє визначати дальність і просторові координати об’єкта за рахунок зондування простору. Поєднання цих режимів розширює функціональні можливості системи та підвищує достовірність прийняття рішення [3].

Перевагою систем радіотехнічного моніторингу є можливість інтеграції просторової селекції сигналів, спектрального аналізу та цифрової кореляційної обробки. Використання фазованих антенних решіток [2] із електронним скануванням дозволяє формувати керовану діаграму спрямованості, зменшувати рівень бічних пелюсток і підвищувати завадостійкість [4]. Застосування фазокодованих сигналів та алгоритмів кореляційної обробки забезпечує енергетичний виграш і покращення співвідношення сигнал/шум при виявленні малорозмірних цілей з малою ефективною площею розсіювання.

Метою роботи є проєктування системи радіотехнічного моніторингу [5] для виявлення БПЛА на дальностях до 2,5 км, обґрунтування основних технічних параметрів антенної та приймально-передавальної підсистем, а також аналіз ефективності запропонованої структури на основі математичного моделювання та енергетичних розрахунків.

II. ДАНІ ТА МЕТОДИ

Для досягнення поставленої мети виконано структурно-функціональний аналіз системи радіотехнічного моніторингу, проведено енергетичні розрахунки на основі радіолокаційного рівняння, а також застосовано методи математичного моделювання та цифрової обробки сигналів. Особливу увагу приділено формуванню антенної підсистеми, оцінюванню чутливості приймального тракту та аналізу ефективності кореляційної обробки фазокодованих сигналів.

Структурна побудова системи радіотехнічного моніторингу визначається її функціональним призначенням: прийманням, селекцією, перетворенням, цифровою обробкою та відображенням радіосигналів у заданому частотному діапазоні. Узагальнена структурна схема запропонованої системи наведена на рисунку 1.

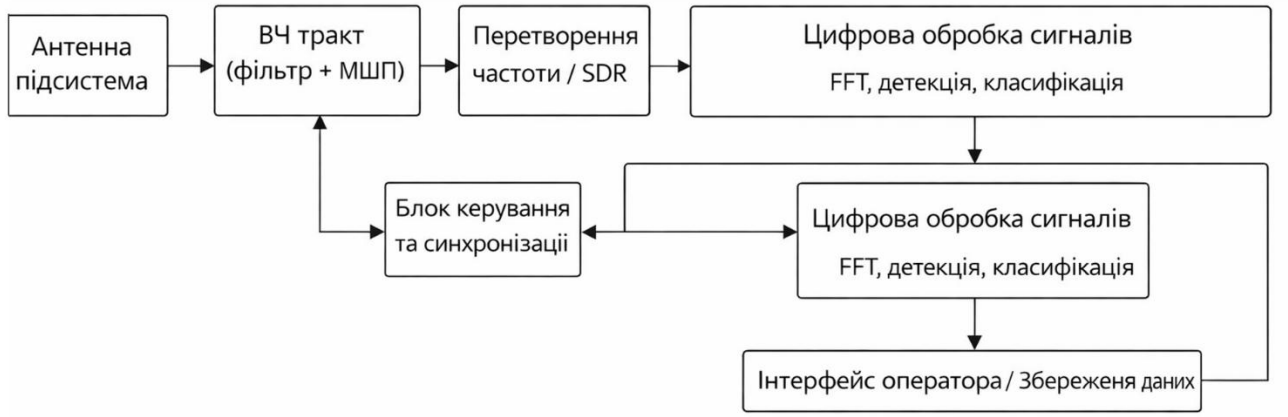


Рисунок 1. *Структурна схема системи радіотехнічного моніторингу*

Структурна організація системи радіотехнічного моніторингу реалізується через послідовність функціональних етапів, що включають приймання сигналів, їх попередню селекцію та підсилення, подальше перетворення частоти або SDR-оцифрування, аналого-цифрове перетворення, цифрову обробку, а також відображення та збереження отриманої інформації. Антенна підсистема здійснює приймання електромагнітних хвиль у заданому діапазоні частот. У ВЧ тракті виконуються фільтрація позасмугових сигналів та попереднє підсилення малошумовим підсилювачем, що забезпечує необхідну чутливість системи. Далі сигнал надходить до блоку перетворення частоти або SDR-модуля, де формується сигнал, придатний для подальшого оцифрування.

Після аналого-цифрового перетворення сигнал обробляється у цифровому блоці, де виконуються спектральний аналіз, детекція, оцінювання співвідношення сигнал/шум та класифікація джерел випромінювання. Блок керування та синхронізації забезпечує узгоджену роботу функціональних модулів та формує необхідні режими сканування.

В активному режимі дальність до об’єкта визначається часовим методом, який ґрунтується на вимірюванні інтервалу часу між моментом випромінювання зондувального сигналу та прийманням його відбиття від цілі. Розрахунок дальності здійснюється відповідно до формули 1.

$$R = \frac{c\tau}{2}, \tag{1}$$

де c – швидкість поширення електромагнітної хвилі,

τ – затримка відбитого сигналу.

У пасивному режимі рішення про наявність джерела випромінювання приймається за критерієм перевищення рівня сигналу над шумом (SNR).

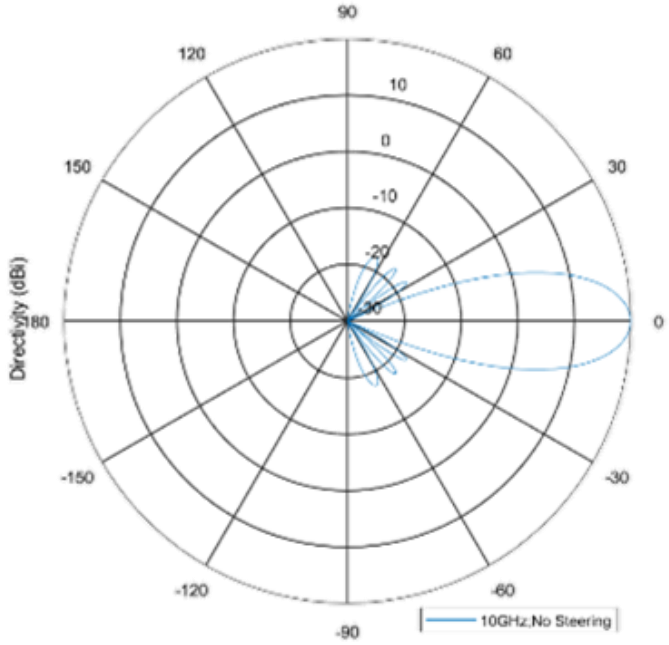
Для підвищення завадостійкості та збереження роздільної здатності використано фазокодований радіоімпульс із кодом Баркера довжиною $N = 13$, що забезпечує низький рівень бокових пелюсток автокореляційної функції та енергетичний виграш після кореляційної обробки. Просторова селекція сигналів реалізується за допомогою антенної решітки з електронним скануванням та амплітудним зважуванням (вікно Хемінга), що забезпечує зменшення рівня бічних пелюсток діаграми спрямованості.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

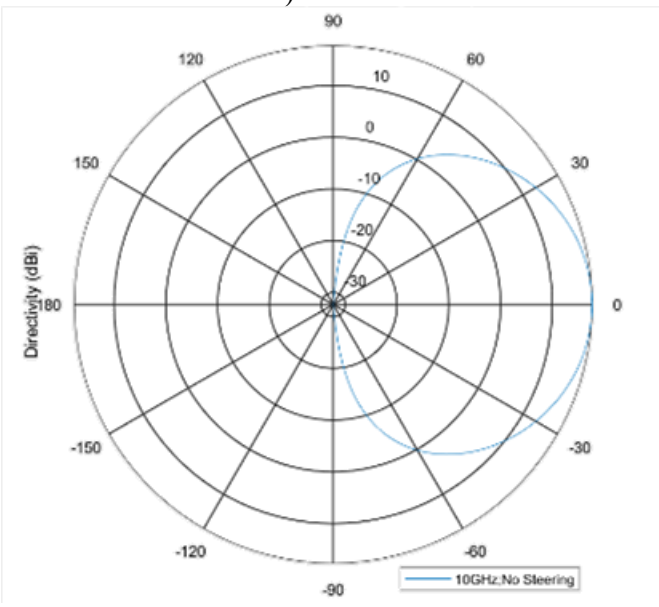
Антенна підсистема системи радіотехнічного моніторингу призначена для приймання сигналів у заданому діапазоні частот, просторової селекції радіовипромінювань та визначення напрямку на джерело сигналу. Основною вимогою є формування вузької діаграми спрямованості в Н-площині для забезпечення високої кутової роздільної здатності та розширеної діаграми в Е-площині для покриття зони контролю за висотою.

У результаті моделювання антенної системи отримано коефіцієнт підсилення 17,7 дБ, що відповідає вимогам до дальності виявлення та просторової селекції цілей. Амплітудний розподіл збудження елементів уздовж апертури сформовано за законом віконної функції Хемінга, що дозволило знизити рівень бічних пелюсток та підвищити завадостійкість системи.

На рисунку 2, а наведено діаграму спрямованості в Н-площині.



а)



б)

Рисунок 2. *Діаграми спрямованості антени в Н- та Е-площинах*

Ширина головної пелюстки за рівнем −3 dB становить 12°, що забезпечує необхідну кутову роздільну здатність під час визначення напрямку на об'єкт. На рисунку 2, б представлено діаграму спрямованості в Е-площині. Її ширина становить близько 60°, що забезпечує покриття зони контролю за висотою та підвищує ймовірність виявлення цілі в межах робочого сектора.

Таким чином, поєднання вузької діаграми спрямованості в Н-площині та розширеної діаграми в Е-площині забезпечує оптимальний баланс між кутовою роздільною здатністю та повнотою просторового контролю.

Для оцінювання можливостей запропонованої системи використано класичне радіолокаційне рівняння дальності, яке визначається формулою 2:

$$R = \sqrt[4]{\frac{P_{pr}G^2\sigma\lambda^2}{(4\pi)^3 P_{pr.min}}} \quad (2)$$

де P_{pr}– потужність передавача,

G– коефіцієнт підсилення антени (17,7 дБ),

σ – ефективна площа розсіювання цілі,

λ – довжина хвилі,

$P_{pr.min}$ – мінімальна приймальна потужність.

Розрахунки показали, що для БПЛА з ефективною площею розсіювання 0,1 м² забезпечується дальність виявлення до 2,5 км, тоді як для малорозмірних цілей з ЕПР 0,01 м² дальність становить близько 1,4 км. Отримані результати підтверджують характер залежності $R \sim \sigma^{1/4}$, тобто навіть при істотному зменшенні ЕПР дальність зменшується відносно повільно, що свідчить про достатній енергетичний потенціал системи.

Для підвищення завадостійкості використано фазокодований радіоімпульс із кодом Баркера довжиною $N = 13$. Нормована автокореляційна функція такого сигналу характеризується низьким рівнем бокових пелюсток (близько −11 dB), що зменшує ймовірність хибних спрацьовувань у присутності шумів і завад.

Після проходження сигналу через оптимальний фільтр відбувається імпульсне стиснення. У результаті кореляційної обробки амплітуда головного максимуму зростає приблизно у N разів, покращується співвідношення сигнал/шум та підвищується точність визначення дальності.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати підтверджують, що запропонована архітектура системи радіотехнічного моніторингу з цифровою обробкою та застосуванням фазокодованих сигналів є практично реалізованою для задач виявлення малорозмірних БПЛА на дальностях до 2,5 км за умови коректного узгодження енергетичного потенціалу, чутливості приймального тракту та параметрів антенної системи. Використання коду Баркера довжиною N=13 забезпечує енергетичний виграш після кореляційної обробки та зменшує вплив шумів і завад, а антена з електронним скануванням підвищує швидкодію та точність просторової селекції.

Подальший розвиток роботи доцільно спрямувати на експериментальну перевірку на реальних сигналах, оцінювання стійкості до активних завад і розширення функцій класифікації у межах SDR-підходу.

Запропонований підхід може слугувати основою для створення адаптивних інтелектуальних систем моніторингу повітряного простору з можливістю масштабування, інтеграції в мережеві комплекси безпеки та застосування в умовах підвищеної радіоелектронної протидії.

ДЖЕРЕЛА

1. Boiko, J., & Karpova, L. (2023). Increasing efficiency in the correlation processing of information signals for radar. In Proceedings of Fourth International Conference on Communication, Computing and Electronics Systems (Lecture Notes in Electrical Engineering, Vol. 977, pp. 549–569). Springer.
2. Boiko, J., Polıkarovskykh, O., Tkachuk, V., Yehoshyna, H., & Karpova, L. (2023). Design concepts for mobile computing direction finding systems. In Mobile Computing and Sustainable Informatics (Lecture Notes on Data Engineering and Communications Technologies, Vol. 166, pp. 89–107). Springer.
3. Boiko, J., Pyatin, I., Eromenko, O., & Karpova, L. (2025). Optimization of Cartesian feedback loops for wideband SDR transmitters in 5G mobile networks. Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia, (100), 27–42.
4. Polikarovskykh, O. I., Kovtun, L. O., Karpova, L. V., Gula, I. V., & Melnychuk, V. M. (2019). Using of residual number systems as mathematical basis for software defined radio. Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia, (76), 21–28.
5. Sumithra, M. G., & Suriya, M. (2024). Improved spectrum prediction model for cognitive radio networks using hybrid deep learning technique. Internat.Journal of Intelligent Networks, 5, 286–292.



ВІТАЛІЙ АНДРІЙЧУК
Здобувач ступеню бакалавра з електронних комунікацій та радіотехніки, група ЕКРс-23-1, у Хмельницькому національному університеті.
E-mail: boiko_julius@ukr.net
Наукові інтереси: радіотехнічні системи спостереження та виявлення, обробка сигналів у складній завадовій обстановці, цифрові методи аналізу спектра, програмно-конфігуровані радіосистеми, підвищення завадостійкості телекомунікаційних каналів.



ЮЛІЙ БОЙКО
д.т.н., професор, професор кафедри телекомунікацій, медійних та інтелектуальних технологій, Хмельницький національний університет.
ORCID:0000-0003-0603-7827
E-mail: boykoym@khmnu.edu.ua
Наукові інтереси: обробка сигналів, синхронізація, телекомунікації, кодування, електронні компоненти, діагностика, інформаційні системи.



ЛЕСЯ КАРПОВА
к.т.н., доцент, доцент кафедри телекомунікацій, медійних та інтелектуальних технологій, Хмельницький національний університет.
ORCID ID: 0000-0001-5015-2107
E-mail: rtlesya@gmail.com
Наукові інтереси: телекомунікації, електронні компоненти, проєктування та оптимізація радіотехнічних систем, бездротова передача даних, антенні системи.

СТІЙКІ ПІДХОДИ ДО ПОБУДОВИ ZERO TRUST АРХІТЕКТУР У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Микита Гришко, Інна Розломій

Анотація. *У роботі досліджено стійкі підходи до побудови архітектур Zero Trust у розподілених інформаційних системах. Проаналізовано сучасні загрози, пов'язані з використанням хмарних сервісів, мікросервісної архітектури та віддаленого доступу. Запропоновано модель впровадження Zero Trust із застосуванням принципів мінімальних привілеїв, мікросегментації, багатофакторної автентифікації та безперервного моніторингу. Обґрунтовано переваги інтеграції політик динамічного контролю доступу для підвищення кіберстійкості організацій.*

Ключові слова: Zero Trust; розподілені системи; кібербезпека; мікросегментація; контроль доступу.

I. ВСТУП

Цифрова трансформація, розвиток хмарних технологій та поширення віддаленої роботи суттєво змінили модель функціонування інформаційних систем. Традиційна периметрова модель безпеки, що базується на довірі до внутрішньої мережі, виявилася недостатньо ефективною в умовах сучасних кіберзагроз.

Концепція Zero Trust передбачає відсутність автоматичної довіри до будь-якого користувача або пристрою незалежно від їх розташування в мережі. Основний принцип моделі формулюється як «ніколи не довіряти, завжди перевіряти». У розподілених інформаційних системах, де ресурси розміщуються в різних сегментах мережі та хмарних середовищах, впровадження Zero Trust є стратегічно важливим для забезпечення стійкості та безперервності функціонування.

Метою дослідження є визначення стійких підходів до побудови Zero Trust архітектур у розподілених інформаційних системах та формування практичних рекомендацій щодо їх впровадження.

II. ДАНІ ТА МЕТОДИ

Дослідження ґрунтується на аналізі сучасних стандартів кібербезпеки, рекомендацій міжнародних організацій та наукових публікацій останніх років. Було використано методи системного аналізу, моделювання архітектурних рішень та порівняльного оцінювання підходів до захисту інформації.

Основні компоненти Zero Trust архітектури включають:

- багатофакторну автентифікацію (MFA);
- принцип мінімальних привілеїв (Least Privilege);
- мікросегментацію мережі;
- безперервний моніторинг та аналіз поведінки;
- централізоване управління політиками доступу.

У межах роботи запропоновано структурну модель впровадження Zero Trust для розподіленої системи, яка включає такі етапи:

1. Ідентифікація критичних активів та потоків даних.
2. Класифікація користувачів і сервісів.
3. Впровадження політик умовного доступу.
4. Інтеграція систем виявлення аномалій.

5. Постійна оцінка ризиків і коригування політик безпеки.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Запропонована модель Zero Trust базується на безперервному аналізі контексту доступу та динамічному застосуванні політик безпеки. Основна ідея полягає у тому, що кожен запит до ресурсу розглядається як потенційно недовірений.

Як показано на схемі, архітектура складається з трьох ключових рівнів:

- користувачі та пристрої;
- механізми контролю безпеки;
- інформаційні ресурси.

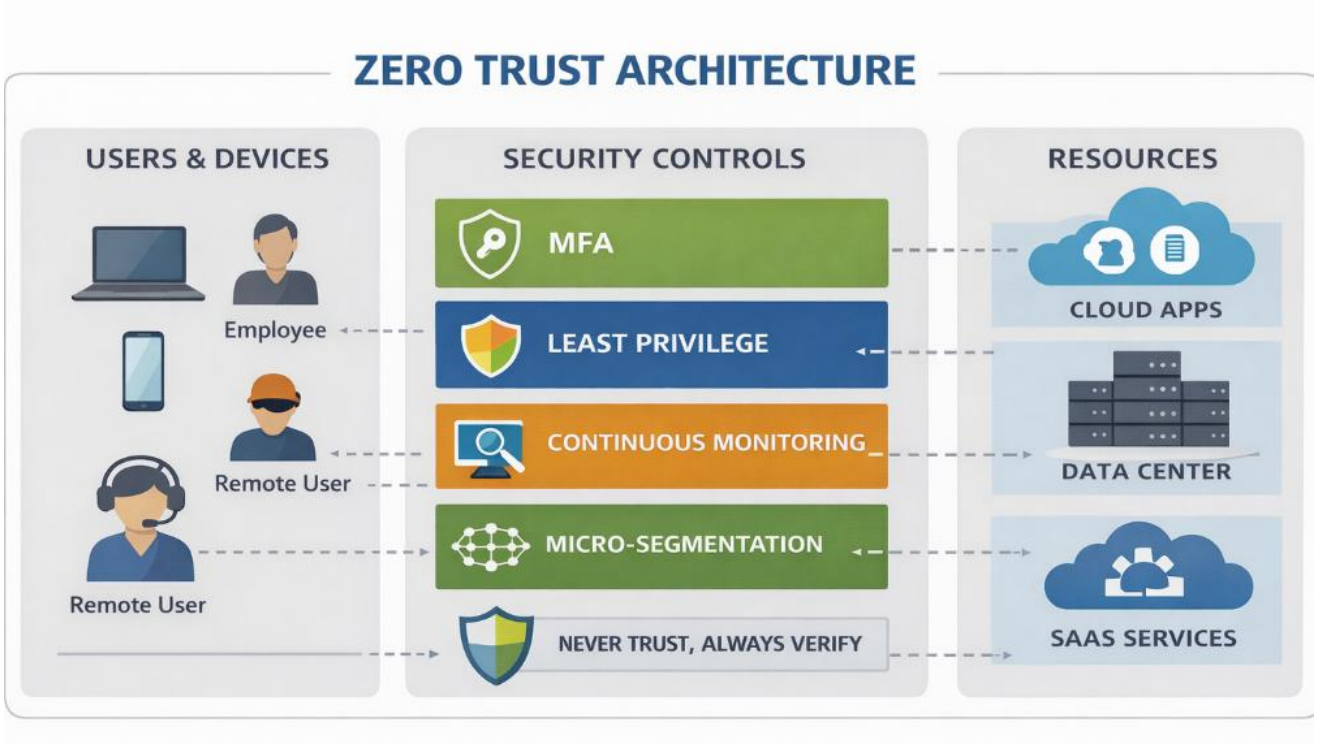


Рисунок 1. *Модель Zero Trust архітектури у розподіленій системі.*

Використання мікросегментації дозволяє локалізувати потенційні інциденти безпеки, а застосування принципу мінімальних привілеїв мінімізує ризик компрометації системи.

Отримані результати демонструють, що впровадження Zero Trust підвищує контроль над доступом та забезпечує більш ефективне реагування на кіберінциденти.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

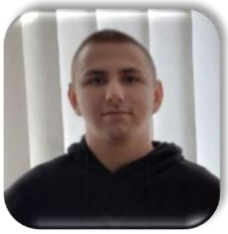
У роботі обґрунтовано необхідність переходу від периметрової моделі безпеки до концепції Zero Trust у розподілених інформаційних системах. Визначено ключові складові стійкої архітектури, зокрема мікросегментацію, багатофакторну автентифікацію, безперервний моніторинг та адаптивне управління доступом.

Запропонована модель впровадження дозволяє підвищити рівень кіберстійкості організацій, мінімізувати вплив внутрішніх та зовнішніх загроз і забезпечити безпечну інтеграцію хмарних сервісів.

Подальші дослідження можуть бути спрямовані на розробку автоматизованих механізмів оцінювання зрілості Zero Trust архітектур та їх інтеграцію з системами штучного інтелекту для прогнозування кіберінцидентів.

ДЖЕРЕЛА

1. Rose S., Borchert O., Mitchell S., Connelly S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. Journal of Computer and Communications, Vol.12 No.3, March 29, 2024 https://doi.org/10.6028/nist.sp.800-207
2. Kindervag J. (2021). No More Chewy Centers: Introducing The Zero Trust Model of Information Security. Forrester Research. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security For Security & Risk Professionals. September 17, 2010
3. Chen L., Liu Y. (2022). Zero Trust Security Model in Cloud Computing Environments. IEEE Access. DOI: 10.1186/s42400-024-00320-x
4. Ahmad, A., Maynard, S. B., & Park, S. (2019). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent & Fuzzy Systems, 36(5), 4625–4636.
5. Kumar R., Mishra P. (2024). Micro-Segmentation Strategies in Modern Enterprise Networks. Journal of Network Security.
6. Santra J. Leveraging ServiceNow and Cloud Architectures for Seamless Integration of DevSecOps in Enterprise Environments. IJETCSIT [Internet]. 2025 May 18 [cited 2026 Mar. 17];:448-5. Available from: https://ijetcsit.org/index.php/ijetcsit/article/view/286



МИКИТА ГРИШКО
студент 3 курсу бакалаврату кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
E-mail: m.s.hryshko.fitis23@chdtu.edu.ua
Науковий інтерес полягає у вивченні та дослідженні IoT-систем моніторингу та контролю, а також практичному застосуванні IoT-технологій у сучасних інформаційних системах.



ІННА РОЗЛОМІЙ
к.т.н., доцент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
ORCID: 0000-0003-2062-2694
E-mail: inna-roz@ukr.net
Отримала ступінь магістра із спеціалізованих комп'ютерних систем у 2014 році у Київському національному університеті технологій та дизайну. Кандидат технічних наук з 2019. Доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету. Наукові інтереси: Інтернет речей, полегшена криптографія, кіберфізичні системи. Автор/співавтор понад 150 публікацій, 5 монографій та 2 патентів.

СУЧАСНІ ЗАГРОЗИ БЕЗПЕЦІ IOT У СКЛАДІ КІБЕРФІЗИЧНИХ ТА КРИТИЧНИХ СИСТЕМ

Дарина Джирма, Інна Розломій

Анотація. *У роботі розглянуто сучасні загрози безпеці Інтернету речей (IoT), що функціонують у складі кіберфізичних систем та об'єктів критичної інфраструктури. Проаналізовано основні типи атак на IoT-пристрої та їх вплив на енергетичні, транспортні й промислові системи. Визначено ключові вразливості архітектури IoT і запропоновано комплексний підхід до забезпечення кіберстійкості на основі сегментації мереж, криптографічного захисту та інтелектуального моніторингу.*

Ключові слова: IoT, кіберфізичні системи, критична інфраструктура, кіберзагрози, моніторинг, інформаційна безпека.

I. ВСТУП

Стрімкий розвиток Інтернету речей (IoT) зумовив його активну інтеграцію у кіберфізичні системи (CPS) та об'єкти критичної інфраструктури: енергетику, транспорт, промисловість і медицину. IoT-пристрої забезпечують безперервний збір, передавання й обробку даних у реальному часі, що дозволяє автоматизувати управління фізичними процесами та підвищити ефективність функціонування складних систем.

Разом із тим збільшення кількості підключених пристроїв розширює поверхню атаки. Вразливості прошивок, недостатній контроль доступу, слабка автентифікація та відсутність належного шифрування створюють передумови для реалізації кібератак [1].

У випадку критичних систем такі інциденти можуть спричинити не лише інформаційні втрати, але й фізичні наслідки.

II. ДАНІ ТА МЕТОДИ

Дослідження ґрунтується на аналізі сучасних наукових публікацій і звітів щодо безпеки IoT [1–3]. Було проведено систематизацію загроз та їх класифікацію за механізмом реалізації.

Основні групи загроз включають:

- мережеві атаки (DDoS, MITM, spoofing);
- шкідливе програмне забезпечення (зокрема ботнети типу Mirai);
- атаки на прошивки та апаратні компоненти;
- компрометацію хмарної інфраструктури;
- експлуатацію вразливостей протоколів MQTT і CoAP.

Узагальнену архітектуру IoT у складі кіберфізичної системи наведено на Рисунку 1.

Архітектура включає рівень сенсорів, шлюзовий рівень, хмарну платформу, центр управління та фізичний об'єкт. Кожен із цих рівнів може бути потенційною точкою реалізації загроз.



Рисунок 1. *Узагальнена архітектура IoT у складі кіберфізичної системи*

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз показав, що найбільшу небезпеку становлять атаки, спрямовані на порушення доступності та цілісності даних. Як показано в Таблиці 1, реалізація таких загроз може призвести до серйозних наслідків для функціонування CPS.

Таблиця 1. *Основні загрози безпеці IoT у критичних системах*

№	Тип загрози	Наслідки для CPS
1	DDoS-атаки	Порушення доступності сервісів
2	Перехоплення трафіку	Компрометація конфіденційних даних
3	Підміна пристроїв	Некоректне керування фізичними процесами
4	Атаки на прошивку	Повний контроль над пристроєм
5	Внутрішні загрози	Несанкціонований доступ до систем управління

Особливістю IoT у CPS є тісна інтеграція цифрових і фізичних компонентів. На відміну від традиційних IT-систем, порушення кібербезпеки може спричинити матеріальні збитки або створити загрозу для життя людей [2].

Для мінімізації ризиків доцільно впроваджувати багаторівневу модель захисту, що передбачає сегментацію мереж, застосування принципів Zero Trust, використання TLS та IPSec, багатофакторну автентифікацію та інтелектуальні системи виявлення аномалій.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

IoT у складі кіберфізичних і критичних систем є важливим елементом цифрової трансформації, однак водночас створює нові ризики.

Основними проблемами залишаються низький рівень стандартизації, обмежені обчислювальні ресурси пристроїв та людський фактор.

Підвищення кіберстійкості можливе лише за умови комплексного поєднання технічних, організаційних і нормативних заходів.

Перспективним напрямом є використання технологій штучного інтелекту для проактивного виявлення аномалій та прогнозування атак.

Забезпечення безпеки IoT у критичній інфраструктурі є стратегічним завданням держави, оскільки від цього залежить стабільність функціонування суспільства та національна безпека.

ДЖЕРЕЛА

1. Conti M., Dehghantanha A., Franke K., Watson S. (2020). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems.
2. Neshenko N., Bou-Harb E., Crichigno J., Kaddoum G., Ghani N. (2021). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and Internet-scale exploitations. IEEE Communications Surveys & Tutorials.
3. Alaba F.A., Othman M., Hashem I.A., Alotaibi F. (2022). Internet of Things security: A survey. Journal of Network and Computer Applications.
4. ENISA (2023). ENISA Threat Landscape 2023. Threat Landscape for IoT. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001



ДАРИНА ДЖИРМА
студентка 3 курсу бакалаврату кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
E-mail: d.v.dzhyrma.fitis23@chdtu.edu.ua
Науковий інтерес полягає у вивченні та дослідженні сучасних інформаційних технологій, зокрема IoT-систем моніторингу та контролю, а також практичному застосуванні IoT-технологій у різних сферах інформаційних систем.



ІННА РОЗЛОМІЙ
к.т.н., доцент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
ORCID: 0000-0003-2062-2694
E-mail: inna-roz@ukr.net
Отримала ступінь магістра із спеціалізованих компютерних систме у 2014 році у Київському національному університеті технологій та дизайну. Кандидат технічних наук з 2019. Доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету. Наукові інтереси: Інтернет речей, полегшена криптографія, кіберфізичні системи. Автор/співавтор понад 150 публікацій, 5 монографій та 2 патентів.

МЕТОДИ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Анна Квятковська

Анотація. *У процесі дослідження авторами встановлено основні вразливості програмно-визначених мереж у середовищі Інтернету речей та визначено ефективні методи підвищення їх інформаційної безпеки. Зазначено, що інтеграція сегментації мережі, багаторівневої автентифікації, криптографічного захисту та систем виявлення аномалій забезпечує комплексний підхід до протидії кіберзагрозам. Актуальність визначається зростанням кількості IoT-пристроїв та підвищенням ризиків атак у цифрових інфраструктурах. Зроблені висновки про доцільність використання програмованих механізмів автоматизації безпеки.*

Ключові слова: *програмно-визначені мережі; Інтернет речей; інформаційна безпека; криптографічний захист; контроль доступу.*

I. ВСТУП

У сучасних умовах цифрової трансформації мережевої інфраструктури питання інформаційної безпеки програмно-визначених мереж (Software-Defined Networking, SDN) набуває особливої актуальності, зважаючи на стрімке зростання кількості підключених пристроїв Інтернету речей (IoT). Стабільність і захищеність IoT-середовищ більше не розглядаються як другорядні технічні аспекти, а виступають ключовими чинниками функціонування критично важливих інфраструктур, промислових систем та міських сервісів. Значні обсяги чутливих даних — включно з геолокаційною інформацією, біометричними параметрами користувачів, комерційними та виробничими показниками — передаються через мережеві середовища, що підвищує вимоги до механізмів їх захисту. Розвиток Інтернету речей суттєво ускладнює архітектуру мереж і збільшує площу потенційної атаки. Уразливості пристроїв, неналежна автентифікація або компрометація каналів передачі даних можуть призводити до масштабних кіберінцидентів, втрати довіри користувачів, фінансових збитків і порушення функціонування розподілених систем управління. Окрім економічних ризиків, порушення безпеки IoT-екосистем може спричинити підвищення енергоспоживання, зростання експлуатаційних витрат та негативні екологічні наслідки. У цьому контексті програмно-визначені мережі, що характеризуються централізованим управлінням і відокремленням площини керування від площини передачі даних, створюють нові можливості для впровадження адаптивних механізмів контролю доступу, сегментації трафіку та криптографічного захисту інформації. Одним із ключових напрямів підвищення рівня безпеки є мережеве сегментування, яке дозволяє ізолювати IoT-пристрої, мінімізувати ризики поширення атак та забезпечити контрольований доступ до ресурсів.

Узагальнюючи зазначимо, що інтеграція технологій Інтернету речей у програмно-визначені мережі потребує розроблення комплексних методів захисту, що поєднують шифрування, багаторівневу автентифікацію, динамічний моніторинг трафіку та інтелектуальні механізми виявлення загроз.

II. ДАНІ ТА МЕТОДИ

Джерельною базою дослідження стали наукові публікації з проблематики інформаційної безпеки програмно-визначених мереж, архітектур Інтернету речей, стандарти та рекомендації міжнародних організацій у сфері кібербезпеки, а також аналітичні матеріали

щодо сучасних моделей загроз у SDN-IoT середовищах. Опрацьовано результати досліджень, присвячених вразливостям площини керування, механізмам автентифікації IoT-пристроїв, протоколам шифрування та системам виявлення вторгнень. Методологічну основу роботи становлять загальнонаукові методи аналізу та синтезу, що дозволили систематизувати існуючі підходи до забезпечення інформаційної безпеки в SDN та визначити їх релевантність у контексті інтеграції технологій IoT. Застосовано метод порівняльного аналізу для зіставлення традиційних мережевих механізмів захисту з архітектурно-орієнтованими рішеннями, притаманними SDN. Застосовано метод концептуального моделювання для формування узагальненої моделі інтегрованої системи захисту SDN-IoT, яка включає механізми сегментації, динамічного контролю доступу, криптографічного захисту та моніторингу мережевої активності. Логіко-теоретичний аналіз дозволив сформулювати узгоджену систему методів підвищення інформаційної безпеки, орієнтовану на мінімізацію ризиків централізації керування та масштабованості IoT-середовищ.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Архітектура SDN передбачає відокремлення площини керування (control plane) від площини передачі даних (data plane). Аналіз наукових досліджень [1;2;3] дозволяє зробити висновки, що ризики пов’язані з:

- централізованим SDN-контролером як критичною точкою відмови;
- перехопленням або модифікацією потоків OpenFlow;
- несанкціонованим підключенням IoT-пристроїв;
- DDoS-атаками на контрольну площину;
- відсутністю стандартизованих механізмів автентифікації пристроїв IoT.

IoT-середовища додатково ускладнюють модель загроз через масштабність, гетерогенність та фізичну доступність кінцевих пристроїв.

Програмно-визначені мережі забезпечують централізований і програмно-керований підхід до управління мережевою інфраструктурою, що значно підвищує її гнучкість, масштабованість і адаптивність до потреб сучасних бізнес-процесів [1]. Водночас інтеграція великої кількості пристроїв Інтернету речей (IoT) у середовище SDN створює нові виклики для забезпечення інформаційної безпеки. Розширені можливості програмного керування мережею, з одного боку, спрощують адміністрування та впровадження політик безпеки, а з іншого — формують додаткові точки потенційної компрометації, особливо в умовах централізації контролю.

Традиційні механізми мережевого захисту були розроблені для статичних архітектур, у яких мережеві пристрої конфігурувалися локально та функціонували ізольовано. У SDN-архітектурі площина керування відокремлена від площини передачі даних, а всі мережеві політики реалізуються через централізований контролер. Така модель, попри свої переваги, може бути використана зловмисниками для здійснення атак на контролер, маніпуляції потоками трафіку або отримання несанкціонованого доступу до IoT-пристроїв. Саме тому інтеграція комплексних механізмів захисту в SDN-середовищі є критично важливою умовою забезпечення надійності мережі.

Одним із ключових напрямів підвищення безпеки є реалізація розширеного контролю доступу. Централізований контролер SDN дозволяє впроваджувати політики доступу на основі ролей, контексту та поведінкових характеристик пристроїв. У середовищах IoT це особливо актуально, оскільки пристрої можуть мати різні рівні довіри та функціональні обмеження. Динамічний контроль доступу дає змогу в реальному часі надавати або обмежувати доступ до мережевих ресурсів залежно від стану пристрою або характеру його трафіку. Важливим компонентом безпеки є постійний моніторинг і аналіз мережевої активності. Завдяки глобальному огляду мережі SDN-контролер здатний збирати дані про

трафік усіх IoT-пристроїв і виконувати централізований аналіз. Інтеграція систем виявлення та запобігання вторгненням (IDPS) у SDN-архітектуру дозволяє оперативно виявляти аномалії, DDoS-атаки та спроби несанкціонованого доступу. Криптографічний захист також є невід'ємним елементом інформаційної безпеки SDN-IoT систем. Використання сучасних протоколів шифрування між контролером і мережевими пристроями гарантує конфіденційність та цілісність даних. Особливої уваги потребує захист каналів зв'язку IoT-пристроїв, які часто мають обмежені ресурси, що вимагає застосування оптимізованих криптографічних алгоритмів. Сегментація мережі в середовищі SDN забезпечує додатковий рівень ізоляції IoT-пристроїв. Завдяки віртуалізації можна створювати окремі логічні сегменти, у межах яких застосовуються специфічні політики безпеки. Такий підхід мінімізує ризик поширення атак у межах усієї мережі.

Окремою перевагою SDN є можливість автоматизації стратегій захисту. Програмованість мережі дозволяє адаптувати політики безпеки відповідно до поточної ситуації, автоматично оновлювати правила фільтрації трафіку та реалізовувати механізми самовідновлення. Таким чином, поєднання контролю доступу, моніторингу, шифрування, сегментації та автоматизованих механізмів реагування формує комплексну модель підвищення інформаційної безпеки програмно-визначених мереж із використанням технологій Інтернету речей.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У результаті дослідження встановлено, що підвищення інформаційної безпеки програмно-визначених мереж із інтегрованими технологіями Інтернету речей потребує комплексного підходу, який поєднує сегментацію мережі, багаторівневу автентифікацію, криптографічний захист і інтелектуальний моніторинг трафіку. Доведено, що централізована архітектура SDN створює як нові можливості для керування безпекою, так і додаткові ризики, що потребують адаптивних механізмів захисту. Запропоновані методи сприяють підвищенню стійкості мережі до кібератак та забезпеченню надійності функціонування IoT-інфраструктури.

ДЖЕРЕЛА

1. Farooq M.S., Riaz S., Alwi A. (2023). Security and privacy issues in software-defined networks (SDN): A systematic literature review. *Electronics*, 12(14), 3077.
2. Pillai S., Polimetla K. (2024). Integration of network security into software-defined networking (SDN) architectures. In International Conference on Integrated Circuits and Communication Systems (ICICACS) pp. 1-6. IEEE.
3. Chodari S., Sanwal R., Sharma N., Anto Pravin Singh D., Deepa G.(2024). Collaboration in Data Science in Human Artificial Intelligence: Optimising Decisions Using Human-Centred Automation, 2024 Second International Conference on Computational and Characterisation Techniques in Engineering and Sciences (IC3TES), 10.1109/IC3TES62412.2024.10877543, 1-6.



АННА КВЯТКОВСЬКА
докторка філософії в галузі знань 01 «Освіта/Педагогіка», викладачка вищої категорії циклової комісії кібербезпеки, електронних комунікацій та економіко-управлінської підготовки, Київський фаховий коледж зв'язку, м.Київ, Україна
ORCID: 0000-0002-4977-5515
email:sobolevanna29@gmail.com
Наукові інтереси зосереджені на проблематиці цифровізації освіти, формування професійних і соціальних компетентностей здобувачів освіти, впровадження інноваційних освітніх технологій, забезпечення академічної доброчесності.

КОРЕЛЯЦІЯ МЕРЕЖЕВИХ ІНДИКАТОРІВ ЯК ОСНОВА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ OSINT-АНАЛІЗУ ФІШИНГОВИХ РЕСУРСІВ

Валерія Кизима, Володимир Наконечний

Анотація. *Кореляція мережевих індикаторів здатна суттєво підвищити ефективність OSINT-аналізу фішингових ресурсів, оскільки окремі ознаки (як-от IP-адреси, доменні патерни, SSL-сертифікати) у сукупності виявляють складові загрози, що індивідуально важко помітити. Застосування інтегрованого набору мережевих індикаторів дозволяє систематизувати процес OSINT-розслідування та зменшити ймовірність помилкових висновків. У роботі демонструються джерела мережевих даних, підходи їх кореляції та значення для виявлення фішингових загроз.*

Ключові слова: OSINT-аналіз, фішингові загрози, мережеві індикатори, кібербезпека, відкриті джерела.

I. ВСТУП

Фішингові атаки залишаються одним із наймасовіших інструментів компрометації інформаційних систем та викрадення конфіденційних даних. Сучасні дослідження підтверджують, що фішинг активно еволюціонує, використовуючи короткоживучі домени, автоматизовану генерацію інфраструктури та адаптивні сценарії соціальної інженерії [1]. У таких умовах традиційні реактивні механізми виявлення демонструють обмежену ефективність. OSINT-технології розглядаються як перспективний напрям підвищення результативності аналітичних процесів у кібербезпеці, оскільки дозволяють використовувати відкриті джерела для побудови розширеного профілю загрози [2]. Дослідники підкреслюють, що саме інтеграція різних типів відкритих даних створює основу для більш глибокого аналізу кіберінцидентів [3].

II. ДАНІ ТА МЕТОДИ

У межах дослідження використовуються відкриті мережеві індикатори, зокрема WHOIS-дані, записи DNS, інформація про SSL/TLS-сертифікати та IP-адреси хостингу. Згідно з сучасними підходами до OSINT-аналізу, ефективність виявлення кіберзагроз зростає за умови поєднання різних джерел інформації та їх подальшої кореляції [2]. Окремі дослідження демонструють, що включення OSINT-характеристик до процесу аналізу фішингових ресурсів підвищує точність моделей виявлення порівняно з використанням одиничних ознак [1]. Тому в роботі застосовано підхід, який передбачає послідовний збір, очищення та кореляцію мережевих індикаторів із подальшою оцінкою їх сукупної інформативності. Кореляція індикаторів здійснюється шляхом виявлення повторюваних або пов’язаних характеристик між різними мережевими об’єктами. Зокрема, аналізується збіг IP-адрес між кількома доменами, повторюваність шаблонів доменних імен (typosquatting, використання однакових префіксів або суфіксів), часові характеристики реєстрації доменів та випуску SSL-сертифікатів. Додатково враховується історичний зв’язок між доменами через пасивні DNS-дані. Це дозволяє перейти від аналізу окремого ресурсу до виявлення потенційно пов’язаної інфраструктури.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз свідчить, що використання одиничних індикаторів (наприклад, лише віку домену або лише IP-адреси) може призводити до помилкових позитивних або

хибнонегативних висновків. Натомість поєднання декількох мережевих характеристик дозволяє виявити стійкі закономірності фішингової активності. Подібний підхід підтверджується сучасними дослідженнями у сфері OSINT, які наголошують на важливості кореляційного аналізу для виявлення складних кіберзагроз [3].

У межах дослідження передбачається використання узагальненого підходу до оцінювання ризику, за якого кожному індикатору може бути умовно присвоєна вага залежно від його інформативності. Наприклад, нещодавня реєстрація домену має нижчу доказову силу порівняно з повторюваним використанням однієї IP-адреси у кількох підозрілих ресурсах. Поєднання декількох вагомих ознак формує комплексний профіль ризику, що підвищує точність аналітичних висновків.

У наукових роботах також підкреслюється необхідність оцінювання достовірності відкритих джерел та перевірки отриманих даних перед формуванням остаточних висновків [4], що є важливим елементом мінімізації ризику хибної інтерпретації результатів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати узгоджуються з висновками сучасних досліджень щодо доцільності використання OSINT у протидії кіберзлочинності [5]. Кореляція мережевих індикаторів дозволяє перейти від фрагментарного аналізу до системного підходу, що підвищує точність і обґрунтованість прийняття рішень. Інтеграція кореляційного підходу в процес OSINT-аналізу створює передумови для підвищення ефективності виявлення фішингових ресурсів та вдосконалення практик реагування на кіберзагрози.

ЛІТЕРАТУРА

1. An, P., Shafi, R., Mughogho, T., & Onyango, O. A. (2025). Multilingual Email Phishing Attacks Detection using OSINT and Machine Learning. arXiv. https://arxiv.org/abs/2501.08723
2. Group-IB. (2025). OSINT: Open Source Intelligence, Frameworks, and Applications. https://www.group-ib.com/resources/knowledge-hub/osint/
3. Rahman, M. S. (2025). The Art of Open Source Intelligence (OSINT): Addressing Cybercrime Opportunities and Challenges. ResearchGate.
4. Szymoniak, S. (2024). Open Source Intelligence Opportunities and Challenges. Advances in Science and Technology Research Journal, 18(2), 1–10.
5. Rybka, D. (2025). OSINT у забезпеченні національної безпеки. Науковий вісник Ужгородського національного університету, 72(1), 115–121.



ВАЛЕРІЯ КИЗИМА
студентка 2 курсу магістратури кафедри кібербезпеки та захисту інформації факультету інформаційних технологій у Київському національному університеті імені Тараса Шевченка.
E-mail: kovalovav@knu.ua
Науковий інтерес полягає в застосуванні OSINT-технологій у виявленні фішингових загроз. Досліджується вплив кореляції мережевих індикаторів на підвищення точності аналітичних висновків.



ВОЛОДИМИР НАКОНЕЧНИЙ
Доктор технічних наук, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій у Київському національному університеті імені Тараса Шевченка.
ORCID: 0000-0002-0247-5400
E-mail: nakonechnyiv@fit.knu.ua
Наукові інтереси: Інформаційна безпека, радіолокація, радіонавігація.

РОЗШИРЕННЯ БАЗОВИХ МЕРЕЖНИХ ПОЛІТИК KUBERNETES ЗА ДОПОМОГОЮ SERVICE MESH ДЛЯ СЕГМЕНТАЦІЇ НА РІВНІ L7

Владислав Литвиненко, Сергій Бучик

Анотація. *У роботі досліджується розширення базової мережевої ізоляції кластерів Kubernetes на рівнях L3/L4 за допомогою технологій Service Mesh для забезпечення безпеки на рівні прикладних протоколів (L7). Проведено порівняльний аналіз використання CNI-плагінів та архітектурного патерну Sidecar за критеріями гранулярності контролю доступу, механізмів автентифікації (mTLS). Обґрунтовано доцільність застосування комбінованого підходу, який поєднує стандартні Network Policies та Service Mesh для побудови ефективного ешелонованого захисту з оптимальним балансом надійності та використання ресурсів.*

Ключові слова: Kubernetes, Service Mesh, Network Policies, Zero Trust, мікросервіси.

I. ВСТУП

Розвиток мікросервісної архітектури та перехід до хмарних середовищ (Cloud-Native) вимагають перегляду класичних підходів до безпеки та маршрутизації [1]. Базовою лінією захисту кластерів Kubernetes є впровадження моделі Zero Trust через стандартні Network Policies із застосуванням парадигми "Default Deny" [2]. Це дозволяє надійно блокувати несанкціонований доступ на транспортному та мережевому рівнях (L3/L4 за моделлю OSI), оперуючи IP-адресами та портами за допомогою CNI-плагінів. Однак сучасні мікросервіси переважно взаємодіють через протоколи прикладного рівня, такі як HTTP/1.1, HTTP/2 та gRPC. Стандартні Network Policies чудово справляються із завданням відсікання небажаного трафіку на рівні мережевих інтерфейсів вузлів [2], проте вони мають низку суттєвих архітектурних обмежень у контексті сучасних додатків. Метою цієї роботи є дослідження методів розширення базової мережевої ізоляції за допомогою технологій Service Mesh, які забезпечують контроль трафіку, безпеку та маршрутизацію на рівні L7 [3].

II. ДАНІ ТА МЕТОДИ

Для вирішення проблеми гранулярної сегментації застосовуються рішення класу Service Mesh (наприклад, Istio, Linkerd) [3]. Дослідження базується на аналізі архітектурного патерну Sidecar: розгортанні проксі-сервера (Envoy) поруч із кожним контейнером додатку. Цей патерн відокремлює площину управління (Control Plane) від площини даних (Data Plane), виділяючи логіку безпеки та маршрутизації за межі вихідного коду мікросервісів.

Для оцінки ефективності підходу проведено порівняльний аналіз CNI-плагінів та L7-проксі за такими критеріями: гранулярність контролю доступу – здатність реалізовувати принцип найменших привілеїв шляхом інспекції HTTP-заголовків, методів та URI; механізми взаємної автентифікації (mTLS) – надійність криптографічної ідентифікації у недовіреному середовищі кластера.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз використання Service Mesh як механізму сегментації на рівні L7 виявив наступні ключові переваги над стандартним підходом.

1. Гранулярний контроль доступу. Service Mesh дозволяє створювати правила, які враховують не лише сервіс-джерело, але й HTTP-заголовки, методи запитів та

наявність валідних JWT-токенів [3]. Це ефективно запобігає атакам типу горизонтального переміщення (lateral movement) на прикладному рівні.

2. Строга ідентифікація через mTLS. Виявлено, що Service Mesh ефективно усуває проблему ефемерних IP-адрес, забезпечуючи взаємну автентифікацію для всіх з'єднань. Кожен мікросервіс отримує унікальний криптографічний сертифікат, що автоматично ротується з допомогою Control Plane. Це гарантує шифрування трафіку при передачі (data in transit) та захист від атак Man-in-the-Middle (MITM) всередині кластера без необхідності модифікувати вихідний код додатків.

Водночас традиційні CNI-плагіни забезпечують надзвичайно високу продуктивність з мінімальними затримками, оскільки фільтрація пакетів відбувається безпосередньо в ядрі операційної системи. Натомість повноцінне впровадження Service Mesh вимагає розгортання sidecar-проксі для кожного поду, що призводить до додаткового споживання обчислювальних ресурсів (CPU та RAM) вузлів та збільшення мережевої затримки.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Service Mesh не є заміною класичним Kubernetes Network Policies, а виступає необхідним еволюційним кроком для побудови комплексного ешелонованого захисту [1].

Оптимальним інженерним рішенням є комбінований підхід. Використання Network Policies (на рівнях L3/L4) залишається обов'язковим для масового відсікання нелегітимного трафіку з майже нульовим впливом на прикладні процеси. Водночас точкове та автоматизоване застосування Service Mesh бере на себе завдання тонкого управління трафіком на рівні L7 та забезпечення криптографічної ідентифікації [3]. Таке поєднання дозволяє досягти балансу між надійністю, гнучкістю маршрутизації та раціональним використанням обчислювальних ресурсів у кластерах Kubernetes.

ДЖЕРЕЛА

1. Chandramouli, R. (2022). Implementation of DevSecOps for a microservices-based application with service mesh (NIST Special Publication 800-204C). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-204C

2. Kubernetes Documentation. (2026). Network policies. Retrieved from https://kubernetes.io/docs/concepts/services-networking/network-policies/

3. Istio Documentation. (2026). Security. Retrieved from https://istio.io/latest/docs/concepts/security/ (Accessed: 2 March 2026).



ВЛАДИСЛАВ ЛИТВИНЕНКО
студент 2 курсу магістратури кафедри кібербезпеки та захисту інформації факультету інформаційних технологій у Київському національному університеті імені Тараса Шевченка.
E-mail: lytvynenkov@knu.ua
Науковий інтерес полягає в області розгортання та захисту хмарних інфраструктур, SRE, DevOps, забезпечення стійкості кластерів Kubernetes.



СЕРГІЙ БУЧИК
Доктор технічних наук, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій у Київському національному університеті імені Тараса Шевченка.
E-mail: buchyk@knu.ua
Наукові інтереси: інформаційні технології, інформаційна безпека, кібербезпека, теорія прийняття рішень.

КРИПТОГРАФІЧНІ ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЙНОГО ОБМІНУ В МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ 6G

Захар Малига

Анотація. *У роботі розглянуто сучасні криптографічні підходи до забезпечення безпеки інформаційного обміну в мережах наступного покоління 6G. Проаналізовано виклики, пов'язані зі зростанням швидкостей передачі даних, використанням штучного інтелекту та масовим підключенням пристроїв IoT. Досліджено перспективні криптографічні механізми, зокрема постквантову криптографію, легковагові алгоритми шифрування та протоколи безпечної автентифікації. Запропоновано багаторівневу модель захисту інформаційного обміну для забезпечення конфіденційності, цілісності та автентичності даних*

Ключові слова: 6G, криптографія, постквантова криптографія, безпечні протоколи, мережі наступного покоління.

I. ВСТУП

Розвиток мобільних мереж нового покоління спрямований на досягнення надвисоких швидкостей передачі даних, мінімальних затримок і підтримки великої кількості підключених пристроїв. Мережі 6G розглядаються як еволюційний етап після 5G, що інтегрує штучний інтелект, edge computing та нові архітектури мережевої взаємодії.

Зростання складності мережевої інфраструктури створює нові виклики для забезпечення інформаційної безпеки. Традиційні криптографічні механізми можуть виявитися недостатніми через появу квантових обчислень та нових типів атак.

Метою роботи є аналіз криптографічних підходів до захисту інформаційного обміну в мережах 6G та визначення перспективних напрямів розвитку.

II. ДАНІ ТА МЕТОДИ

У дослідженні застосовано методи порівняльного аналізу сучасних криптографічних алгоритмів і протоколів.

Основні криптографічні підходи:

- постквантові алгоритми шифрування;
- легковагові криптографічні алгоритми для IoT-пристроїв;
- end-to-end шифрування;
- протоколи безпечної автентифікації;
- криптографія на основі блокчейн-технологій.

Особлива увага приділяється вимогам до низької затримки та високої продуктивності, які є критичними для мереж 6G.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз показав, що класичні алгоритми шифрування можуть бути вразливими до майбутніх квантових атак. У зв'язку з цим перспективними є постквантові криптографічні підходи, які забезпечують стійкість до квантових обчислень.

Запропонована модель захисту включає:

1. Гібридні криптографічні протоколи (класична + постквантова криптографія).
2. Динамічне управління ключами.
3. Zero Trust принципи автентифікації.

4. Інтеграцію AI для виявлення аномалій.

Результати свідчать, що використання гібридних криптографічних механізмів дозволяє забезпечити високий рівень безпеки без значного зниження продуктивності мережі.



Рисунок 1. *Модель криптографічного захисту інформаційного обміну в мережах 6G.*

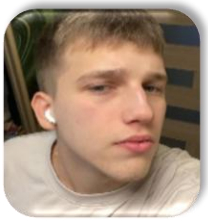
IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Мережі 6G потребують нових підходів до криптографічного захисту, які враховують квантові загрози та високі вимоги до швидкості передачі даних. Використання постквантової криптографії, легковагових алгоритмів і багаторівневих моделей автентифікації забезпечує перспективний напрям розвитку безпечних мережевих технологій.

Подальші дослідження можуть бути спрямовані на оптимізацію криптографічних алгоритмів для високошвидкісних мереж і інтеграцію AI-механізмів управління безпекою.

ДЖЕРЕЛА

1. Zhang Z. Security Challenges in 6G Networks. IEEE Communications Magazine, 2022.
2. NIST Post-Quantum Cryptography Standardization, 2023.
3. Chen L. Lightweight Cryptography for IoT Systems. ACM Computing Surveys, 2021.
4. Saad W. Vision of 6G Wireless Systems. IEEE Network, 2020.



ЗАХАР МАЛИГА
Студент 3 курсу бакалаврату спеціальності 125 «Кібербезпека», факультет інформаційних технологій і систем (ФІТІС), Черкаський державний технологічний університет (ЧДТУ), Черкаси, Україна
E-mail: z.p.malyha.fitis23@chdtu.edu.ua

БЕЗПЕКА ТА КОНТРОЛЬ ІНФОРМАЦІЙНИХ ПОТОКІВ У ВОЛОКОННО-ОПТИЧНИХ МЕРЕЖАХ

Олександр Манько, Людмила Харлай, Ганна Мостович

***Анотація**. У роботі розглядаються сучасні методи та технічні засоби захисту інформації у волоконно-оптичних системах передачі (ВОСП). Акцент зроблено на аналізі можливих каналів витоку інформації, включаючи бічне випромінювання світловодів, нерегулярності волокон, взаємодію спектрально ущільнених сигналів та потенційні дії несанкціонованого доступу. Запропоновано комплексний підхід до захисту інформації, що включає: спектральне розділення каналів із випадковим перемиканням несучих довжин хвиль, застосування оптичних ліній затримки, змішувачів та фільтрів мод, контроль зворотнього розсіяння і моніторинг коефіцієнта похибок на приймачах. Додатково розглянуті організаційні та організаційно-технічні заходи, які обмежують доступ до оптичних кабелів та обладнання, підвищуючи загальний рівень безпеки. Використання ймовірнісного кодування інформації та контроль параметрів оптичної лінії дозволяють мінімізувати ризик перехоплення та забезпечити надійність передачі даних. Отримані результати демонструють, що інтегрований підхід до технічного та організаційного захисту ВОСП забезпечує практично неможливий несанкціонований доступ до конфіденційної інформації та гарантує безпеку комунікацій на рівні сучасних телекомунікаційних стандартів.*

Ключові слова: волоконно-оптичні системи, захист інформації, бічне випромінювання, оптичні кабелі, ймовірнісне кодування, контроль несанкціонованого доступу.

I. ВСТУП

Сучасні телекомунікаційні системи дедалі активніше переходять на волоконно-оптичні технології передачі даних завдяки їх високій пропускній здатності, низьким втратам сигналу та стійкості до електромагнітних завад. Разом із цим виникає гостра потреба в забезпеченні безпеки переданої інформації, оскільки навіть складні волоконно-оптичні системи не є абсолютно захищеними від несанкціонованого доступу та перехоплення.

Захист інформації у волоконно-оптичних системах передачі (ВОСП) потребує комплексного підходу, який поєднує технічні, організаційні та криптографічні засоби. Ключовим завданням є виявлення та мінімізація каналів витоку інформації, таких як бічне випромінювання світловодів, нерегулярності волокон, перехресні впливи спектрально-ущільнених сигналів та доступ до апаратури передачі і прийому.

В основу розробки ефективних методів захисту інформації покладено знання про можливості потенційного зловмисника, зокрема моделі несанкціонованого зйому інформації, створені для аналізу технік іноземної технічної розвідки. Незважаючи на складність технічного доступу до оптичних каналів, постійний розвиток технологій перехоплення робить актуальним впровадження таких методів контролю, які забезпечують практично неможливий несанкціонований доступ при одночасному збереженні ефективності передавання інформації.

Мета цієї роботи полягає у систематизації сучасних підходів до захисту інформації у ВОСП, аналізі технічних та організаційних засобів безпеки та розробці рекомендацій щодо їх практичного застосування для забезпечення надійного і стійкого каналу зв’язку.

II. ДАНІ ТА МЕТОДИ

Захист інформації в волоконно-оптичних системах передачі (ВОСП) ґрунтується на розумінні можливостей несанкціонованого доступу та методів зйому інформації. Вихідними даними є характеристики оптичних кабелів (ОК), параметри світловодів (ОВ), довжини хвиль несучих сигналів, показники згасання та інтерференційні ефекти, що виникають при передачі сигналу. Методи дослідження включали:

1. Аналіз можливих каналів витоку інформації, включаючи бічне випромінювання світловодів та витоки на нерегулярностях волокон.
2. Моделювання методів перехоплення інформації на основі адаптованої моделі лазерної розвідки.
3. Розробку технічних засобів захисту, включно зі спектральним розділенням каналів, створення методів оптичної криптографії з використанням оптичних ліній затримки (ОЛЗ), змішувачами мод, фільтрами оболонкових мод та системами контролю зворотного розсіяння.
4. Експериментальне визначення порогів виявлення несанкціонованого доступу, оцінка ефективності ймовірнісного кодування інформації та контролю коефіцієнта похибок.
5. Впровадження організаційних заходів для обмеження доступу до оптичних кабелів та обладнання.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Дослідження показало, що:

- Несанкціонований доступ до ВОСП можливий лише за наявності спеціалізованої апаратури для виведення додаткового випромінювання з ОК, причому ефективність таких спроб залежить від рівня бічного випромінювання та ступеня захисту оболонки.
- Використання спектрального розділення каналів із випадковим перемиканням несучих довжин хвиль і генерацією псевдовипадкових сигналів практично виключає можливість перехоплення інформації на проміжних ділянках лінії.
- Застосування ОЛЗ, змішувачів мод і фільтрів оболонкових мод дозволяє формувати стаціонарний модовий розподіл, що суттєво знижує рівень бічного випромінювання.
- Контроль параметрів лінії через зворотнє розсіяння та вимірювання коефіцієнта похибок на приймачах забезпечує оперативне виявлення спроб несанкціонованого доступу.
- Застосування методів оптичної криптографії за допомогою пасивних оптичних елементів при формуванні лінійного сигналу дозволяє значно підвищити рівень захисту інформаційних потоків.
- Використання ймовірнісного кодування інформації додатково підвищує криптографічний захист, змушуючи потенційного зловмисника відводити значні додаткові потужності для спроб зйому сигналу, що одразу фіксується системою контролю.

Аналіз показав, що інтеграція технічних та організаційних заходів забезпечує комплексний захист і мінімізує ризик витоку інформації. Організаційні заходи, такі як персональна відповідальність, обмеження доступу до приміщень, контроль за обладнанням та криптографічне шифрування, доповнюють технічні методи і підвищують ефективність загального захисту.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Дослідження підтвердило, що волоконно-оптичні системи за своєю природою мають підвищений рівень захисту, проте це не виключає необхідності впровадження додаткових заходів. Найбільш ефективною стратегією є поєднання:

1. **Технічних засобів захисту**: спектральне розділення каналів, оптична криптографія, ОЛЗ, змішувачі і фільтри мод, контроль зворотнього розсіяння, ймовірнісне кодування інформації.
2. **Організаційних заходів**: обмеження доступу до ОК, контроль обробки інформації, фізичне розташування обладнання, системи блокування у випадку перевищення порогів похибок.

3. **Систем контролю несанкціонованого доступу**: моніторинг бічного випромінювання та контроль оптичних параметрів, що дозволяє миттєво реагувати на спроби перехоплення.

Реалізація запропонованих методів дозволяє забезпечити безпеку передачі конфіденційної інформації у волоконно-оптичних мережах на рівні, який суттєво перевищує захист традиційних металевих кабелів, забезпечуючи практично неможливий несанкціонований доступ до даних без фіксації спроби. Таким чином, інтегрований підхід до захисту ВОСП на основі технічних і організаційних заходів, а також застосування криптографічних властивостей ймовірнісного кодування, є оптимальним способом забезпечення безпеки інформації, що передається оптичними каналами.

ДЖЕРЕЛА

1. Agrawal, G. P. (2019). *Fiber*-optic communication systems (5th ed.). Wiley.
2. Keiser, G. (2021). Optical fiber communications (6th ed.). McGraw-Hill Education.
3. Kaminow, I. P., Li, T., & Willner, A. E. (Eds.). (2013). Optical fiber telecommunications: Systems and networks (6th ed.). Academic Press.
4. Saleh, B. E. A., & Teich, M. C. (2019). Fundamentals of photonics (3rd ed.). Wiley.
5. Agrawal, G. P., & Olsson, N. A. (1989). Fiber-optic communication: Nonlinear effects and security considerations. Journal of Lightwave Technology, 7(4), 657–663. https://doi.org/10.1109/50.30484
6. Boyd, R. W. (2020). Nonlinear optics (4th ed.). Academic Press.
7. Senior, J. M., & Jamro, M. Y. (2009). Optical fiber communications: Principles and practice (3rd ed.). Pearson.
8. Kharlai Liudmila, Kunakh Nataliya, Sotnichenko Yulia, Konovalov Oleksiy, Skubak Olexandr, Manko Oleksandr. Dynamic Information Protection Method on Computer Optical Networks, International Journal of Advanced Trends in Computer Science and Engineering. 2020/Vol. 9, #3, May – June. pp. 3666 - 3670.



ОЛЕКСАНДР МАНЬКО
Доктор технічних наук, професор, викладач циклової комісії кібербезпеки, електронних комунікацій та економіко-управлінської підготовки, Київський фаховий коледж зв'язку, м.Київ, Україна
ORCID: 0000-0002-2131-3597
email: manko_kiev@ukr.net
З 2012 — викладач Київський фаховий коледж зв'язку.



ЛЮДМИЛА ХАРЛАЙ
Кандидат технічних наук, доцент, голова циклової комісії кібербезпеки, електронних комунікацій та економіко-управлінської підготовки, Київський фаховий коледж зв'язку, м.Київ, Україна
ORCID: 0000-0002-7633-933X
email: ikskkz202@gmail.com
З 2008 — викладач Київський фаховий коледж зв'язку.



ГАННА МОСТОВИЧ
викладач, спеціаліст вищої категоріїю, викладач циклової комісії кібербезпеки, електронних комунікацій та економіко-управлінської підготовки, Київський фаховий коледж зв'язку, м.Київ, Україна
email: mos-tikanna@gmail.com
З 2008 — викладач Київський фаховий коледж зв'язку.

БЕЗПЕКА ДАНИХ У МУЛЬТИХМАРНИХ ТА МІЖПЛАТФОРМНИХ МЕРЕЖЕВИХ АРХІТЕКТУРАХ

Сергій Натура

Анотація. *У роботі досліджено сучасні підходи до забезпечення безпеки даних у мультихмарних та міжплатформних мережевих архітектурах. Проаналізовано виклики, пов'язані з використанням різних хмарних провайдерів і гетерогенних платформ. Розглянуто механізми управління доступом, шифрування даних, Zero Trust підходи та централізований моніторинг безпеки. Запропоновано модель багаторівневого захисту інформаційного обміну, що дозволяє мінімізувати ризики витоку даних і підвищити стійкість інфраструктури.*

Ключові слова: мультихмара, кібербезпека, міжплатформні системи, Zero Trust, захист даних

I. ВСТУП

Мультихмарні та міжплатформні архітектури набувають широкого поширення завдяки можливості оптимізації ресурсів, підвищення відмовостійкості та уникнення залежності від одного провайдера. Організації дедалі частіше використовують одночасно кілька хмарних платформ, поєднуючи їх із локальною інфраструктурою.

Разом із перевагами такі архітектури створюють додаткові виклики для забезпечення безпеки даних. Відсутність єдиного стандарту конфігурації, різні політики доступу та складність централізованого контролю збільшують ризики витоку інформації.

Метою роботи є аналіз методів захисту даних у мультихмарних середовищах та визначення ефективних моделей безпеки.

II. ДАНІ ТА МЕТОДИ

Дослідження базується на аналізі сучасних практик кібербезпеки в мультихмарних системах.

Основні підходи до захисту:

- централізоване управління ідентифікацією (IAM);
- end-to-end шифрування;
- Zero Trust архітектура;
- сегментація мережі;
- моніторинг і аудит подій безпеки;
- автоматизоване управління конфігураціями.

Особливу увагу приділено загрозам, пов'язаним із помилками налаштування міжхмарних з'єднань.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз показав, що найбільш критичними ризиками є:

- некоректні політики доступу між платформами;
- відсутність централізованого управління ключами;
- різнорідність механізмів безпеки у різних хмарах.

Запропонована модель безпеки включає:

1. Уніфіковане управління доступом через федерацію ідентифікації.
2. Використання Zero Trust принципів.

3.Шифрування даних на всіх етапах передачі.
4.Автоматичне виявлення аномалій.



Рисунок 1. *Модель забезпечення безпеки даних у мультихмарній мережевій архітектурі.*

Застосування запропонованого підходу дозволяє підвищити контроль над даними та зменшити ризики кіберінцидентів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Безпека мультихмарних систем потребує комплексного підходу, який поєднує криптографічний захист, централізоване управління доступом і постійний моніторинг. Використання Zero Trust та автоматизованих механізмів аналізу подій дозволяє забезпечити високий рівень захисту в умовах складних міжплатформних архітектур.

Подальші дослідження можуть бути спрямовані на використання AI для автоматичного управління політиками безпеки.

ДЖЕРЕЛА

1. ENISA Cloud Security Guidelines, 2023.
2. NIST Cloud Security Framework, 2022.
3. Kumar R. Multi-Cloud Security Architecture. Journal of Network Security, 2024.
4. Zhang Z. Zero Trust in Hybrid Networks. IEEE Communications Magazine, 2021.



СЕРГІЙ НАТУРА
Студент 3 курсу бакалаврату спеціальності 125 «Кібербезпека», факультет інформаційних технологій і систем (ФІТІС), Черкаський державний технологічний університет (ЧДТУ), Черкаси, Україна
E-mail: s.r.natura.fitis23@chdtu.edu.ua

ЗАХИСТ ПЕРСОНАЛЬНИХ І ЧУТЛИВИХ ДАНИХ У СИСТЕМАХ ІЗ ВБУДОВАНИМИ МЕХАНІЗМАМИ ШТУЧНОГО ІНТЕЛЕКТУ

Максим Норенко, Інна Розломій

Анотація. *У роботі розглянуто проблематику забезпечення конфіденційності персональних і чутливих даних у системах із вбудованими механізмами штучного інтелекту. Проаналізовано основні ризики витоку інформації під час навчання моделей машинного навчання та їх експлуатації. Досліджено сучасні методи захисту даних, включаючи диференційну приватність, федеративне навчання та криптографічні механізми. Запропоновано комплексний підхід до побудови безпечних AI-систем із урахуванням сучасних загроз кібербезпеки.*

Ключові слова: штучний інтелект, персональні дані, конфіденційність, AI security, диференційна приватність.

I. ВСТУП

Активний розвиток технологій штучного інтелекту призвів до їх широкого застосування в інформаційних системах різного призначення, зокрема у фінансовому секторі, медицині та державному управлінні. Такі системи обробляють значні обсяги персональних і чутливих даних, що створює додаткові ризики для конфіденційності та інформаційної безпеки. Традиційні підходи до захисту інформації часто не враховують специфіку роботи AI-моделей, які можуть зберігати статистичні залежності та потенційно розкривати дані через непрямі канали. Тому виникає необхідність впровадження нових методів захисту, адаптованих до особливостей машинного навчання.

Метою роботи є дослідження ефективних підходів до забезпечення захисту персональних даних у системах із вбудованими AI-механізмами.

II. ДАНІ ТА МЕТОДИ

У дослідженні використано методи системного аналізу сучасних підходів до забезпечення конфіденційності даних у системах машинного навчання.

Основні механізми захисту:

- анонімізація та псевдонімізація наборів даних;
- застосування диференційної приватності;
- федеративне навчання без централізованого збору інформації;
- контроль доступу та аудит операцій;
- використання криптографічних протоколів для передачі даних.

Особлива увага приділяється атакам типу membership inference, model inversion та data reconstruction.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз показав, що AI-системи можуть бути джерелом непрямих витоків інформації навіть за наявності базових механізмів захисту. Виявлено, що традиційні підходи до безпеки не забезпечують достатнього рівня конфіденційності без інтеграції спеціалізованих AI-security механізмів.

Запропонована модель захисту базується на багаторівневому підході:

- захист даних на етапі підготовки;

- безпечне навчання моделей;
- контроль доступу до inference API;
- постійний моніторинг поведінкових аномалій.

Використання федеративного навчання дозволяє мінімізувати передачу чутливих даних у центральні сховища, що суттєво знижує ризики витоку.



Рисунок 1. *Модель захисту персональних даних у системах із використанням штучного інтелекту*

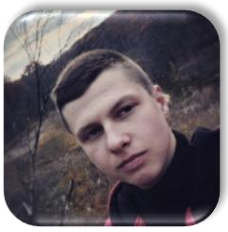
IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Системи із вбудованими механізмами штучного інтелекту потребують комплексного підходу до забезпечення інформаційної безпеки. Поєднання сучасних методів конфіденційності, криптографії та контролю доступу дозволяє підвищити рівень захищеності персональних даних.

Запропонований підхід може бути використаний для створення безпечних AI-рішень у середовищах із високими вимогами до конфіденційності.

ДЖЕРЕЛА

1. Dwork C. Differential Privacy. Communications of the ACM, 2021.
2. Kairouz P. Advances in Federated Learning. Machine Learning Journal, 2022.
3. Papernot N. AI Security Challenges. ACM Computing Surveys, 2023.
4. Shokri R. Membership Inference Attacks. IEEE Security & Privacy, 2020.



МАКСИМ НОРЕНКО
студент 3 курсу бакалаврату кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
E-mail: m.s.norenko.fitis23@chdtu.edu.ua
Наукові інтереси зосереджені на дослідженні IoT-технологій, систем збору та обробки даних, систем моніторингу та контролю, а також питаннях інформаційної безпеки в IoT-інфраструктурах.



ІННА РОЗЛОМІЙ
к.т.н., доцент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
ORCID: 0000-0003-2062-2694
E-mail: inna-roz@ukr.net
Наукові інтереси: Інтернет речей, полегшена криптографія, кіберфізичні системи. Автор/співавтор понад 150 публікацій, 5 монографій та 2 патентів.

РИЗИК-ОРІЄНТОВАНА МОДЕЛЬ ІНТЕГРАЦІЇ ДАНИХ КІБЕРЗАГРОЗ ТА ОПТИМАЛЬНОГО АВТОМАТИЗОВАНОГО РЕАГУВАННЯ В МУЛЬТИХМАРНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Світлана Рзаєва, Дмитро Рзаєв, Юлія Костюк

Анотація. *У дослідженні розглянуто підхід, що поєднує дані кіберзагроз у мультихмарі, що дозволяє узгоджено аналізувати різноманітні події безпеки та визначати узагальнений рівень ризику системи. Побудовано математичну модель взаємозв'язків подій та розроблено алгоритм автоматичного вибору засобів захисту з урахуванням наявних ресурсів. Результати моделювання показали зростання точності виявлення атак, зменшення часу реакції та стабільну роботу системи навіть за збільшення інтенсивності загроз.*

Ключові слова: ризик-орієнтована модель, мультихмарна інфраструктура; автоматичне реагування; аналіз подій; кібербезпека.

I. ВСТУП

Мультихмарні інформаційні системи характеризуються розподіленістю, гетерогенністю та високою динамікою процесів обробки даних, що істотно ускладнює завдання забезпечення кібербезпеки. Події безпеки, які виникають у різних сегментах такого середовища, мають неоднорідну природу, різний рівень достовірності та відмінні часові характеристики. Унаслідок цього традиційні локальні підходи до аналізу інцидентів не дозволяють сформувати узгоджену глобальну оцінку ризику та забезпечити своєчасне реагування.

У роботі пропонується ризик-орієнтований підхід, у межах якого процес інтеграції даних про кіберзагрози та вибів захисних дій формалізується як задача відображення розподіленого простору подій у керований простір станів безпеки системи.

II. ДАНІ ТА МЕТОДИ

Процес аналізу кіберзагроз у мультихмарній інформаційній системі можна зобразити як завдання Інтеграція розподілених векторів подій, що надходять із різних джерел $S = \{s_1, s_2, \ldots, s_n\}$, де кожне джерело надсилає власний простір спостережень $X_j \subset R^{n_j}$. Система подій для "мультихмарти" є добутком $X = X_1 \times X_2 \times \cdots \times X_n$,, тобто якщо x є вектором, який представляє натуральний стан безпеки, то $x(t) \in X$.

Метою узгодження різних подій та врахування міжподійних залежностей є інтеграційно-кореляційний оператор I : X → Z, який нормалізує параметри, ураховує зсуви по часу та підсилює корельовані інциденти. Результатом цього є інтегрований стан загрози z (t) = I (x (t)), що відображає узгоджену черговульцію кібер-загрози в мультихмарній системі.

Оцінка небезпеки базується на орієнтованому на межі ризику підході. За цим принципом вводиться функціонал загального ризику $R : Z \rightarrow R+$. Оцінка ризику системи $u = R(z(t))$ знаходиться в часи t:

$$r(t) = R\big(z(t)\big) = \sum_{i=1}^{k} W_i I_i P_i\big(z(t)\big), \quad (1)$$

де W_i – вага критичності активу,

I_i – значимість/імпакт активу;

$P_i\big(z(t)\big)$ – ймовірність реалізації загрози на основі інтегрованого стану.

Це дозволяє перейти від локального аналізу інцидентів до комплексної оцінки безпеки.

Функціонал враховує критичність активів, накопичувальний ефект загроз та узгодженість подій у часі, що дозволяє перейти від аналізу окремих інцидентів до комплексної оцінки стану безпеки.

Процес реагування формалізується як задача керування. Множина допустимих захисних дій задається як $U = \{u_1, u_2, \ldots, u_m\}$, а динаміка зміни стану системи описується співвідношенням $z(t+1) = \Phi(z(t), u(t))$ де Φ відображає вплив застосованих контрзаходів на конфігурацію загроз. Метою керування є переведення системи в область допустимих станів $Z_s \subset Z$.

Вибір оптимальних дій здійснюється шляхом мінімізації інтегрального критерію:

$$J(u) = \int_{t_0}^{t_f} (\lambda_1 r(t) + \lambda_2 d(z(t), u(t)) + \lambda_3 c(u(t)))dt, \quad (2)$$

де $r(t)$ – рівень глобального ризику,

$d(z(t), u(t))$ – затримка реагування,

$c(u(t))$ – витрати ресурсів на контрзаходи, а коефіцієнти λ_i визначають пріоритети безпеки, швидкодії та економії ресурсів.

Ризик-орієнтована модель інтеграції даних кіберзагроз ґрунтується на положенні, що результативність захисту мультихмарної інформаційної системи визначається не лише здатністю точно фіксувати окремі інциденти безпеки, але й можливістю комплексного аналізу їх сукупного впливу на загальний стан захищеності системи (структуру моделі наведено на рис. 1).

У межах такого підходу ризик трактується як інтегральний показник, який характеризує актуальний стан загроз з урахуванням їх взаємозв'язків, часових змін та рівня критичності захищених інформаційних даних.

Модель реалізує поетапне перетворення розподілених подій безпеки, що надходять із різних хмарних середовищ, у єдиний узгоджений простір станів загроз. На цьому етапі здійснюється інтеграція різнорідних даних шляхом уніфікації їх параметрів та врахування кореляційних залежностей між подіями. Такий підхід забезпечує можливість ідентифікації складних та багатокрокових сценаріїв атак, які залишаються непоміченими в разі ізольованого аналізу окремих інцидентів.

У моделі застосовується механізм ризик-орієнтованої агрегації, у межах якого окремі події безпеки трансформуються в узагальнену оцінку глобального ризику мультихмарної системи. Такий підхід забезпечує ієрархічне представлення загроз, починаючи від локального рівня окремих інцидентів і завершуючи системним рівнем, що характеризує загальний стан інфраструктурної безпеки. Це, у свою чергу, створює умови для обґрунтованої пріоритизації подій та фокусування механізмів реагування на найбільш критичні ділянки системи.

На основі сформованої інтегральної оцінки ризику в моделі реалізується керований контур автоматизованого реагування. Процес вибору захисних дій формалізується як задача оптимізації, спрямована на мінімізацію залишкового ризику за наявності обмежень щодо часу виконання та обчислювальних ресурсів. Така постановка задачі забезпечує можливість адаптивно коригувати стратегії реагування на події, в залежності від поточного стану системи, інтенсивності атак та доступності ресурсів, забезпечуючи баланс між швидкістю реакції та ефективністю захисту.

Ризик-орієнтована модель інтеграції та реагування на атаки забезпечує тісний зв'язок між аналітичною частиною системи кіберзахисту та механізмами прийняття рішень, а це, в свою чергу, створює передумови для побудови інтелектуальних систем автоматизованого

захисту мультихмарних інформаційних систем, здатних функціонувати в умовах високої динаміки загроз і гетерогенності сучасних хмарних інфраструктур.



Рисунок 1. *Структура ризик-орієнтованої моделі інтеграції даних кіберзагроз*

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Ефективність запропонованого підходу була досліджена на основі абстрактного мультихмарного середовища, змодельованого з використанням платформи CloudSim Plus, яка відтворювала розподілену інфраструктуру з кількома зонами доступності та змінними параметрами мережевих затримок. Аналіз показав, що використання інтеграційного оператора I забезпечує формування стійкого узгодженого стану загроз навіть за умов суттєвого зростання інтенсивності потоку подій безпеки.

Оцінювання глобального ризику за допомогою функціонала R дозволило зменшити вплив шумових і малозначущих/ слабоінформативних інцидентів, зосередивши увагу реагування системи на подіях, що формують критичні сценарії атак. У порівнянні з

підходами, заснованими на ізольованому аналізі подій, спостерігається зниження кількості хибних спрацювань і підвищення стабільності оцінювання ризику.

Оптимізаційна модель реагування на події забезпечила адаптивний розподіл ресурсів між контрзаходами. Мінімізація критерію J (u) дозволила скоротити затримку реагування без суттєвого зростання обчислювальних витрат, що є особливо важливим в умовах динамічних і багатокрокових атак. Отримані результати підтверджують, що ризик-орієнтоване керування є ефективним інструментом балансування між рівнем захищеності системи та навантаженням на її інфраструктурні ресурси.

IV. ВИСНОВКИ

Запропонований підхід забезпечує математично узгоджене подання процесів інтеграції подій безпеки та ризик-орієнтованого реагування в мультихмарному середовищі, встановлюючи формальний зв'язок між поточним рівнем загроз і вибором відповідних захисних дій. Отримані результати підтверджують, що інтеграція різнорідних подій безпеки на основі ризик-орієнтованого підходу забезпечують підвищення точності оцінювання загроз, зменшують час реагування та ефективно використовують обчислювальні ресурси середовища. Науковою цінністю дослідження є формалізація процесів аналізу подій та реагування на інциденти у вигляді математичної моделі, яка відображає взаємозв'язок між локальними подіями та глобальним станом безпеки системи. Практичне значення отриманих результатів визначається можливістю застосування запропонованих методів у складі систем моніторингу та реагування на інциденти в мультихмарних інформаційних інфраструктурах.

Подальші дослідження планується спрямувати на розроблення механізмів адаптивного налаштування параметрів оптимізаційного критерію, розширення моделі з урахуванням стохастичного характеру факторів впливу, а також на інтеграцію прогнозних компонентів, орієнтованих на забезпечення проактивного реагування на кіберзагрози.

ДЖЕРЕЛА

1. Deevi, S. R. (2023). *Machine Learning-Driven Threat Detection in Multi-Cloud* Environments. International Journal of Computing and Engineering, 4(4), 17–27. https://doi.org/10.47941/ijce.3262

2. Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments. arXiv. https://doi.org/10.48550/arXiv.2404.05602

3. Miryala, N. K. (2024). Effective Multi Cloud Security Using AI Technologies. International Journal of Computer Trends and Technology, 72(11), 143–149. https://doi.org/10.14445/22312803/IJCTT-V72I11P115

4. Mollah, M. H.-O. R. (2025). AI-Driven Threat Detection and Response Framework for Cloud Infrastructure Security. American Journal of Scholarly Research and Innovation, 4(01), 494–535. https://doi.org/10.63125/e58hzh78

5. Pitkar, H. (2025). Cloud Security Automation Through Symmetry: Threat Detection and Response. Symmetry, 17(6), 859. https://doi.org/10.3390/sym17060859

6. Shaffi, S. M., Vengathattil, S., Nikarthil Sidhick, J., & Vijayan, R. (2025). AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience. arXiv. https://doi.org/10.48550/arXiv.2505.03945

7. Sarraf, G., & Pal, V. (2026). Autonomous Threat Detection and Response in Cloud Security: A Comprehensive Survey of AI-Driven Strategies. arXiv. https://doi.org/10.48550/arXiv.2601.03303

8.Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions. (2025). Computers & Security, 157, 104599. https://doi.org/10.1016/j.cose.2025.104599 Yakoviv, I., Sharadkin, D., & Kulikov, V. (2025). Cyber Threat Information Intelligence Integration Models. Collection "Information Technology and Security, 13(2), 236–252. https://doi.org/10.20535/2411-1031.2025.13.2.344710
9. Thaqi, R., Krasniqi, B., Mazrekaj, A., & Rexha, B. (2024). Literature Review of Machine Learning and Threat Intelligence in Cloud Security. Preprints.org. https://doi.org/10.20944/preprints202410.0512.v1
10. Рзаєва С. Л., Складанний П. М., Костюк Ю. В., Абрамов В. О., Кравченко В. Г. (2025) Адаптивне управління інформаційною безпекою в хмарно-орієнтованих інтелектуальних транспортних системах Безпека інформації, 31 (1). с. 23-36. https://doi.org/10.18372/2225-5036.31.20634
11. Складанний П., Костюк Ю., Рзаєва С., Мазур, Н. (2025). Паралельна обробка даних у розширюваних хеш-структурах та оцінка їх продуктивності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 242–269. https://doi.org/10.28925/2663-4023.2025.31.1015
12. Костюк Ю., Складанний П., Рзаєва С., Самойленко Ю., Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956



СВІТЛАНА РЗАЄВА
к.т.н., доцент кафедри комп'ютерних наук факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.
ORCID: 0000-0002-7589-2045
E-mail: s.rzaieva@kubg.edu.ua
З 1998 року почала свою викладацьку кар'єру на посаді асистента кафедри інформаційних систем та мереж Київського державного торговельно-економічного університету. Коло наукових інтересів: бази даних, інформаційно-інтелектуальні системи, хмарні технології, кібербезпека.



ДМИТРО РЗАЄВ
старший викладач кафедри інформатики та системології інституту інформаційних технологій в економіці Київського національного економічного університету імені Вадима Гетьмана.
ORCID: 0000-0002-7149-4971
E-mail: rzaiev@kneu.edu.ua
З 1997 року почав свою викладацьку кар'єру на посаді асистента кафедри інформатики Київського державного економічного університету. Коло наукових інтересів: моделюванням інтелектуальної діяльності людини та його застосуванням в системах штучного інтелекту.



ЮЛІЯ КОСТЮК
доктор філософії (PhD), доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.
ORCID: 0000-0001-5423-0985
E-mail: y.kostiuk@kubg.edu.ua
З 2016 року почала свою викладацьку кар'єру на посаді асистента кафедри програмної інженерії та інформаційних систем Київського державного торговельно-економічного університету. Коло наукових інтересів: бази даних, інформаційно-інтелектуальні системи, хмарні технології, кібербезпека.

ДОСЛІДЖЕННЯ ІНСТРУКЦІЇ БЕЗУМОВНОГО ПЕРЕХОДУ

Олександр Рисований

Анотація. *У роботі показано, що інструкція безумовного переходу перенаправляє виконання програми на іншу адресу пам'яті чи мітку без аналізу умов. Багаторазове використання інструкції призводить до неструктурованого коду та збільшення часу виконання програми. Її часто застосовують для протидії реверсингу, щоб заплутати код виконання, коли хакер має доступ лише до exe-файлу. Процес аналізу виконання коду у налагоджувачі ускладнюється при переходах від більших адрес до менших. Хакеру дуже часто доводиться аналізувати переходи, які здійснюються від великих адрес розташування коду до менших. В роботі наведено, що така ситуація виникає тоді, коли важливі байти програми (паролі, коди ініціалізації, прихована текстова інформація) записані в заголовки файлу (у DOS-заголовок, область DOS stub, PE-заголовок) і не видно навіть у налагоджувачі.*

Ключові слова: інструкція jmp, PE-формат, переходи, розгалуження.

I. ВСТУП

Сучасні процесори використовують конвеєрне виконання інструкцій та механізми передбачення переходів для підвищення продуктивності (Hyungseok, 2025). Інструкція безумовного переходу jmp впливає на керування потоком виконання програми, роботу конвеєра та ефективність апаратних оптимізацій (Brian, 2025). Її використання може знижувати продуктивність при неправильному розміщенні коду (Zhanyu, 2024).

Мета статті – дослідження інструкції безумовного переходу з метою визначення кількості байтів при передачі управління як з менших адрес до великих, так і від великих адрес до менших. Такі дослідження необхідні при захисті коду програми та аналізі умов впровадження в чужий код.

II. ДАНІ ТА МЕТОДИ

Команда jmp має важливе значення у програмах організації розгалужень (переходів). Вона дозволяє здійснювати безумовний перехід, ускладнювати аналіз коду при великій кількості переходів, та змінювати послідовність виконання коду при його впровадженні.

Команда jmp має різні коди операцій та різну розмірність у байтах. Ближній перехід (стрибок) обмежений від –128 до +127 від поточного значення EIP. Він займає 2 байти (код операції EB та 1 байт зміщення). Далекий перехід використовується для переходів через 128 і більше байтів і займає 5 байтів (код операції E9 та 4 байти зміщення) [5].

Адреса переходу для ближнього переходу розраховується додаванням до адреси першого байту після команди кількості байтів переходу.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

При переходах від менших адрес до великих (переходи «вперед») використовується дальній перехід з кодом операції E9 та довжиною 5 байтів. Наприклад, перехід на 256 байтів має формат E9 00010000h.

При переходах від великих адрес до менших (переходи «назад») часто використовуються переходи «назад». Код операції команди jmp залишається EB для короткого переходу, але кількість байтів записується у зворотному коді. Для короткого переходу назад число байтів записується у зворотному коді. Для довгого переходу назад код

операції – E9, а кількість байтів має формат 32 розряду та записується з молодших адрес до старших у зворотному коді (наприклад, FAFE FFFF).

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Використання великої кількості команд переходу до менших адрес вносить труднощі в аналіз коду для тих, у кого відсутній текст програми. Ближній перехід обмежений від –128 до +127 байт щодо покажчика адреси наступної інструкції (EIP).

Подальші плани досліджень включають процес втручання в PE-заголовок з метою приховування важливої інформації за допомогою інструкції розгалуження.

ДЖЕРЕЛА

1. Hyungseok, Kim., Soomin, Kim., Sang, Kil Cha. (2025) Towards Sound Reassembly of Modern x86-64 Binaries – ASPLOS '25: Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2 Pages 1317 - 1333 https://doi.org/10.1145/3676641.3716026.
2. Brian, Zhao., Yiwei, Yang., Yusheng, Zheng., Andi, Quinn. (2025) Exploiting Control-flow Enforcement Technology for Sound and Precise Static Binary Disassembly — UC Santa Cruz, USA https://doi.org/10.48550/arXiv.2506.09426.
3. Zhanyu, Sha., Carlton, Shepherd., Amir, Rafi., Konstantinos, Markantonakis. (2024) Control-Flow Attestation: Concepts, Solutions, and Open Challenges Computers & Security Volume 150, March 2025, 104254 https://doi.org/10.1016/j.cose.2024.104254.
4. Marco, Chilese., Richard, Mitev., Meni, Orenbach., Ahmad, Atamli., Ahmad-Reza, Sadeghi. (2024) One for All and All for One: GNN-based Control-Flow Attestation for Embedded Devices – 2024 IEEE Symposium on Security and Privacy (SP) | 979-8-3503-3130-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/SP54263.2024.00251.
5. Рисований, О.М. (2025) Реверсне програмування. Формат файлу PE. Середовище програмування masm64: навчально-методичний посібник для студентів спеціальності 123 "Комп'ютерна інженерія". Харків: НТУ «ХПІ». https://repository.kpi.kharkov.ua/handle/KhPI-Press/95746.



ОЛЕКСАНДР РИСОВАНИЙ
Професор, кафедра «Комп'ютерна інженерія та програмування», Харківський технічний університет «Харківський політехнічний інститут», м. Харків, Україна
ORCID: 0000-0003-0616-1617
E-mail: rysov81524@gmail.com
Професор НТУ ХПІ, кандидат технічних наук, 20.02.14 – Озброєння і військова техніка. Працює в НТУ ХПІ з 2006 р. Має більш 400 наукових праць, з яких 6 підручників з грифами міністерства освіти і науки України, більше 50 навчальних посібників, більше 100 винаходів. Область наукових досліджень: розвиток теорії недвійкового сигнатурного аналізу для підвищення ефективності діагностування цифрових систем, реверсна інженерія, низькорівневе програмування, захист програм і даних, сигнатурна математика.

МОДЕЛІ ДОСТУПУ ABAC/CAPBAC/HYBAC ДЛЯ IOT-КОНТРОЛЮ ДО СПЕЦОБ'ЄКТІВ

Артем Рімек, Ольга Кравченко

Анотація. *У роботі порівняно підходи ABAC, CapBAC і HyBAC для IoT-систем контролю доступу на об'єктах спеціального призначення. Запропоновано критерії вибору моделі за контекстністю, автономністю edge-вузлів, делегуванням тимчасових прав, відкликанням доступу та аудитом. Показано, що «чистий» ABAC забезпечує найвищу гнучкість політик, CapBAC найкращу роботу в розподіленому та офлайн середовищі, а гібрид HyBAC дає збалансоване рішення для режимів підвищеної загрози та обмеженої мережі.*

Ключові слова: IoT, Контроль доступу, ABAC, CapBAC, HyBAC.

I. ВСТУП

IoT-контроль доступу на об'єктах спеціального призначення (критична інфраструктура, військові та правоохоронні зони, сховища, серверні, лабораторії) відрізняється від класичного СКУД тим, що рішення про доступ приймається в розподіленому середовищі. Тобто частина логіки працює на edge-контролерах дверей та шлюзах, інша частина у сервісах ідентифікації, біометрії, журналювання та аналітики. Додатково зростає кількість контекстних сигналів (наприклад режим охорони, час, зона, статус пристрою, якість біометричної перевірки, наявність супроводу, тощо), які бажано враховувати в політиках.

Для спецоб'єктів ключовими вимогами є: принцип найменших привілеїв, доказовий аудит подій доступу, стійкість до компрометації окремих вузлів і мінімізація єдиних точок відмови, можливість автономної роботи в режимі ізоляції або деградації мережі, оперативне делегування тимчасових прав (підрядники, ремонтні бригади, аварійні роботи) та швидке відкликання доступу при інцидентах.

В подальших розділах буде порівняно моделі ABAC (атрибутно-орієнтований контроль доступу), CapBAC (контроль доступу на основі можливостей (capabilities)) і HyBAC (гібридний контроль доступу) для IoT-контролю доступу, сформування критерії вибору та обґрунтування, який підхід є практично оптимальним для спецоб'єктів.

II. ДАНІ ТА МЕТОДИ

В цьому розділі був виконаний порівняльний аналіз моделей доступу за набором операційно-безпекових критеріїв, релевантних до спецоб'єктів. Критерії сформовано на основі типових вимог до IoT-доступу (контекстність, розподіленість, обмежені ресурси, потреба в офлайн-режимах) та сучасних підходів у дослідженнях з контролю доступу в IoT-середовищах.

ABAC розглядається як модель, де рішення «дозволити/заборонити» базується на атрибутах суб'єкта, об'єкта, дії та середовища. Для реалізації ABAC у промислових системах часто застосовуються мови політик на кшталт XACML, для яких існують підходи формальної валідації й тестування, що є важливим для критичних систем.

CapBAC розглядається як модель, де право виконати дію задається «здатністю» (capability) - криптографічно захищеним токеном із визначеним обсягом прав (scope) та часовими обмеженнями. У IoT CapBAC часто позиціюють як легковагий підхід для edge-вузлів із локальною перевіркою токенів.

HyBAC трактуємо як гібрид, що поєднує виразність політик ABAC і практичність CapBAC у розподіленому середовищі. Зокрема, в літературі описуються підходи, які

інтегрують атрибутні та capability-механізми (наприклад, Attribute-Capability-Based Access Control) для досягнення одночасно гнучкості й автономності.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Для спецоб'єктів вирішальним є те, як модель підтримує контекстні правила, автономну роботу edge-компонентів, делегування тимчасових прав, відкликання доступу, аудит і пояснюваність рішень. Узагальнений результат порівняння наведено в Таблиці 1.

Таблиця 1. *Порівняння ABAC, CapBAC та HyBAC за критеріями спецоб'єктів*

Критерій	**ABAC**	**CapBAC**	**HyBAC**
Контекстність (час, режим, зона, ризик)	Висока: політики напряму описують умови	Середня: умови треба «вшивати» у токен	Висока: контекст у ABAC, виконання через токен
Автономність edge-рішень	Залежить від PDP/кешів; офлайн складніше	Висока: локальна перевірка підпису	Висока: edge працює на коротких токенах
Делегування тимчасового доступу	Можливо, але складніше адмініструвати атрибути	Сильна сторона: видача capability під задачу	Сильна сторона: делегування через CapBAC у межах ABAC-правил
Відкликання доступу	Швидке при онлайн-оцінці політик	Складніше: TTL/denylist/ротація ключів	Керовано: короткий TTL + зміни політик
Аудит і пояснюваність	Добре пояснює «чому дозволено/заборонено»	Добре фіксує факт використання токена	Найкраще при зв'язці логів ABAC і edge-подій

ABAC демонструє найкращу придатність до політик, що залежать від режимів об'єкта. Наприклад, при посиленій охороні можна вимагати двофакторну автентифікацію, присутність відповідальної особи або підвищений поріг біометричної впевненості. Однак ABAC потребує надійної доставки атрибутів і синхронізації політик. У випадку втрати зв'язку з центральним модулем прийняття рішень (PDP) необхідні механізми кешування nf реплікації політик або локальний PDP, що підвищує складність і вимоги до edge-пристроїв.

CapBAC, навпаки, природно узгоджується з розподіленою IoT-архітектурою: edge-контролер може локально перевірити підпис capability-токена і виконати дію без запиту до центра. Це корисно для ізольованих контурів, де мережа нестабільна або навмисно сегментована. CapBAC також спрощує тимчасовий доступ: токен можна видати під конкретну задачу з TTL і вузьким scope (двері,зона,дія). Основний ризик - відкликання прав до завершення TTL, що вимагає denylist та CRL або коротких токенів і дисципліни керування ключами.

HyBAC для спецоб'єктів доцільно реалізувати як: ABAC - це ядро політик (контекст, режим, ризик), CapBAC – це механізм доставки прав на edge. Типовий цикл: ABAC-движок оцінює політику й, у разі дозволу, видає короткоживучий capability-токен, далі edge-контролер перевіряє токен локально та веде журнал. При зміні режиму (тривога або інцидент) ABAC змінює правила, а видані токени видаляються за TTL або відкликаються. Такий підхід зменшує залежність від постійного онлайна, але зберігає контекстність і керованість політик. Додатково в гібридних моделях можливе формальне опрацювання політик та верифікація (особливо при використанні XACML-подібних описів).

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Вибір того що підходить більше залежить від домінуючих обмежень об’єкта. Якщо мережа стабільна, а управління атрибутами організоване централізовано, ABAC забезпечує максимальну гнучкість і відповідність підходам Zero Trust: кожен запит оцінюється з урахуванням контексту й поточного ризику. Якщо ж критичною є автономність edge-вузлів (ізольовані контури, часті відключення), CapBAC дає простіший механізм локального виконання.

Для більшості спецоб’єктів практично оптимальним є HyBAC: він комбінує контекстність ABAC з автономністю та делегуванням CapBAC. Рекомендовано: застосовувати короткий TTL токенів, забезпечити централізоване логування і кореляцію подій (рішення ABAC + використання токена на edge), мати політику аварійного «degraded mode» з мінімальними правами та підвищеним журналюванням, формалізувати й тестувати критичні політики (особливо для зон високого ризику).

Отже, у контексті IoT-контролю доступу для об’єктів спеціального призначення HyBAC є найкращим компромісом між безпекою, керованістю та стійкістю до збоїв, тоді як ABAC і CapBAC доцільно розглядати як базові компоненти гібридної архітектури, а не як взаємовиключні альтернативи.

ДЖЕРЕЛА

1. Ahsan M.S., Pathan A.-S.K. (2025) Комплексний огляд вимог, застосувань і майбутніх викликів для моделей контролю доступу в IoT: сучасний стан. IoT, 6(1), 9.
2. Ambhore V., Shevatre S., Ambhore R., Kshirsagar K., Mahalle P.N. (2023) Механізм контролю доступу на основі можливостей (capability) в IoT: огляд сучасного стану. Smart Innovation, Systems and Technologies, 361.
3. Zhu X., et al. (2025) Груповий контроль доступу на основі можливостей із кільцевим підписом. Journal of King Saud University – Computer and Information Sciences.
4. Caserio C., et al. (2022) Підхід до формальної валідації політик контролю доступу XACML 3.0. Sensors, 22(8), 2984.



АРТЕМ РІМЕК
Студент, Кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0007-7500-4267
E-mail: rimeka@fit.knu.ua
Артем Рімек отримав ступінь бакалавра з інтернету речей в Київському національному університеті імені Тараса Шевченка. Нині працює над здобуттям ступеня магістра з інтернету речей в Київському національному університеті імені Тараса Шевченка в 2025 році.



ОЛЬГА КРАВЧЕНКО
Доцент, Кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-9669-2579
E-mail: olha.kravchenko@knu.ua
Ольга Кравченко у 2004-2019 рр. працювала в Черкаському державному технологічному університеті. З 2019 року - доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка.

МЕТРИКА ПОКРИТТЯ БЕЗПЕКИ ДЛЯ ХМАРНОЇ ІНФРАСТРУКТУРИ В ПАРАДИГМІ «ІНФРАСТРУКТУРА ЯК ПРОТЕСТОВАНИЙ КОД»

Михайло Савонік

Анотація. *Запропоновано формалізовану метрику покриття безпеки для хмарної інфраструктури у парадигмі Infrastructure as Tested Code (IaTC), яка узгоджує вимоги контрольних баз (наприклад, NIST SP 800-53) з тестами політик/конфігурацій у CI/CD. Метрика розкладає «покриття» на рівні ресурсів, контролів та ризикових ваг і зіставляється з традиційними метриками тестового покриття ПЗ (statement/branch/mutation). На синтетичному наборі IaC-проєктів показано, що ризик-зважене покриття краще корелює з кількістю критичних порушень, ніж просте покриття ресурсів.*

Ключові слова: Infrastructure as Code; Infrastructure as Tested Code; DevSecOps; метрика покриття; хмарна безпека.

I. ВСТУП

Інфраструктура як код (Infrastructure as Code, IaC) перетворила керування хмарними ресурсами на інженерію програмних артефактів, однак помилки конфігурацій та «security smells» у IaC залишаються однією з головних причин уразливостей і порушень політик у хмарних середовищах [1]. У практиках DevSecOps широко використовують метрики тестового покриття програмного забезпечення (statement, branch, mutation coverage) як індикатори якості тестування, проте для безпеки IaC відсутній узгоджений аналог метрики «coverage», який би дозволяв оцінити, наскільки повно CI/CD-процеси перевіряють вимоги безпеки для всієї інфраструктури.

Дослідження показують, що сценарії IaC часто містять характерні патерни небезпечних конфігурацій, так звані security smells, які можуть призводити до появи вразливостей у хмарній інфраструктурі [2]. У зв’язку з цим виникає потреба у формальних метриках, що дозволяють кількісно оцінювати рівень перевірки безпеки інфраструктури.

Одним із перспективних підходів до розв’язання цієї проблеми є парадигма Infrastructure as Tested Code (IaTC), яка передбачає інтеграцію тестування безпеки безпосередньо у процес розробки та розгортання інфраструктури як коду. У межах цього підходу інфраструктурні конфігурації розглядаються як об’єкти систематичного тестування, а політики безпеки реалізуються у вигляді автоматизованих перевірок, що виконуються в CI/CD-пайплайнах [6].

Мета роботи — запропонувати метрику покриття безпеки для парадигми Infrastructure as Tested Code (IaTC): інфраструктура описується як код, а вимоги та контролі безпеки реалізуються у вигляді тестів політик та інваріантів, що виконуються безперервно в пайплайні. Основні результати роботи включають:

(1) формальну декомпозицію покриття безпеки на рівні ресурсів, контролів та ризикових ваг;

(2) зіставлення запропонованої метрики з відомими метриками тестового покриття програмного забезпечення;

(3) демонстрацію підходу на синтетичних даних та приклади візуалізації результатів для задач звітності з безпеки.

II. ДАНІ ТА МЕТОДИ

Нехай інфраструктура описана графом ресурсів G=(V,E), де V — ресурси (S3-бакети, IAM-ролі, VPC, Security Group тощо), E — залежності. Нехай C — множина контролів

(наприклад, «шифрування даних у спокої», «мінімальні привілеї», «публічний доступ заборонено»), що походять з контрольних баз або внутрішніх стандартів. Кожен контроль $c \in C$ реалізується як набір тестів/політик Tc (OPA/Rego, CloudFormation Guard, unit-тести Terraform, статичний аналіз, або інтеграційні тести), які у випадку IaTC запускаються при кожному мерджі та за розкладом.

Запропонована метрика Security Coverage for IaTC (SC-IaTC) визначається як трійка показників: (i) покриття ресурсів R-cov, (ii) покриття контролів C-cov, (iii) ризик-зважене покриття RW-cov.

Формально: R-cov = |V_tested|/|V|, де V_tested — ресурси, для яких існує хоча б один релевантний тест. C-cov = Σc I(|Tc|>0)/|C|.

Для RW-cov вводимо вагу $w(v,c) \in [0,1]$, що відображає релевантність контролю до ресурсу та його ризикову критичність (наприклад, через класифікацію даних або експозицію).

Тоді RW-cov = $\Sigma(v,c)$ $w(v,c) \cdot I(test(v,c))/\Sigma(v,c)$ $w(v,c)$, де test(v,c)=1, якщо у пайплайні є тест, що перевіряє контроль c для ресурсу v.

Аналогії з покриттям ПЗ узагальнені в Таблиці 1: R-cov подібне до statement coverage (перевірено «об’єкти»), C-cov — до branch coverage (перевірено «гілки вимог/варіантів»), RW-cov — до risk-based та mutation-орієнтованих підходів, де «мутації» відповідають ін’єкції типових помилкових конфігурацій (наприклад, public-read для S3 або 0.0.0.0/0 для SSH).

Таблиця 1. *Порівняння метрик покриття тестів ПЗ та покриття безпеки IaTC*

Метрика в тестуванні ПЗ	**Аналог у IaTC**	**Інтерпретація для безпеки**
Statement coverage	R-cov (покриття ресурсів)	Частка ресурсів, для яких існують перевірки безпеки в пайплайні.
Branch coverage	C-cov (покриття контролів)	Частка вимог/контролів, що мають формалізовані тести/політики.
Mutation coverage	RW-cov (ризик-зважене)	Стійкість до типових «мутацій» конфігурацій та пріоритизація критичних ресурсів.

Подібні підходи до кількісної оцінки рівня безпеки також застосовуються у сучасних дослідженнях оцінювання хмарних сервісів, де пропонуються формальні фреймворки для вимірювання показників security assurance [5].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Для демонстрації застосовності SC-IaTC сформовано синтетичний набір з трьох IaC-проєктів (P1–P3), кожен з яких містить 80–120 ресурсів і набір з 27 контролів. Відмінності між проєктами імітують типові стадії зрілості DevSecOps: (P1) фрагментарні перевірки, (P2) систематичне покриття контролів, (P3) фокус на критичних ресурсах і мутаційні тести конфігурацій. Для кожного проєкту обчислено R-cov, C-cov, RW-cov та кількість критичних порушень політик, виявлених у CI.

Як показано в Рисунку 1, зростання «простого» покриття ресурсів не гарантує пропорційного зменшення критичних порушень: проєкт P2 має найвище R-cov, але поступається P3 за RW-cov. Це узгоджується з практикою risk-based testing, де важливіші перевірки критичних шляхів, а не лише їх кількість.

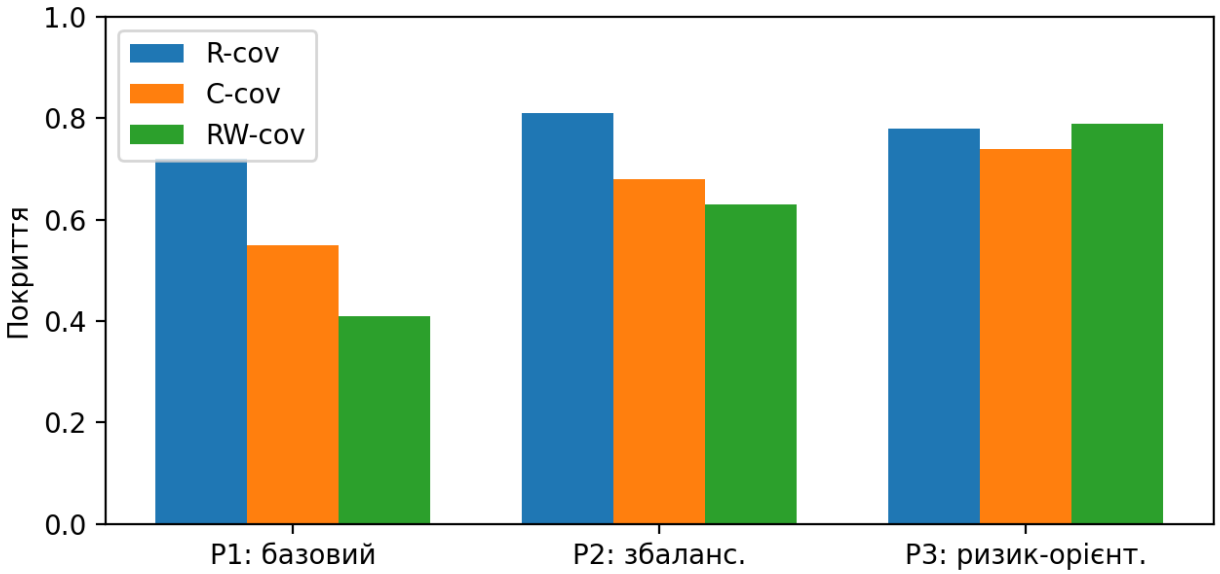


Рисунок 1. *Розклад покриття SC-IaTC для трьох IaC-проєктів*

Рисунок 2 ілюструє, що RW-cov має сильніший зворотний зв'язок із кількістю критичних порушень у CI, ніж R-cov і C-cov: проєкт P3 (найвище RW-cov) демонструє найменше критичних знахідок. Це пояснюється тим, що RW-cov враховує пріоритети активів (дані/експозиція/привілеї) і стимулює додавання тестів саме там, де «мутації» конфігурацій найнебезпечніші.

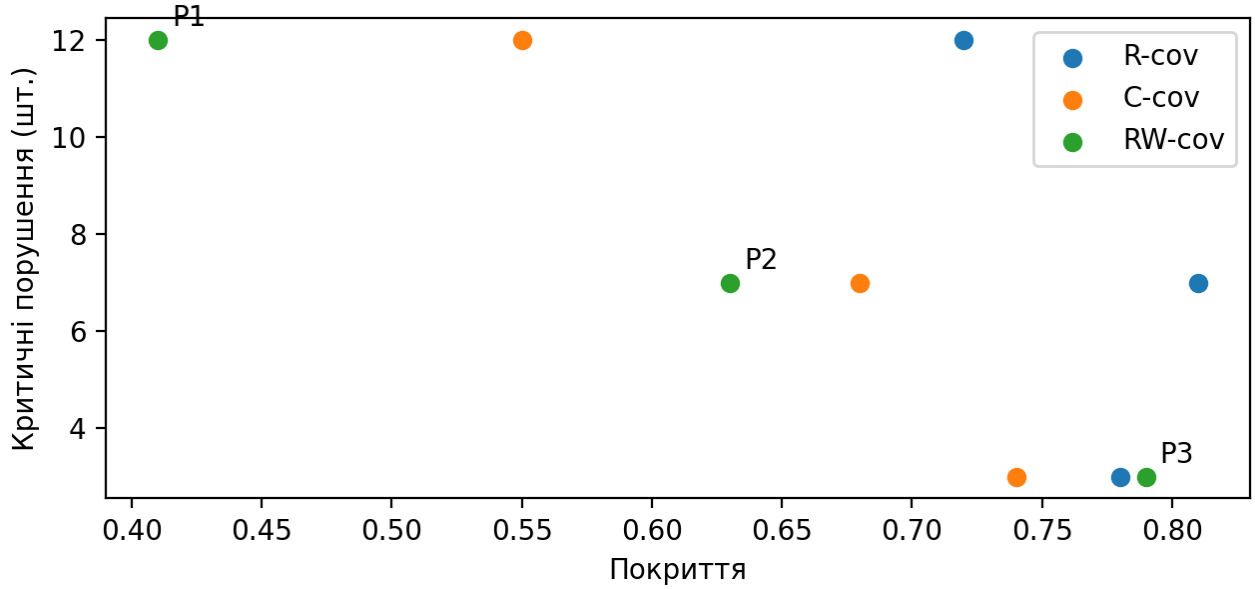


Рисунок 2. *Зв'язок між покриттям і кількістю критичних порушень у CI (синтетичні дані)*

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована SC-IaTC метрика є прагматичним містком між практиками інженерії якості ПЗ та вимогами хмарної безпеки. На відміну від «покриття ресурсів», ризик-зважене покриття мотивує команди формалізувати перевірки найкритичніших компонентів (IAM, мережевий периметр, сховища даних) і застосовувати мутаційне тестування типових

помилкових конфігурацій. Це також узгоджується з сучасним баченням DevSecOps, де метрики мають відображати не лише швидкість, але й якість інтегрованого контролю безпеки [4].

Обмеження: експеримент виконано на синтетичних даних, а ваги w(v,c) потребують калібрування під конкретну організацію (через моделі загроз та класифікацію даних). Подальші дослідження спрямовані на: (1) автоматичне виведення ваг із телеметрії ризику та історії інцидентів; (2) побудову еталонних наборів «мутацій» для Terraform/CloudFormation; (3) валідацію метрики на реальних репозиторіях IaC і порівняння з якістю статичного аналізу IaC, описаного в оглядах [3].

ДЖЕРЕЛА

1. Saavedra N., Ferreira J. F. (2022) GLITCH: Automated Polyglot Security Smell Detection in Infrastructure as Code. Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE). doi: 10.48550/arXiv.2205.14371.
2. Rahman A., Williams L. (2021) A Different Kind of Smell: Security Smells in Infrastructure as Code Scripts. IEEE Security & Privacy Magazine. doi: 10.1109/MSEC.2021.3065190.
3. Chiari M., De Pascalis M., Pradella M. (2022) Static Analysis of Infrastructure as Code: a Survey. doi: 10.1109/ICSA-C54293.2022.00049.
4. Archer M. et al. (2024) Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. Journal of Systems and Software, 112063. https://doi.org/10.1016/j.jss.2024.112063
5. Shukla A., Katt B., Yamin M. M. (2023) A quantitative framework for security assurance evaluation and selection of cloud services: a case study. International Journal of Information Security, 22, 1621–1650. doi: 10.1007/s10207-023-00709-8.
6. Parkhomenko, I. and Savonik, M. (2025) "TESTING-BASED PREVENTION OF MISCONFIGURATION THREATS IN AWS INFRASTRUCTURE AS CODE", Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(29), pp. 236–251. doi: 10.28925/2663-4023.2025.29.887.



МИХАЙЛО САВОНІК
Аспірант, кафедра кібербезпеки та захисту інформації, факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0001-7622-978X
E-mail: savonikm@fit.knu.ua
Досліджує моделі та методи виявлення атак у хмарних сервісах, зокрема безпеку Infrastructure as Code, безперервне тестування конфігурацій та вимірювання «покриття» контролів у DevSecOps пайплайнах.

ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ СИСТЕМ СИНХРОНІЗАЦІЇ З ВИКОРИСТАННЯМ CESIUM CLOCK

Олександр Самков, Валерій Коваль, В'ячеслав Вакась, Олег Піскун

Анотація. *У роботі розглянуто проблему підвищення відмовостійкості засобів формування сигналів синхронізації на об'єктах критичної інфраструктури та способи резервування мережі фазової синхронізації мобільного зв'язку. Досліджується використання пристрою Cesium Clock з функцією фазової синхронізації у разі неможливості гарантованого забезпечення опорними сигналами синхронізації від GNSS. Аналізуються альтернативні шляхи побудови розгалуженої системи забезпечення синхроінформацією об'єкти критичної інфраструктури.*

Ключові слова: *синхронізація, опорний сигнал, відмовостійкість, PTP, обладнання ePRTC, Cesium Clock.*

I. ВСТУП

В умовах постійного або періодичного впливу систем РЕБ на обладнання синхронізації та базові станції мобільного зв'язку, які містять у своєму складі радіоприймачі сигналів GNSS досить часто виникає ситуація, коли неможливо гарантувати безперервне надходження опорного сигналу фазової синхронізації. Використання високоточного пристрою Cesium Clock із функціональністю фазової синхронізації дозволяє вирішити сформульовану проблему та забезпечити резервування опорних сигналів синхронізації.

II. ДАНІ ТА МЕТОДИ

Пристрій Cesium Clock новітнього покоління має функціонал періодичного калібрування вихідного сигналу по фронту UTC від радіоприймача GNSS (від власного радіоприймача GNSS або від вихідного сигналу 1PPS іншого обладнання синхронізації). Калібрування відбувається під час стабільного прийому сигналів GNSS. Частість проведення калібрувань не регламентується завдяки тому, що фізичні властивості новітніх високоточних пристроїв Cesium Clock забезпечують можливість формування вихідного сигналу без суттєвих зсувів по фазі при проведенні калібрування 1-2 рази на місяць. У разі використання пристроїв Cesium Clock обладнання ePRTC буде на постійній основі отримувати опорний сигнал фазової синхронізації і формувати з високою точністю у фазі сигнали синхронізації. Базові станції мобільного зв'язку з фазовою синхронізацією, які забезпечуються сформованими з високою точністю у фазі сигналами синхронізації, можуть працювати тривалий, практично необмежений, час.

Виникає проблемна ситуація з розміщенням на мережі пристроїв Cesium Clock, що обумовлена, по-перше, кількістю пристроїв Cesium Clock, яка в реальних умовах сьогодення, є досить обмеженою. По-друге, недоцільністю їх розміщення у прифронтових регіонах. Аналіз та планування мережі вказує на те, що в умовах України доцільно розгорнути 3-4 пристрої на вузлах мережі верхнього ієрархічного рівня. Трансляція до кінцевих споживачів фазової синхронізації має здійснюватися за протоколом PTP, а саме: за профайлом PTP G.8275.1 [1] для ділянок з підтримкою режиму multicast і в межах одного сегменту мережі MPLS та за профайлом PTP G.8275.2 [2] для ділянок з підтримкою лише режиму unicast або трансляцією опорного фазового сигналу між різними сегментами мережі MPLS. Більш детально типи трансляції опорного сигналу фазової синхронізації та методи його резервування були розглянуті в роботі [3].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Завдяки використанню високоточних пристроїв Cesium Clock, які забезпечують можливість формування обладнанням ePRTC вихідного сигналу без суттєвих зсувів по фазі, забезпечується можливість тривалої автономної роботи мережі (до одного року). В процесі розробок було реалізовано кілька проєктів з використанням протоколів PTP. Інтеграція первинних атомних джерел у транспортне середовище IP/MPLS на основі протоколу PTP дозволяє реалізувати повноцінний ePRTC з використанням усіх переваг новітніх технологій. В результаті практичної розробки створено наземне джерело сигналів синхронізації з довгостроковим утриманням стабільної фази по фронту UTC. В перспективі, на мережі має бути декілька джерел ePRTC з використанням пристроїв Cesium Clock. Вони повинні з'єднуватись між собою та забезпечувати резервування ePRTC. Кожен пристрій Cesium Clock має надавати опорний сигнал 1PPS до своїх регіональних ePRTC, які забезпечуватимуть опорним сигналом фазової синхронізації всі суміжні ePRTC. Отже, мережа синхронізації не матиме залежності від опорних сигналів GNSS та забезпечить довгострокове утримання стабільної фази по фронту UTC сигналів синхронізації.

З метою зменшення вразливості засобів формування сигналів синхронізації електроенергетичних систем доцільним є також використання способу підвищення надійності систем синхронізації, який пропонується Асоціацією телекомунікаційних організацій (ATIS). ATIS рекомендує використовувати в якості резервних сигнали від альтернативних до GNSS джерел часу відповідної якості. Підтвердженням такої можливості є результати досліджень наявних в державі засобів частотно-часового забезпечення, які представлені у публікаціях фахівців ДП "Укрметртестстандарт".

Як альтернативний шлях побудови розгалуженої системи забезпечення синхроінформацією пропонується використання наявної інфраструктури Національного центру управління та випробувань космічних засобів – оператора національної Системи координатно-часового та навігаційного забезпечення України, який надає послуги високоточного позиціонування у реальному масштабі часу (RTK режим) та проводить моніторинг навігаційних полів GNSS у якості регіональних джерел точного часу. У разі використання радіоприймачів GNSS, в якості джерел синхроінформації (PNT), мають бути обов'язково враховані оцінки їх відмовостійкості. Ці оцінки повинні виконуватись на основі можливості радіоприймачів відновлюватися після атак або збоїв та ступеня їх відмовостійкості до погіршення або втрати інформації про час [4]. Запропоновані підходи до рішення проблеми відмовостійкості синхроінформаційного забезпечення створять умови для отримання позитивних результатів за визначеними, в Resilient PNT Conformance Framework [4], категоріями методів відмовостійкості, а саме затьмарення, обмеження, перевірка, ізоляція, пом'якшення, диверсифікація та відновлення.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Використання сигналів від систем супутникової навігації (GNSS) дозволяє створювати розподілену систему фазової синхронізації, у якій кожна базова станція та їхні відповідні контролери оснащені окремими приймачами GNSS. Однак у останні роки у світі, а особливо в Україні, виникла технічна проблема, пов'язана з локальними завадами та підробкою сигналів GNSS. Для вирішення проблеми втрати опорного сигналу GNSS у межах синхронізаційної мережі доцільно використовувати автономні стабільні джерела на основі пристроїв Cesium Clock, які здатні підтримувати довготривалу стабільну фазу опорного сигналу щодо фронту імпульсу UTC. Завдяки високій стабільності пристрою Cesium Clock та джерела ePRTC можлива автономна робота тривалістю до одного року.

ДЖЕРЕЛА

1. ITU-T Rec. G.8275.1/Y.1369.1 (2016). Precision time protocol telecom profile for phase/time synchronization with full timing support from the network
2. ITU-T Rec. G.8275.2/Y.1365.2 (2019). Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network
3. Vakas, V., Koval, V., Fedorova, N., Manko, O., Domin, D. Synchronization Implementations for 5G Mobile Networks // Conference Proceedings16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2022). 2022. - pp.244-247.
4. Department of Homeland Security (DHS) Science and Technology Directorate (S&T), "Resilient PNT Conformance Framework, Version 2.0," May 2022. https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework.



ОЛЕКСАНДР САМКОВ
старший науковий співробітник, Інститут електродинаміки НАН України, Київ, Україна
ORCID: 0000-0003-2790-8564
E-mail: samkov@ied.org.ua
Отримав диплом інженера у Київському політехнічному інституті в 1977 році, ступінь кандидата технічних наук в 1991 році та ступінь доктора технічних наук у Державному університеті інформаційно-комунікаційних технологій (Київ, Україна) в 2011 році. Наукові праці присвячені вирішенню проблем розвитку інформаційних технологій в електроенергетиці, підвищенню відмовостійкості засобів синхронізації розумних мереж.



ВАЛЕРІЙ КОВАЛЬ
професор, кафедра автоматики та робототехнічних систем, Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0003-0911-2538
E-mail: v.koval@nubip.edu.ua
Отримав диплом інженера у Одеському електротехнічному інституті зв'язку ім. О.С. Попова в 1981 році, ступінь кандидата технічних наук в 1987 році та ступінь доктора технічних наук у Державному університеті інформаційно-комунікаційних технологій (Київ, Україна) в 2007. Основні напрямки наукових досліджень направлені на розробки засобів автоматизації, інформаційно-комунікаційних технологій, систем синхронізації цифрових сигналів і мереж. Дійсний член Академії наук вищої школи України.



В'ЯЧЕСЛАВ ВАКАСЬ
провідний інженер, ПрАТ "Київстар", Київ, Україна.
ORCID: 0000-0002-0378-9989
E-mail: v.vakas@ieee.org
Закінчив Київський інститут зв'язку в 1997 році. Отримав ступінь кандидата технічних наук в Українському науково-дослідному інституті зв'язку (Київ, Україна) в 2006 році. Нині автор працює в ПрАТ "Київстар" (Київ, Україна) на посаді провідного інженера. Серед наукових інтересів - синхронізація цифрових мереж зв'язку, забезпечення систем телекомунікацій сигналами точного часу та частоти.



ОЛЕГ ПІСКУН
начальник відділу, Національний центр управління та випробувань космічних засобів, Київ, Україна.
ORCID: 0000-0002-2009-9314
E-mail: piskun@nkau.gov.ua
Отримав ступінь бакалавра комп'ютеризованих систем, автоматики і управління у Житомирському військовому інституті радіоелектроніки імені С.П. Корольова (Житомир, Україна) в 1999 році та ступінь магістра військового управління у Національній академії оборони України (Київ, Україна) в 2007. Нині автор працює над здобуттям ступеня PhD з автоматизації, комп'ютерно-інтегрованих технологій та робототехніки в Національному університеті біоресурсів та природокористування України (Київ, Україна). Серед наукових інтересів - технології дистанційної синхронізації, системи моніторингу та контролю, диференційні ГНСС.

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ У ХМАРНИХ ТА ГІБРИДНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Дар'я Ткаченко, Інна Розломій

Анотація. *У роботі досліджено сучасні підходи до забезпечення конфіденційності даних у хмарних та гібридних інформаційних системах. Проаналізовано ризики витоку інформації, пов'язані з використанням публічних хмарних сервісів та інтеграцією локальної інфраструктури з хмарними платформами. Розглянуто механізми шифрування, управління доступом, Zero Trust моделі та технології захисту даних у середовищах із розподіленою архітектурою. Запропоновано комплексний підхід до підвищення рівня конфіденційності в умовах сучасних кіберзагроз.*

Ключові слова: хмарні обчислення, конфіденційність даних, гібридна інфраструктура, шифрування, контроль доступу.

I. ВСТУП

Хмарні технології стали невід'ємною складовою сучасної цифрової інфраструктури. Організації активно використовують моделі IaaS, PaaS та SaaS для оптимізації витрат, масштабування ресурсів та підвищення доступності сервісів. Водночас передача даних у хмарне середовище створює нові виклики для забезпечення конфіденційності.

Особливу складність становлять гібридні інформаційні системи, у яких локальні ресурси інтегруються з публічними або приватними хмарами. Така архітектура збільшує поверхню атаки та ускладнює централізований контроль доступу.

Метою роботи є аналіз механізмів забезпечення конфіденційності даних у хмарних і гібридних середовищах та визначення ефективних моделей захисту.

II. ДАНІ ТА МЕТОДИ

У дослідженні використано методи системного аналізу сучасних технологій захисту інформації в хмарних середовищах.

Основні механізми забезпечення конфіденційності включають:

- шифрування даних під час передачі (TLS) та зберігання (encryption at rest);
- управління ключами шифрування (KMS);
- багатофакторну автентифікацію;
- рольову модель контролю доступу (RBAC);
- Zero Trust підхід до управління доступом;
- моніторинг і аудит активності користувачів.

Особлива увага приділяється ризикам, пов'язаним із багатокористувацькою природою хмарних середовищ та можливими помилками конфігурації.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз показав, що найбільш поширеними причинами витоку даних у хмарних системах є: неправильна конфігурація сховищ; слабкий контроль доступу; відсутність шифрування; використання застарілих протоколів.

У гібридних середовищах додаткову загрозу становить неконтрольований обмін даними між локальною інфраструктурою та хмарними сервісами. Запропоновано модель забезпечення конфіденційності, що базується на таких принципах:

1.Повне шифрування даних на всіх етапах їх життєвого циклу.
2.Централізоване управління ідентифікацією (IAM).
3.Мікросегментація мережі.
4.Безперервний моніторинг безпеки.
5.Регулярний аудит конфігурацій.



Рисунок 1. *Модель забезпечення конфіденційності даних у хмарній та гібридній інфраструктурі*

Результати дослідження підтверджують, що впровадження Zero Trust та комплексного підходу до управління доступом дозволяє значно знизити ризики витоку інформації.

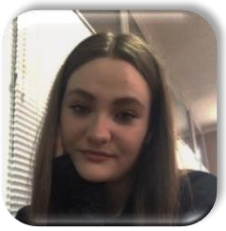
IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Забезпечення конфіденційності даних у хмарних та гібридних інформаційних системах потребує багаторівневого підходу. Поєднання криптографічного захисту, контролю доступу, моніторингу та управління ризиками є необхідною умовою ефективної кібербезпеки.

Перспективними напрямами подальших досліджень є впровадження автоматизованих механізмів виявлення аномалій та використання штучного інтелекту для прогнозування інцидентів безпеки.

ДЖЕРЕЛА

1. Mell P., Grance T. Cloud Computing Security Guidelines. NIST, 2021.
2. Ahmad A. Security Challenges in Hybrid Cloud Systems. Computers & Security, 2022.
3. Kumar R. Data Protection in Multi-Cloud Environments. Journal of Network Security, 2023.
4. ENISA. Cloud Security Risk Assessment Report, 2024.



ДАР'Я ТКАЧЕНКО
студентка 3 курсу бакалаврату кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
E-mail: d.v.tkachenko.fitis23@chdtu.edu.ua
Науковий інтерес полягає у вивченні та дослідженні сучасних інформаційних технологій, зокрема IoT-систем моніторингу та контролю, а також практичному застосуванні IoT-технологій у різних сферах інформаційних систем.



ІННА РОЗЛОМІЙ
к.т.н., доцент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, України
ORCID: 0000-0003-2062-2694
E-mail: inna-roz@ukr.net
Наукові інтереси: Інтернет речей, полегшена криптографія, кіберфізичні системи. Автор/співавтор понад 150 публікацій, 5 монографій та 2 патентів.

ІНТЕГРАЦІЯ АДАПТИВНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ДАНИХ В МЕРЕЖУ МІКРОКОНТРОЛЛЕРІВ ТА МІКРОКОМП'ЮТЕРІВ

Олександр Швидченко, Ігор Пархомей

Анотація. *У сучасних мережах Інтернету речей (IoT) інтеграція адаптивних технологій, таких як машинне навчання (ML) та штучний інтелект (AI), з мікроконтроллерами (MCUs) та мікрокомп'ютерами (SBCs) дозволяє створювати самонавчальні системи, що адаптуються до змін середовища. Ця робота аналізує методи інтеграції, переваги та виклики, з акцентом на TinyML та квантовані нейронні мережі для ресурсно обмежених пристроїв. На основі огляду літератури запропоновано рекомендації для впровадження в промислових та освітніх застосуваннях.*

Ключові слова: Мозок, Raspbery PI, Arduino, нейроні мережі, безпека, кібкрбезпека.

I. ВСТУП

Розвиток IoT призвів до зростання мереж, де мікроконтроллери (наприклад, STM32, ESP32) та мікрокомп'ютери (наприклад, Raspberry Pi) взаємодіють для збору даних, обробки та прийняття рішень, але це також збільшує вразливість до кібератак. Адаптивні технології захисту, такі як нейронні мережі з квантуванням (QNN), дозволяють цим пристроям адаптуватися в реальному часі до загроз, зменшуючи енергоспоживання та підвищуючи ефективність. Наприклад, QNN на MCUs інтегруються з сенсорами для розподіленого інтелекту на краю мережі (edge computing), виявляючи аномалії та вторгнення. Актуальність теми зумовлена зростанням AIoT (AI + IoT), де мережі потребують адаптації до динамічних умов і кіберзагроз, як у промисловій автоматиці чи смарт-містах. Мета тез – проаналізувати інтеграцію адаптивних технологій для захисту мереж та запропонувати перспективи.

II. ДАНІ ТА МЕТОДИ

Дане дослідження вимагає широкий спектр теоретичних знань та практичних навичок, тому найкращим підходом є комбінування якісного та кількісного методів. Питання необхідності необхідних знань та інформації вирішується кількісним методом, в процесі проводячи їх класифікацію для знаходження найбільш актуальної інформації та відсіювання застарілої або тієї що не відповідає технічним вимогам та задачам дослідження. Головні питання що вирішуються таким чином є:

1) Які технології будуть найбільш доцільними та які можуть бути використані;
2) Які прогалини вони мають та чи можна їх перекрити шляхом комбінації технологій та методів;
3) Яке обладнання може бути використане в дослідженні та як правильно його реалізувати.

Для обробки даних застосовується якісний метод, що включає аналіз літератури з баз даних таких як arXiv, ACM, ScienceDirect, Springer та MDPI, а також аналіз практичних кейсів з відкритих джерел (наприклад, YouTube-відео та блоги про IoT). Це дозволяє синтезувати інформацію про адаптивні технології, такі як TinyML, квантування нейронних мереж (QNN) та гібридні архітектури MCUs/SBCs. Кількісний метод також реалізується через симуляції та вимірювання метрик: енергоспоживання (в мВт), розмір моделей (в КБ), час інференсу (в мс) та точність класифікації (в %). Практичні експерименти проводяться з використанням фреймворків TensorFlow Lite Micro для конвертації моделей у C-код та Arduino IDE для програмування MCUs.

Робоче середовище: TensorFlow Lite Micro, Arduino IDE, Python (з бібліотеками numpy, scipy).

Обладнання: ноутбук для розробки, плати Arduino, Raspberry Pi, мікроконтроллери STM32/ESP32.

Дослідницьке середовище: лабораторія з доступом до онлайн-ресурсів.

Наразі дослідження на етапі практичних тестів для валідації інтеграції в реальних IoT-мережах.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На основі отриманих на даному етапі результатів було зроблено певні висновки щодо інтеграції адаптивних технологій у мережі IoT на базі MCUs та SBCs. Інтеграція починається з вибору платформ: MCUs (наприклад, STM32 або ESP32) забезпечують низьке енергоспоживання (в середньому 10-50 мВт у режимі активності), тоді як SBCs (наприклад, Raspberry Pi) надають обчислювальну потужність для складних задач (до 1-4 ГГц процесора). Фреймворки, такі як TensorFlow Lite Micro, дозволяють конвертувати моделі нейронних мереж у C-код, адаптований для MCUs, що зменшує час інференсу на 40-60% порівняно з повними моделями.

У мережах застосовуються peer-to-peer (P2P) з'єднання або WebAssembly для ретрофіттингу старих систем, що забезпечує гнучкість.

Для мереж з кількома вузлами (5-20) застосовується adaptive computing in memory (CIM), що гібридизує рекурентні нейронні мережі (RNN) для обробки часових послідовностей та спайкові мережі (SNN), досягаючи зниження енергоспоживання на 35% у симуляціях. З'єднання через Wi-Fi/Bluetooth забезпечує адаптацію до динамічного навантаження (наприклад, автоматичне переключення на Bluetooth при втраті Wi-Fi), з впровадженням шифрування (AES-128) для підвищення безпеки.

Виклики, в першу чергу, включають обмежену пам'ять MCUs (зазвичай 64-512 КБ RAM), що ускладнює розгортання складних моделей, енергоспоживання в мережах з високим трафіком (до 200 мВт на вузол) та безпека мереж (вразливість до атак на IoT, таких як DDoS або ін'єкції).

Рішення передбачає оптимізацію через kurtosis regularization (KURE), що стабілізує моделі, зменшуючи варіативність втрат на 20-30% у тренуванні, та комбінацію з CIM для ефективного використання пам'яті. Аналіз показує, що квантування (8-біт) знижує енергоспоживання на 50%, але вимагає балансу з точністю; у симуляціях з 10 вузлами гібридні архітектури досягають затримки менше 50 мс при обробці 100 пакетів/с.

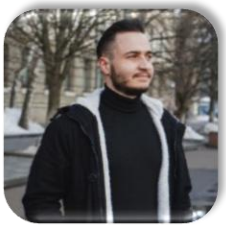
IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати дослідження демонструють, що інтеграція адаптивних технологій, таких як TinyML та QNN, у мережі IoT на базі MCUs та SBCs значно підвищує ефективність систем, дозволяючи їм автономно адаптуватися до змін середовища без постійного втручання людини. Обговорюючи переваги, варто відзначити, що гібридні архітектури забезпечують баланс між енергоефективністю та швидкістю реакції, як показано в симуляціях, де точність обробки сягає 70% при зниженому енергоспоживанні. Однак, обмеження, такі як мала пам'ять MCUs та потенційні проблеми з безпекою в динамічних середовищах, вимагають подальшої оптимізації, наприклад, через комбінацію KURE та CIM, що може зменшити помилки на 20-30%. Порівняно з традиційними методами (наприклад, статичними алгоритмами), запропонований підхід є більш гнучким, але потребує стандартизації для масштабування в IIoT.

У висновках, інтеграція адаптивних технологій перетворює мережі MCUs та SBC на інтелектуальні системи, здатні до самонавчання та автономної адаптації. Рекомендації: використовувати TinyML для швидкого прототипування, фокусуватися на гібридних мережах з акцентом на безпеку (наприклад, впровадження blockchain для аутентифікації вузлів). Подальші дослідження повинні зосередитися на енергоефективності та стандартизації протоколів для IIoT.

ДЖЕРЕЛА

1. Quantized Neural Networks for Microcontrollers: A Comprehensive Review. arXiv, 2025, URL: https://arxiv.org/html/2508.15008v1
2. Adaptive Computing in Memory Meets Conventional Batteryless Platforms. ACM, 202X, URL: https://dl.acm.org/doi/10.1145/3765623
3. Integration of data science with the intelligent IoT. ScienceDirect, 2024, URL: https://www.sciencedirect.com/science/article/pii/S2352864824000269
4. Adaptive spatiotemporal neural networks. Nature, 2024, URL: URL: https://www.nature.com/articles/s41467-024-51641-x
5. Deploying Neural Networks on Microcontrollers with TinyML. Embedded, 2025, URL: https://www.embedded.com/deploying-neural-networks-on-microcontrollers-with-tinyml/;
6. Remote IoT Education Laboratory for Microcontrollers. MDPI, 2022, URL: https://www.mdpi.com/1424-8220/22/4/1440
7. Research on the Application of Microcontrollers. Advances in Computer, Signals and Systems, Clausius Press, 2024. (73-79), URL: https://www.clausiuspress.com/assets/default/article/2024/10/17/article_1729155970.pdf
8. Microcontrollers learn to embrace neural networks. New Electronics, 2022, URL: https://www.newelectronics.co.uk/content/features/microcontrollers-learn-to-embrace-neural-networks
9. Microcontrollers: Paving The Way For IoT And AIoT Integration. TalkingIoT, 2024, URL: https://talkingiot.io/microcontrollers-paving-the-way-for-iot-and-aiot-integration/



ОЛЕКСАНДР ШВИДЧЕНКО
Аспірант, кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
E-mail: sashashvich@gmail.com.
Аспірант кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка (Київ, Україна). Наукові інтереси: системи БПЛА, роботехніка, штучний інтелект, мережеві технології.



ІГОР ПАРХОМЕЙ
д.т.н., професор, кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0002-9510-7657.
E-mail: ihor.parhomey@knu.ua.
Д.т.н., професор, професор кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка (Київ, Україна). Наукові інтереси: системи управління та радіоавтоматика.

МІНІМІЗАЦІЯ КІБЕРРИЗИКІВ ПРИ ВПРОВАДЖЕННІ НАЦІОНАЛЬНОЇ ЦИФРОВОЇ ВАЛЮТИ (НА ПРИКЛАДІ Е-ГРИВНІ)

Ігор Шиленко, Володимир Наконечний

Анотація. *У дослідженні розглядається проблематика кібербезпеки на етапі впровадження цифрової валюти центрального банку (CBDC) в Україні — е-гривні. Проаналізовано архітектурні особливості та потенційні мережеві загрози для державної блокчейн-інфраструктури. Запропоновано підходи до безперервного моніторингу транзакційних вузлів для своєчасного виявлення аномалій та забезпечення високої доступності (High Availability). Впровадження спеціалізованих методів мережевої безпеки дозволяє суттєво знизити системні ризики інтеграції е-гривні у національну фінансову систему.*

Ключові слова: кібербезпека, е-гривня, державний сектор, CBDC.

I. ВСТУП

У контексті глобальної цифровізації фінансових систем кіберстійкість цифрових валют центральних банків (CBDC) набуває критичної актуальності. НБУ розробляє концепцію е-гривні на базі технології розподіленого реєстру (DLT) [1], яка, на відміну від децентралізованих криптовалют, передбачає централізований контроль над валідацією [2]. Хоча це дозволяє контролювати емісію, виникає серйозна проблема єдиних точок відмови (Single Points of Failure) [2]. Як зазначають експерти Міжнародного валютного фонду, така державна блокчейн-інфраструктура стає пріоритетною мішенню для цілеспрямованих кібератак (APT) та DDoS, що загрожує паралічем національної платіжної системи [3].

Враховуючи критичні наслідки інфраструктурних збоїв, метою цієї роботи є дослідження методів мінімізації кіберризиків при розгортанні повноцінної мережі е-гривні та надання пропозиції щодо архітектури системи мережевого моніторингу вузлів е-гривні.

Для досягнення цієї мети ставиться завдання проаналізувати вразливості інфраструктури CBDC та обґрунтувати доцільність застосування передових інженерних практик центрів управління мережею (NOC) для захисту державних реєстрів.

II. ДАНІ ТА МЕТОДИ

Для оцінки загального рівня загрози інфраструктурі е-гривні застосовується комплексна метрика ризику, яка враховує ймовірність експлуатації вразливості, рівень загрози та потенційний фінансовий вплив. На основі формули 1 може бути розрахований сумарний ризик R_{sys} :

$$R_{sys} = \sum_{i=1}^{n} (v_i \times T_i \times I_i), \quad (1)$$

де v_i — рівень вразливості конкретного мережевого компонента (наприклад, API-шлюзу НБУ), T_i — ймовірність реалізації атаки,I_i — критичність наслідків зупинки транзакцій.

Дослідження базується на:

- аналізі відкритих звітів НБУ щодо пілотних тестувань е-гривні;
- моделюванні мережевого навантаження на контрольовані державою вузли;
- методах проактивного моніторингу мережевої інфраструктури (NOC-практики).

Для практичної реалізації запропонованої метрики ризику передбачається використання сучасного стеку технологій моніторингу. Збір телеметрії з вузлів мережі е-гривні доцільно здійснювати за допомогою систем класу Prometheus, що дозволяє агрегувати метрики продуктивності серверів у режимі реального часу. Для візуалізації стану мережі та налаштування системи сповіщень (Alerting) пропонується інтеграція інструментів рівня

Grafana. Такий підхід забезпечить фахівцям центру управління мережею (NOC) комплексну видимість (Observability) інфраструктури та дозволить оперативно реагувати на відхилення від базового рівня нормальної активності (Baseline).

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У процесі дослідження було визначено, що ефективна робота системи е-гривні вимагає створення відмовостійкої мережі, яка здатна витримувати пікові навантаження та ізолювати скомпрометовані вузли без зупинки всього реєстру. Для вирішення цього завдання авторами розроблено та запропоновано архітектуру системи мережевого моніторингу вузлів е-гривні (Рисунок 1).

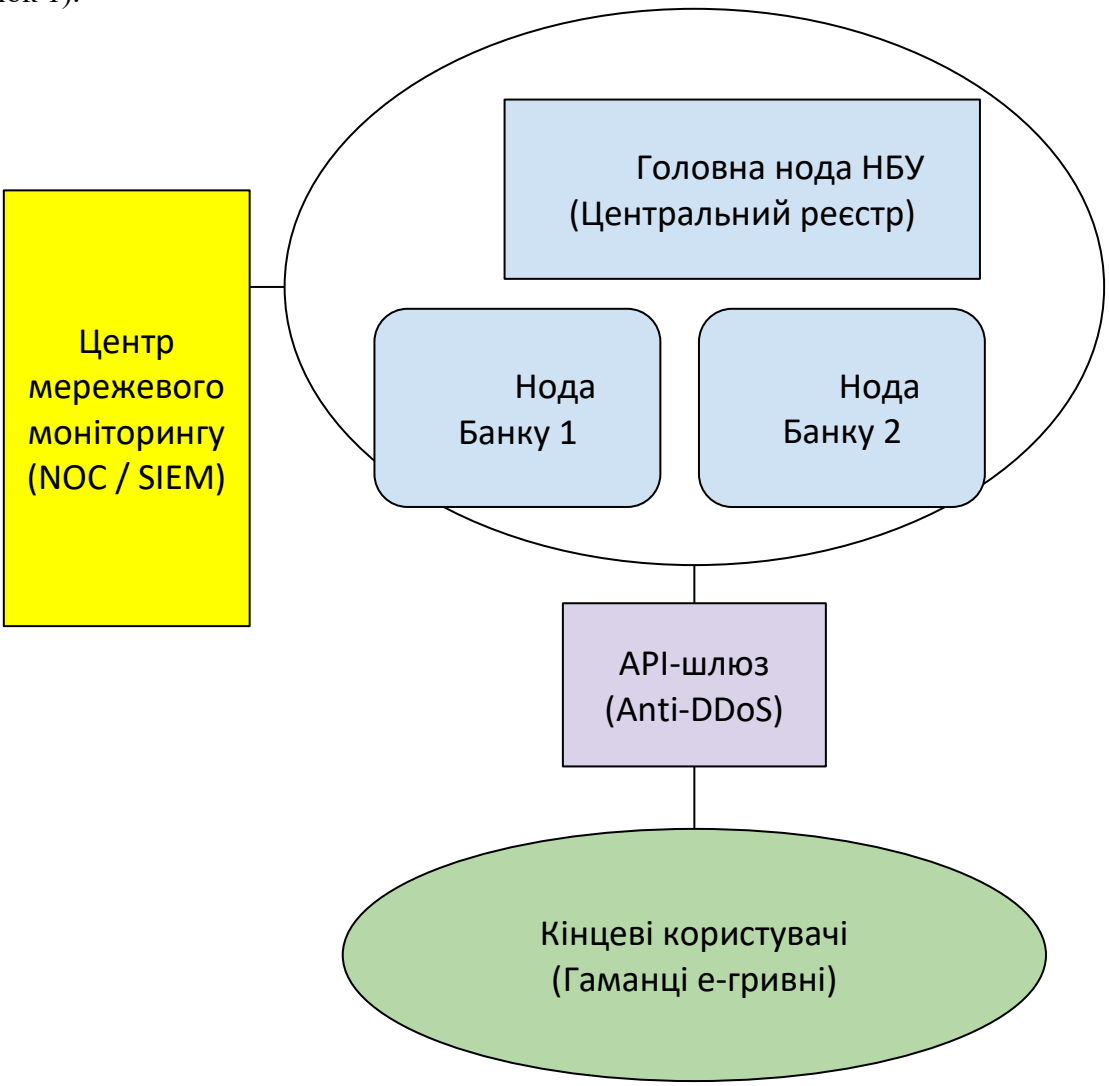


Рисунок 1. *Архітектура системи мережевого моніторингу вузлів е-гривні (розроблено авторами)*

Основна загроза для CBDC полягає не стільки у підробці активів (що криптографічно складно), скільки у порушенні доступності сервісу. На основі аналізу мережевих аномалій, авторами сформовано порівняльну матрицю специфічних загроз для е-гривні та технічних методів їх нейтралізації (Таблиця 1).

Таблиця 1. *Типи кібератак на інфраструктуру CBDC та методи їх нейтралізації. Джерело: складено авторами*

№	Тип атаки	Вектор впливу	Метод нейтралізації
1	DDoS на API-шлюзи	Недоступність гаманців е-гривні для громадян, затримка платежів	Багаторівнева фільтрація трафіку, Anycast-маршрутизація
2	Компрометація ноди банку-партнера	Спроба ін'єкції невалідних транзакцій у загальний реєстр	Строга сегментація мережі, ізоляція вузла при аномальному трафіку
3	Атака на канали зв'язку	Перехоплення або підміна службових даних між серверами НБУ	Використання шифрування на рівні каналу (IPsec, TLS 1.3)
4	Підміна мережевої маршрутизації (BGP Hijacking / DNS Spoofing)	Перенаправлення трафіку банків та користувачів на шахрайські вузли, перехоплення сесій	Впровадження RPKI для BGP, DNSSEC, моніторинг глобальних таблиць маршрутизації
5	Експлуатація вразливостей програмованої логіки (смарт-контрактів)	Несанкціоноване блокування активів, збій логіки транзакцій у системі е-гривні	Формальна верифікація коду, інтеграція систем автоматизованого аудиту (DevSecOps)

Як показано в Таблиці 1, більшість критичних ризиків для цифрової валюти лежить у площині класичної мережевої безпеки, що робить роль центрів управління мережею ключовою в підтримці працездатності системи.

Окрім захисту від зовнішніх атак, критично важливим аспектом відмовостійкості є забезпечення катастрофостійкості (Disaster Recovery) державної мережі. У разі успішної компрометації або апаратного збою на одній із нод комерційного банку-партнера, архітектура системи повинна передбачати механізми автоматичного перемикання трафіку (Failover) на резервні вузли. Це вимагає розробки суворих регламентів щодо цільового часу відновлення (RTO) та цільової точки відновлення (RPO) для транзакційних баз даних е-гривні, щоб унеможливити втрату фінансових даних клієнтів навіть за умови повної фізичної недоступності окремого дата-центру.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Впровадження е-гривні є стратегічним кроком для фінансового сектору України, однак воно вимагає жорстких стандартів кібербезпеки на рівні архітектури вузлів.

Запропонована у роботі концепція доводить, що ризики використання державних цифрових активів піддаються ефективному контролю за умови створення безперервного

циклу мережевого моніторингу. Забезпечення видимості всього трафіку між вузлами реєстру та подальше розгортання автоматизованих систем реагування (SOAR) дозволить гарантувати безперебійну роботу е-гривні навіть в умовах активних кібератак.

Подальші дослідження доцільно спрямувати на розробку спеціалізованих сценаріїв реагування на інциденти (playbooks) для інтеграції у державні центри моніторингу безпеки. Застосування алгоритмів предиктивної аналітики для аналізу on-chain метрик та мережевих логів дозволить створити проактивну систему захисту, здатну адаптуватися до нових векторів кіберзагроз.

Важливо підкреслити, що розгортання технічних засобів моніторингу є лише частиною комплексного рішення. Для ефективної протидії сучасним кіберзагрозам необхідна розробка спеціалізованих регламентів реагування на інциденти (Incident Response Playbooks), адаптованих специфічно під архітектуру CBDC. Ці регламенти мають чітко визначати ролі та зону відповідальності фахівців Національного банку та комерційних банків при виявленні мережевих аномалій, що дозволить мінімізувати час від виявлення загрози до її повної нейтралізації.

ДЖЕРЕЛА

1. Національний банк України (2022). Проєкт е-гривня. Офіційне інтернет-представництво НБУ. https://bank.gov.ua/admin_uploads/article/Analitichna_zapiska_E-grivnya.pdf
2. Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. BIS Quarterly Review, March.
3. Bharath, A., Paduraru, A. and Gaidosch, T. (2024) Cyber Resilience of the Central Bank Digital Currency Ecosystem. IMF Fintech Note 2024/003. Washington, DC: International Monetary Fund.



ІГОР ШИЛЕНКО
аспірант 1 курсу факультету інформаційних техонологій у Київському національному університеті імені Тараса Шевченка.
E-mail: shylenkoihor@gmail.com
Науковий інтерес полягає в області забезпечення кіберстійкості державного фінансового сектору. Серед наукових інтересів — мережевий моніторинг блокчейн-інфраструктури, безпека смарт-контрактів та захист систем е-гривні (CBDC).



ВОЛОДИМИР НАКОНЕЧНИЙ
Доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації у Київському національному університеті імені Тараса Шевченка.
ORCID: 0000-0002-0247-5400
E-mail: volodym.nakonechnyi@knu.ua
З 2011 року обіймав керівні посади, зокрема директора Навчально-наукового інституту захисту інформації в ДУТ, а з 2017 року працює в Київському національному університеті імені Тараса Шевченка. Автор понад 170 наукових праць, монографій та публікацій, у тому числі у міжнародних наукометричних базах Scopus та Web of Science.
Коло наукових інтересів: комплексні системи захисту інформації, кібербезпека, автоматизовані системи управління та радіотехнічні пристрої.

КОМПЛЕКСНА КРИПТОГРАФІЧНА АРХІТЕКТУРА ПІДВИЩЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ

Людмила Шпорт, Юлія Сотніченко

Анотація. *У роботі досліджено актуальні проблеми захисту електронних міжбанківських платежів в умовах ескалації кіберзагроз і цифровізації фінансових сервісів. Проаналізовано підходи до забезпечення безпеки у міжнародних платіжних інфраструктурах, зокрема SWIFT та SEPA. Визначено основні обмеження чинних архітектур захисту: складність управління криптографічними ключами, недостатню масштабованість, залежність від людського фактора та ризики централізованих компонентів. Запропоновано комплексну модульну криптографічну архітектуру, що інтегрує шифрування, багаторівневу автентифікацію, системи виявлення вторгнень, аудит подій безпеки та сучасні криптографічні механізми, включно з гомоморфним шифруванням і технологіями розподіленого реєстру. Обґрунтовано доцільність її впровадження для підвищення стійкості фінансової інфраструктури до сучасних атак.*

Ключові слова: міжбанківські платежі; криптографічний захист; кібербезпека; HSM; IDS/IPS; гомоморфне шифрування; блокчейн.

I. ВСТУП

Електронні міжбанківські розрахунки є фундаментом функціонування глобальної фінансової системи. Через міжнародні платіжні мережі щоденно проходять мільйони транзакцій, що забезпечують роботу банків, бірж, корпоративного сектору та державних фінансових установ. Зростання цифровізації супроводжується суттєвим збільшенням кількості кібератак, спрямованих на фінансові установи. Особливо небезпечними є атаки на інфраструктуру міжбанківських розрахунків, оскільки їх наслідки можуть мати системний характер. Міжнародні системи, такі як SWIFT та SEPA, реалізують багаторівневий підхід до безпеки, що включає криптографічний захист, сегментацію мереж, апаратні модулі безпеки та політики контролю доступу. Проте розвиток технологій атак, зокрема цільових APT-кампаній, DDoS-атак та атак на ланцюги постачання програмного забезпечення, вимагає переосмислення архітектурних підходів до побудови систем захисту. Метою дослідження є формування комплексної криптографічної архітектури, здатної забезпечити високий рівень конфіденційності, цілісності та доступності міжбанківських транзакцій за умов зростаючих кіберзагроз.

II. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Методологічною основою роботи є системний та комплексний підхід до аналізу інформаційної безпеки фінансових систем.

У процесі дослідження застосовано:

- аналіз міжнародних стандартів і практик захисту платіжних систем;
- порівняльний аналіз криптографічних алгоритмів (AES, RSA, ECC);
- концептуальне моделювання багаторівневої архітектури безпеки;
- імітаційне моделювання сценаріїв кібератак;
- оцінювання показників пропускної здатності та затримки транзакцій.

Дослідження враховує вимоги масштабованості, сумісності з чинними фінансовими стандартами та мінімізації затримок обробки платежів у реальному часі.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Аналіз показав, що основними ризиками є:

- компрометація облікових даних та криптографічних ключів;
- атаки на централізовані компоненти інфраструктури;
- недостатня сегментація мереж;
- використання застарілих криптографічних протоколів;
- людський фактор (помилки конфігурації, соціальна інженерія).

Додаткову загрозу становить перспектива квантових обчислень, що потенційно можуть знизити стійкість традиційних алгоритмів асиметричного шифрування.

Запропонована криптографічна архітектура - архітектура побудована за модульним принципом і включає такі компоненти:

- Модуль шифрування даних - використовує AES-256 для симетричного шифрування та ECC для обміну ключами. Управління ключами реалізується через HSM із підтримкою генерації, ротації та резервування ключів.
- Модуль автентифікації та авторизації - забезпечує багатофакторну перевірку особи користувача (пароль, апаратний токен, біометрія) та реалізацію принципу мінімальних привілеїв.
- Модуль IDS/IPS - здійснює моніторинг мережевого трафіку в режимі реального часу, виявляє аномалії та автоматично блокує підозрілу активність.
- Модуль аудиту та моніторингу - забезпечує централізоване журналювання подій, аналітику безпеки та контроль внутрішніх загроз.
- Додаткові технології:
    - гомоморфне шифрування для обробки зашифрованих даних без розкриття їх змісту;
    - технології розподіленого реєстру для забезпечення незмінності транзакційних записів;
    - підготовка до переходу на постквантові криптографічні алгоритми.

Моделювання показало, що система зберігає високу пропускну здатність навіть за пікових навантажень. Відсоток успішного відбиття атак типу DDoS перевищує 95%, а атаки на криптографічні ключі були нейтралізовані завдяки використанню HSM та механізмів ізоляції. Збільшення затримки транзакцій при використанні гомоморфного шифрування є помірним і знаходиться в межах прийнятних значень для фінансових операцій.

IV. ПОСТКВАНТОВА КРИПТОГРАФІЯ ТА МОДЕЛЬ ЗАГРОЗ STRIDE

Сучасні міжбанківські платіжні системи використовують асиметричні алгоритми RSA та ECC для обміну ключами та цифрового підпису. Їхня стійкість базується на складності задач факторизації та дискретного логарифмування [5]. Однак із розвитком квантових обчислень алгоритм Шора потенційно дозволяє розв’язувати ці задачі за поліноміальний час, що створює ризик компрометації криптографічної інфраструктури в перспективі 10–15 років [3].

Відповідно до рекомендацій міжнародної криптографічної спільноти та досліджень з прикладної криптографії [6], доцільним є поступовий перехід до постквантових алгоритмів, зокрема:

- CRYSTALS-Kyber — алгоритм обміну ключами на основі решіток;
- CRYSTALS-Dilithium — постквантовий алгоритм цифрового підпису;
- NTRU — криптосистема, що базується на проблемі найближчого вектора в решітці.

Постквантові алгоритми демонструють високу стійкість до атак із використанням квантових комп'ютерів, проте потребують оптимізації через збільшений розмір ключів і підписів [6].

У запропонованій архітектурі реалізується гібридна модель, у якій класичні алгоритми (ECC) використовуються паралельно з постквантовими (Kyber), що дозволяє забезпечити криптостійкість як до сучасних, так і до перспективних загроз.

Для систематизації ризиків застосовано модель STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), яка широко використовується при проєктуванні безпечних інформаційних систем [4].

- S – Spoofing (підміна особи) - використання викрадених облікових даних або компрометація сертифікатів. Механізмом протидії є багатофакторна автентифікація, апаратні токени, цифрові підписи [1].
- T – Tampering (модифікація даних) - зміна транзакцій у процесі передачі. Механізмом протидії є TLS 1.3, HMAC, цифрові підписи, використання HSM [4].
- R – Repudiation (відмова від авторства) - заперечення факту проведення транзакції. Механізмом протидії є незаперечність через криптографічний підпис та журналювання подій [6].
- I – Information Disclosure (витік інформації) - перехоплення платіжних даних. Механізмом протидії є AES-256, сегментація мереж, гомоморфне шифрування для обробки чутливої інформації [4].
- D – Denial of Service (відмова в обслуговуванні) - DDoS-атаки на платіжну інфраструктуру. Механізмом протидії є IDS/IPS, балансування навантаження, сегментація трафіку [2].
- E – Elevation of Privilege (підвищення привілеїв) - отримання несанкціонованого адміністративного доступу.

Механізмом протидії є принцип мінімальних привілеїв, контроль доступу на основі ролей (RBAC) [1]. Застосування STRIDE дозволяє формалізувати модель загроз та інтегрувати механізми протидії на етапі архітектурного проєктування.

Для мінімізації ризиків міграція до постквантових алгоритмів здійснюється поетапно:

1. Впровадження гібридного обміну ключами (ECC + Kyber).
2. Пілотне використання Dilithium для підпису транзакцій.
3. Аудит криптографічної інфраструктури відповідно до ISO/IEC 27001 [1].
4. Підготовка до повного переходу на PQC після затвердження міжнародних стандартів.

Такий підхід дозволяє зберегти сумісність із чинними фінансовими системами та мінімізувати ризики деградації продуктивності.

V. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати дослідження підтверджують, що забезпечення безпеки міжбанківських платежів потребує інтеграції криптографічних, мережевих та організаційних механізмів у єдину архітектурну модель.

Запропонована комплексна криптографічна архітектура:

- підвищує стійкість до зовнішніх і внутрішніх загроз;
- забезпечує баланс між продуктивністю та рівнем захисту;
- підтримує масштабованість та сумісність із міжнародними стандартами;
- створює основу для подальшої адаптації до постквантових викликів.

Практична цінність роботи полягає у можливості застосування запропонованої моделі для модернізації національних та міжнародних платіжних інфраструктур в умовах зростаючих кіберризиків.

ДЖЕРЕЛА

1. Журавльов О.В., Хорошко В.О. Криптографічний захист інформації в банківських системах. – Київ: НАУ, 2020.
2. SWIFT Customer Security Controls Framework. – 2023. URL: https://www.swift.com
3. ENISA. Threat Landscape for Financial Sector. – 2023. URL: https://www.enisa.europa.eu
4. European Central Bank. Cyber resilience oversight expectations. – 2022. URL: https://www.ecb.europa.eu
5. Конахович Г.Ф., Пузиренко О.В. Інформаційна безпека банківських систем. – Київ: КПІ, 2019.
6. Stallings W. Network Security Essentials. – Pearson, 2022.



ЛЮДМИЛА ШПОРТ
викладачка першої категорії циклової комісії кібербезпеки, електронних комунікацій та економіко-управлінської підготовки, Київський фаховий коледж зв'язку, м.Київ, Україна
ORCID:0009-0006-3114-4965
email: luda.kaziuchits@gmail.com

З 2009 року почала свою викладацьку кар'єру на посаді викладача Київського фахового коледжу зв'язку. Маю тривалий досвід викладання навчальних дисциплін у галузі кібербезпеки та інформаційних технологій, здійснюю професійну підготовку здобувачів освіти за напрямом G5. Наукова діяльність зосереджена на питаннях цифрової трансформації освіти, розвитку ключових професійних і соціальних компетентностей, інтеграції сучасних освітніх технологій та забезпеченні принципів академічної доброчесності. Є авторкою публікацій у фахових виданнях України, учасницею національних науково-практичних заходів. Беру участь у проєктуванні та оновленні освітніх програм і методичного забезпечення підготовки фахівців у сфері електроніки, електронних комунікацій, приладобудування та радіотехніки (галузь G5).



ЮЛІЯ СОТНІЧЕНКО
Викладач-методист, спеціаліст вищої категорії, завідувач відділення кібербезпеки та інформаційно-комунікаційних технологій, фахівець у сфері кібербезпеки, інформаційних технологій та інфокомунікацій.
ORCID 0000-0002-1281-9238
email: iktkkz@ukr.net

Має багаторічний досвід педагогічної діяльності, забезпечує викладання фахових дисциплін з кібербезпеки та інфокомунікаційних систем, здійснює професійну підготовку здобувачів освіти галузі знань G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка».

Професійні інтереси охоплюють проблематику розвитку сучасної педагогіки у сфері інфокомунікацій, модернізацію освітнього середовища, впровадження цифрових рішень у навчальний процес, формування фахових і надпрофесійних компетентностей майбутніх спеціалістів.

Є авторкою наукових і методичних праць, бере активну участь у фахових конференціях та семінарах. Долучається до вдосконалення освітніх програм і створення навчально-методичних матеріалів для підготовки фахівців у сфері електронних комунікацій та телекомунікаційних технологій.

ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ СИСТЕМ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ ТРИФАКТОРНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Діана Язвінська, Анатолій Ніколенко

Анотація. *У представленому дослідженні розглянуто важливість та актуальність розробки методики багатофакторної біометричної автентифікації для систем контролю доступу в освітніх установах. Робота аналізує проблематику вразливості традиційних методів ідентифікації та демонструє, як інтеграція RFID-технологій із розпізнаванням обличчя та відбитків пальців може забезпечити надійний моніторинг та безпеку освітнього середовища. Завдяки використанню трирівневої верифікації система сприяє точному обліку робочого часу персоналу та запобіганню несанкціонованому доступу сторонніх осіб, мінімізуючи вплив людського фактору в умовах надзвичайних ситуацій.*

Ключові слова: IoT; багатофакторна автентифікація; біометрія; система контролю доступу; освітні установи; безпечне середовище.

I. ВСТУП

Сучасний етап цифровізації освітнього простору потребує впровадження надійних систем ідентифікації, оскільки традиційні методи на основі лише RFID-карток або паролів не здатні запобігти ризикам відчуження ідентифікатора від власника. Основним інструментом вирішення цієї проблеми є розробка та впровадження методики багатофакторної біометричної автентифікації, яка забезпечує нерозривний зв’язок між фізичною особою та її цифровим профілем у системі доступу [1].

Метою роботи є дослідження та розробка методики трифакторної автентифікації, що базується на інтеграції фізичного ідентифікатора з двома незалежними біометричними модальностями: геометрією обличчя та відбитком пальця. Такий підхід дозволяє перенести фокус із загальних засобів безпеки на створення математично обґрунтованого алгоритму багаторівневої верифікації користувачів у режимі реального часу.

Застосування даної методики спрямоване на оптимізацію процесів розпізнавання шляхом мінімізації ймовірностей помилок першого та другого роду (FAR та FRR). Використання комбінованого аналізу біометричних ознак дозволяє досягти високої точності ідентифікації, що є критично важливим для об’єктів інфраструктури закладів освіти та забезпечення академічної доброчесності [2].

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз стану систем безпеки в закладах вищої та фахової передвищої освіти Вінницької області виявив критичний розрив між сучасними вимогами до безпечного освітнього середовища та наявною інфраструктурою. Дослідження засвідчило, що у переважній більшості закладів фахової передвищої освіти автоматизовані системи ідентифікації повністю відсутні, а контроль доступу обмежується фізичною присутністю чергового персоналу. Такий підхід базується на суб'єктивному людському факторі, де фіксація часу прибуття чи залишення робочого місця викладачами та іншим персоналом здійснюється вручну в паперових журналах, а також зафіксовано випадки повної відсутності моніторингу трафіку персоналу, що дестабілізує систему безпеки закладу. Це створює значні ризики, пов'язані з несанкціонованим доступом сторонніх осіб, неможливістю оперативного реагування у разі надзвичайних ситуацій та низькою достовірністю даних щодо перебування учасників освітнього процесу в будівлі, тому в умовах виникнення надзвичайних ситуацій

техногенного або воєнного характеру (зокрема, під час сигналів повітряної тривоги) критично важливим стає наявність верифікованих даних про кількість осіб у приміщенні.

Навіть у тих нечисленних університетах регіону, де впроваджено карткові системи (RFID), рівень безпеки залишається недостатнім через специфічні вразливості однофакторної автентифікації. Основним ризиком використання лише пластикової картки є її відчужуваність від власника: можливість передачі колегам для фіктивного "логіну" або копіювання ідентифікатора зловмисниками. У контексті створення безпечного освітнього середовища, над яким наразі ведеться робота в одному з коледжів області, було визначено, що встановлення камер відеонагляду було лише первинним етапом моніторингу. Запропоноване рішення інтегрується з існуючою мережею відеоспостереження, що дозволяє використовувати наявну апаратну базу для потреб біометричної верифікації. Наступним стратегічним кроком є впровадження запропонованого проєкту триетапної перевірки, де програмний модуль об'єднує зчитування картки з обов'язковим розпізнаванням обличчя та верифікацією відбитка пальця. Таке рішення нівелює недоліки ручного обліку та слабкі місця звичайних СКУД, перетворюючи систему з простого інструменту реєстрації на надійний механізм захисту життя та здоров'я кожного учасника освітнього процесу.

Запропонована методика багатофакторної біометричної автентифікації реалізується через послідовний алгоритм процедурних кроків: етап 1 передбачає первинну апаратну ідентифікацію шляхом зчитування персонального фізичного ідентифікатора (RFID-картки) для ініціалізації запиту та пошуку відповідного профілю користувача у базі даних; на етапі 2 здійснюється біометрична детекція та розпізнавання обличчя із застосуванням алгоритмів комп’ютерного зору для виділення унікальних дескрипторів та їх порівняння з еталонним шаблоном у режимі реального часу; етап 3 полягає у фінальній верифікації за відбитком пальця, що забезпечує найвищий рівень достовірності підтвердження особи та нівелює ризики, пов’язані з відчуженням фізичного носія; завершальний етап 4 охоплює автоматичне прийняття рішення щодо надання або відмови у доступі з обов’язковим логуванням події та фіксацією точного часу перебування персоналу в інформаційній системі.

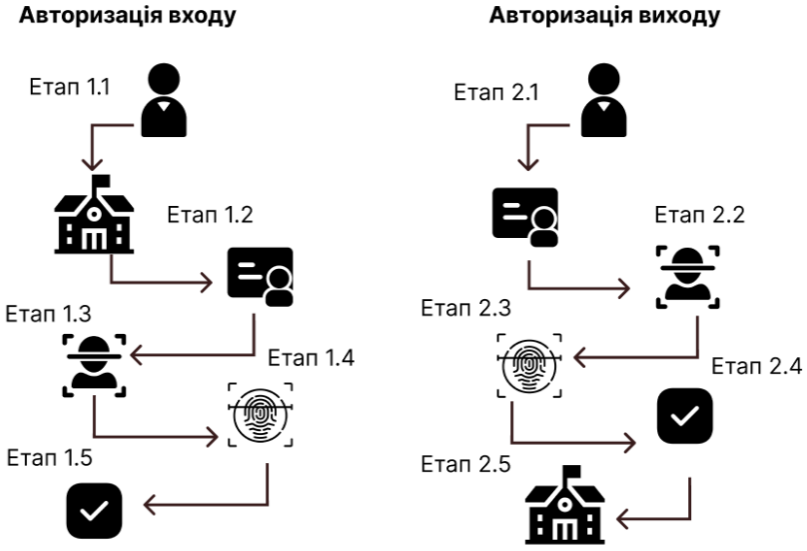


Рисунок 1. *Схема багаторівневої автентифікації користувачів у системі контролю доступу*

На Рисунку 1 представлена розроблена схема етапів методики бакатофакторної біометричної автентифікації для систем контролю доступу в освітній установі. Згідно з наведеною схемою, процедура авторизації входу (ліва частина рисунка) розпочинається з етапу 1.1 — прибуття користувача до контрольно-пропускного пункту навчального закладу. На етапі 1.2 відбувається первинна ідентифікація за допомогою зчитування персональної RFID-картки, що дозволяє системі ініціалізувати запит у базі даних. Після успішного

зчитування карти реалізується етап 1.3 — детекція та розпізнавання обличчя за допомогою методів комп'ютерного зору. На етапі 1.4 виконується фінальна біометрична верифікація через сканування відбитка пальця, що забезпечує найвищий рівень достовірності підтвердження особи. Завершальним етапом (1.5) є автоматичне розблокування механізму доступу та логування події прибуття в інформаційній системі.

Процедура авторизації виходу (права частина рисунка 1) реалізується за дзеркальним алгоритмом, де етапи 2.1–2.3 забезпечують повторну ідентифікацію через RFID-носій та біометричну верифікацію особи. Такий підхід гарантує неможливість вибуття сторонніх осіб за чужими ідентифікаторами. Після фінального підтвердження (етап 2.4) система реєструє факт завершення робочого часу (етап 2.5), що забезпечує автоматизацію обліку та наявність актуальної статистики перебування персоналу на об'єкті в режимі реального часу.

Для технічного втілення запропонованої методики передбачається використання кросплатформеного середовища розробки, що підтримує роботу з високорівневими бібліотеками комп’ютерного зору та алгоритмами машинного навчання. Програмний комплекс базуватиметься на модульній архітектурі, яка дозволяє незалежно налаштовувати та масштабувати окремі компоненти системи.

Ключовим елементом програмного забезпечення виступає модуль відеоаналітики, призначений для детекції обличчя в потоковому відео та автоматичного порівняння отриманих дескрипторів із еталонними зразками, що зберігаються в системі. Надійний зв’язок із зовнішніми сканерами RFID-карт та біометричними сенсорами відбитків пальців забезпечується спеціалізованим інтерфейсом взаємодії з периферійними пристроями через стандартні протоколи передачі даних.

Захищене зберігання персональної інформації співробітників та ведення журналів подій у реальному часі покладається на систему управління базою даних. Управління правами доступу, моніторинг поточної ситуації та формування аналітичної звітності про присутність персоналу здійснюється через графічний інтерфейс адміністративної панелі. Остаточний вибір конкретного стеку технологій, включаючи мову програмування та тип СКБД, буде здійснено на етапі детального проєктування, виходячи з критеріїв швидкодії на цільовому апаратному забезпеченні та можливості інтеграції з розгорнутою інфраструктурою відеоспостереження закладу.

Сучасний ринок систем контролю доступу пропонує широкий спектр рішень для комерційного сектору, зокрема для фітнес-центрів та бізнес-центрів, де пріоритетом є автоматизація ідентифікації співробітників за допомогою RFID-носіїв або біометрії обличчя. У професійному сегменті розробка таких систем зазвичай базується на мовах програмування високого рівня, як-от C++ або C#, що дозволяє забезпечити максимальну швидкість взаємодії з апаратним забезпеченням та створення стабільних інтерфейсів керування. Проте більшість комерційних продуктів є закритими екосистемами, що ускладнює їх адаптацію під специфічні потреби бюджетних освітніх закладів.

Запропонований проєкт базується на використанні кросплатформених середовищ та бібліотек з відкритим вихідним кодом, що дозволяє реалізувати гнучку трифакторну модель автентифікації без значних фінансових витрат на ліцензування. Такий підхід забезпечує високу продуктивність модулів відеоаналітики та надійну інтеграцію з різнорідними периферійними пристроями, створюючи ефективне рішення для моніторингу присутності персоналу, яке враховує регіональні особливості інфраструктури закладів фахової передвищої освіти.

У таблиці 1 наведено порівняльний аналіз ключових інструментальних засобів, що можуть бути використані для програмної реалізації запропонованої методики автентифікації. Проведений розгляд дозволяє оцінити ефективність мов програмування Python, C# та C++ за критеріями швидкодії та складності розробки. На основі цих даних обґрунтовано доцільність обрання високорівневих середовищ, які забезпечують оптимальний баланс між точністю розпізнавання даних та термінами впровадження системи в освітній простір.

Таблиця 1. *Порівняння основних програмних засобів*

Критерій порівняння	**Python (OpenCV + TensorFlow)**	**C# / .NET (Emgu CV / ML.NET)**	**C++ (OpenCV + Qt)**
Швидкість розробки	Найвища: велика кількість готових бібліотек для біометрії	Середня: зручний інструмент для створення Windows-інтерфейсів	Доволі низька: потребує багато часу на написання та налагодження коду
Продуктивність (швидкість обробки)	Середня (достатньо для коледжу)	Висока	Максимальна: найкращий вибір для систем реального часу
Робота з базами даних	Легка (інтеграція з SQLite/PostgreSQL за кілька рядків)	Рідна підтримка Entity Framework та MS SQL	Потребує підключення зовнішніх важких бібліотек

III. ВИСНОВКИ

У ході дослідження було обґрунтовано необхідність переходу від застарілих методів контролю доступу до сучасних інтелектуальних систем багаторівневої автентифікації. Аналіз стану безпеки в закладах фахової передвищої освіти Вінницької області підтвердив, що відсутність автоматизованих засобів ідентифікації створює критичні ризики для освітнього процесу. Розроблена методика трифакторної перевірки, яка послідовно поєднує використання фізичного ідентифікатора, розпізнавання обличчя та верифікацію відбитка пальця, дозволяє нівелювати вплив людського фактору та забезпечити високу достовірність обліку робочого часу. Впровадження системи, що реалізує запропоновану методику багатофакторної біометричної автентифікації як логічного продовження модернізації безпекової інфраструктури коледжу стане важливим кроком у створенні захищеного цифрового середовища для всіх учасників освітнього процесу. Перспективи подальшого дослідження полягають у практичній програмній реалізації модулів системи та оцінці їхньої ефективності при піковому навантаженні на контрольно-пропускних пунктах закладу.

ДЖЕРЕЛА

1. Ідентифікація і класифікація ризиків URL: https://qualityexpert.com.ua/articles/657215-identyfikatsiya-i-klasyfikatsiya-ryzykiv
2. Що таке багатофакторна автентифікація (MFA)? URL: https://www.protectimus.com/uk/what-is-multi-factor-authentication-mfa/



ДІАНА ЯЗВІНСЬКА
студентка 1 курсу магістратури спеціальності Комп'ютерні науки Національного університету «Одеська політехніка»
E-mail: yazvinskadiana@gmail.com
Науковий інтерес полягає в області розробки та застосування мультимодальних систем біометричної ідентифікації. Серед наукових інтересів — інтелектуальні системи контролю та управління доступом (СКУД).



АНАТОЛІЙ НІКОЛЕНКО
к.т.н., доцент кафедри інформаційних систем Національного університету «Одеська політехніка»
ORCID: 0000-0002-9849-1797
E-mail: nikolenko@op.edu.ua
Професійні (наукові) інтереси: Методологія інформаційних технологій, Цифрова обробка сигналів та зображень.

Section

Systems and technologies of artificial intelligence

Секція

Системи та технології штучного інтелекту

MODIFIED RADON PROJECTIONS FOR OVERLAP DETECION IN AGRICULTURAL LAND MAPPING

Stepan Bilan, Dmytro Berezhnyi

Abstract. *Accurate overlap detection is vital for stitching agricultural UAV imagery used in crop monitoring and precision farming. This study evaluates a modified Radon-based overlap matching pipeline on high-resolution farmland tiles, combining binarization, rejection of near-uniform windows, and mass-based candidate pruning. Results show fewer spurious correspondences than the standard setting and more reliable, interpretable overlap partner selection using compact 0°/90° projection verification.*

Keywords: UAV, overlap, Radon, binarization, matching.

I. INTRODUCTION

UAV-based imaging is widely used for rapid mapping, environmental monitoring, and post-disaster assessment, where large scenes are captured as many partially overlapping image tiles. Determining whether two tiles overlap, and roughly where the overlap lies, is an important step because it influences subsequent image registration and mosaicking. In practical UAV datasets, overlap estimation is complicated by illumination changes, motion blur, repetitive structures, and weak-texture areas (e.g., fields or water). At the same time, processing pipelines often need to handle large tile collections under limited compute budgets, which motivates methods that avoid heavy feature extraction or exhaustive pairwise comparisons.

Recent UAV mosaicking and stitching studies emphasize the importance of efficiently handling large image collections and accurately analyzing overlapping regions, since errors in overlap estimation propagate to alignment quality and can introduce visible artifacts in the overlap areas. [1]

In this study, a modification of a Radon-based matching approach was investigated for identifying overlap between UAV image tiles. The modification focuses on using a reduced set of Radon directions and simple intermediate criteria to support overlap reasoning in large tile collections, while keeping the method applicable under typical radiometric variability.

II. DATA AND METHODOLOGY

The proposed methodology identifies, for each UAV image tile A, the most likely overlapping tile B and highlights a small set of corresponding regions. First, each tile is converted into a binary image (0/1, with black = 1). This binarization reduces sensitivity to illumination and color differences and makes later computations simple integer operations. Each tile is then scanned with a sliding 64×64 window using a stride of 32 pixels, and for every window a scalar score S is computed as the number of ones (black pixels). To reduce false matches caused by uniform areas, windows that are nearly empty or nearly full are discarded, since such patches contain little structural information and can produce similar projection profiles across many unrelated regions, making them unreliable for subsequent Radon-based verification.

Next, candidate window correspondences between tiles A and B are generated using a coarse filter based on the window mass S (the number of ones in the binarized window). Based on Formula 1, we compute the absolute difference between the masses of a window pair (wa,wb) and retain only those pairs whose difference does not exceed a predefined tolerance ΔS. This step prunes the majority of unlikely correspondences before the Radon-based verification stage.

$$|S_a(w_a) - S_b(w_b)| \leq \Delta S \quad (1)$$

The core verification stage is based on a modification of the Radon approach. Instead of computing a full Radon transform over many angles (a complete sinogram), the method computes only two discrete projection profiles per window, denoted R^0 and R^{90}, corresponding to 0° and 90° . In practice, these are simply column sums and row sums. This is the central modification: Radon projections are used as a compact, local descriptor for checking window consistency rather than for multi-angle analysis or reconstruction. Using Radon-domain descriptors for matching and localization has also been explored in recent applied settings, e.g., for roto-translation-invariant representations and for Radon-based detection/localization in UAV imagery.

For a candidate window pair (w_a,w_b), the projection differences are computed as in **Formulas 2-3:**

$$d^0 = \mathrm{R}_\mathrm{a}^0 - \mathrm{R}_\mathrm{b}^0 \quad (2)$$

$$d^{90} = \mathrm{R}_\mathrm{a}^{90} - \mathrm{R}_\mathrm{b}^{90} \quad (3)$$

A pair is accepted if, in each direction, the fraction of projection indices k satisfying the tolerance condition *CI* is at least p (Formulas 4-5):

$$\frac{1}{L}\sum_{k=1}^{l} 1(|d^0[k]| \le CI) \ge p \quad (4)$$

$$\frac{1}{L}\sum_{k=1}^{l} 1(|d^{90}[k]| \le CI) \ge p \quad (5)$$

Finally, for each tile A, the tile B that produces the largest number of verified window-level matches is selected as the most likely overlap partner. For interpretability, the matches are ranked and the top 3 window pairs are visualized on the original tiles.

The dataset consists of aerial photographs of agricultural fields obtained from the EOS Crop Monitoring Platform (https://crop-monitoring.eos.com) and used as the input imagery in this study. The images cover farmland areas near the villages of Novoselivka and Cherniakiv and were selected under similar lighting conditions to reduce illumination-induced variability during matching experiments.

III. RESULTS AND ANALYSIS

As shown in Figure 1, the algorithm identifies Tile 1 and Tile 12 as the best-matching pair, reporting 21 verified matched windows ("total matched windows = 21" in the figure header). This number reflects how many window pairs passed the full verification procedure (coarse mass filtering followed by the 0°/90° projection agreement test), so it serves as an aggregate indicator of overlap consistency for the selected tile pair.

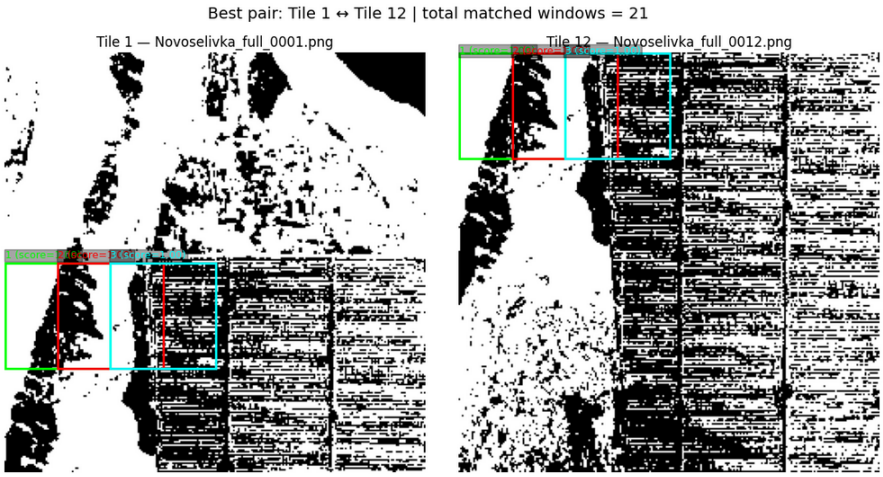


Figure 1. *Tile overlap result: Tile 1 ↔ Tile 12 (**21** matched windows).*

In Figure 1, the top-3 highest-scoring matched windows (colored rectangles) appear in corresponding locations in both tiles and are concentrated near the transition between a large low-texture region and a highly structured field pattern. The fact that these matches are spatially coherent, rather than scattered across unrelated areas, suggests that the method localizes the most informative part of the overlap and bases the pair selection on regions with stable structure. Overall, Figure 1 simultaneously demonstrates the pair selection outcome (Tile 1 ↔ Tile 12) and an interpretable overlap localization cue via the highlighted matched windows.

Figure 2 contrasts the baseline and the modified pipeline:

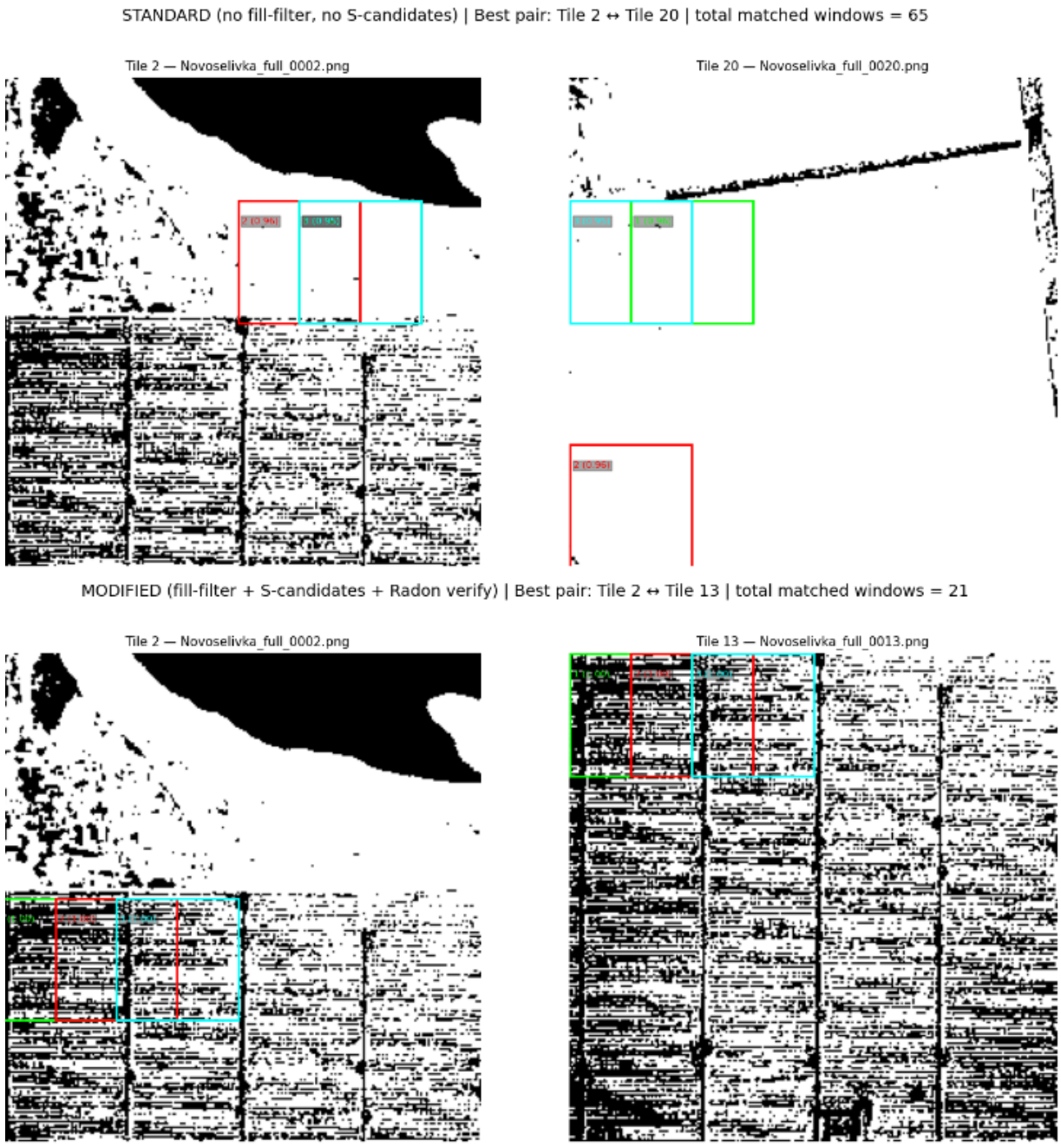


Figure 2. *Standard vs. modified overlap matching (Tile 2).*

In the standard setting, the method reports many matches (65) but they concentrate in near-uniform, low-information regions, which can inflate match counts and lead to an unreliable best-pair choice. With the modified pipeline (fill-filter + S-candidates + Radon verification), the selected

pair changes and yields fewer matches (21), yet the matches align with structured field patterns and are spatially consistent across tiles. Overall, the modification reduces spurious correspondences and improves the reliability of overlap partner selection.

IV. DISCUSSION AND CONCLUSION

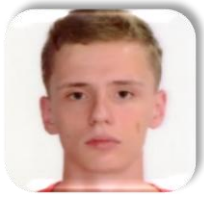
The study shows that combining near-uniform window rejection with S-based candidate pruning and reduced-angle (0°/90°) Radon projection verification improves the reliability of UAV tile overlap detection. Compared to the unmodified setting, the modified pipeline produces fewer spurious correspondences from low-information regions and yields more spatially coherent, interpretable matches on structured scene patterns. The comparison also indicates that a higher raw match count in the unmodified pipeline can be misleading, since many matches originate from homogeneous areas that are weakly discriminative. In contrast, the modified pipeline prioritizes fewer but more informative correspondences that better support overlap partner selection and overlap localization. Overall, the modified Radon-based verification scheme provides a practical way to select overlapping tile pairs using compact projection descriptors rather than full multi-angle Radon representations.

REFERENCES

1. Pham N. T., Park S., Park C. S. (2021) Fast and efficient method for large-scale aerial image stitching.
2. Lu S., Xu X., Tang L., Xiong R. (2023) DeepRING: Learning roto-translation invariant representation for LiDAR based place recognition.
3. Liu J., Dai W., Zhang Y., Xing L., Pan D. (2024) An adaptive radon-transform-based marker detection and localization method for displacement measurements using unmanned aerial vehicles.



STEPAN BILAN
Ph.D., associate professor, the department of intellectual technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: ORCID: 0000-0002-2978-5556
E-mail: stepan.bilan@knu.ua
Stepan Bilan completed his studies at Vinnytsia National Technical University, Vinnytsia, Ukraine. He is currently the associate professor at the department of intellectual technologies at Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. His research interests include artificial intelligence, image processing and recognition, computer graphics, information security, cellular automata, biometric identification, pseudo-random number generators, modeling of dynamic processes.



DMYTRO BEREZHNYI
Ph.D. student, the department of intellectual technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0009-0000-8217-6525
E-mail: berezhnyid@knu.ua
Dmytro Berezhnyi pursued the M.S. degree in Computer Science at Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. He is currently pursuing a PhD at the same university. His research interests include deep learning, machine learning, computer vision, data visualization.

INTELLIGENT MULTIMODAL DATA FUSION FOR ROBUST UAV DETECTION IN COMPLEX ENVIRONMENTS

Stanislav Golouh, Vladyslav Shulga, Ihor Pishta

Abstract. *The rapid growth of unmanned aerial vehicle (UAV) applications has created significant challenges for security, surveillance, and airspace monitoring systems. Conventional UAV detection approaches that rely on a single sensing modality are highly vulnerable to environmental disturbances, such as poor illumination, adverse weather conditions, and acoustic noise. This paper proposes an intelligent multimodal data fusion framework that integrates visual, thermal, and acoustic sensor data using deep learning techniques. The proposed system performs feature-level fusion of heterogeneous sensor representations to construct a unified and robust object representation. The approach aims to improve detection accuracy, reduce false positives, and ensure stable system performance under dynamic and uncertain operational conditions. The results demonstrate that multimodal fusion significantly enhances system reliability compared to single-sensor solutions, making the proposed framework suitable for real-world security and defense applications.*

Keywords: UAV detection, multimodal data fusion, deep learning, thermal imaging, acoustic sensing, sensor fusion, airspace security.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) are increasingly used in civilian, industrial, and military domains, including logistics, environmental monitoring, reconnaissance, and surveillance. At the same time, their accessibility and mobility introduce serious security risks, particularly in restricted or sensitive areas. Reliable UAV detection has therefore become a critical task for modern intelligent security systems.

Traditional UAV detection systems are typically based on a single type of sensor, such as optical cameras, radar, radio-frequency (RF) detectors, or acoustic sensors. Although such systems can be effective under controlled conditions, their performance degrades significantly in complex environments. Visual sensors are highly sensitive to illumination and weather conditions, thermal sensors suffer from background heat interference, and acoustic sensors are affected by environmental noise. These limitations reduce detection accuracy and increase the number of false alarms.

Multimodal data fusion provides a promising solution to these challenges by integrating complementary information from multiple sensing modalities. By combining heterogeneous data sources, the system can compensate for the weaknesses of individual sensors and form a more complete situational understanding of the observed environment. Advances in deep learning and neural network architectures have further enabled efficient representation learning and fusion of multimodal data streams, making intelligent multisensor systems feasible for real-time applications.

This paper presents an intelligent multimodal UAV detection framework based on deep neural networks and feature-level data fusion. The proposed system integrates visual, thermal, and acoustic information into a unified representation, enabling robust detection in complex and dynamically changing environments.

II. OBJECTIVE OF THE STUDY

The main objective of this research is to design and evaluate a multimodal UAV detection system that improves reliability, accuracy, and robustness under real-world conditions. The specific goals of the study are:

- To analyze the limitations of single-sensor UAV detection systems;

- To develop a multimodal architecture for heterogeneous sensor integration;
- To implement feature-level fusion using deep neural network representations;
- To evaluate the performance of the fused model in complex environmental scenarios;
- To demonstrate the advantages of multimodal fusion for security and surveillance applications.

SYSTEM ARCHITECTURE AND METHODS

The proposed system is based on a three-channel sensing architecture that includes visual, thermal, and acoustic data sources. Each modality is processed independently using specialized neural network models before integration.

VISUAL PROCESSING MODUL

Visual data are processed using a convolutional neural network (CNN) designed for object detection and feature extraction. The network learns spatial and structural patterns of UAVs from RGB images, producing high-level latent feature representations.

THERMAL PROCESSING MODULE

Thermal infrared data are processed using a modified CNN architecture optimized for heat signature recognition. This module enables detection in low-light and nighttime conditions, where conventional optical sensors are ineffective.

ACOUSTIC PROCESSING MODULE

Acoustic signals are analyzed using a one-dimensional convolutional neural network (1D-CNN) that extracts temporal and frequency-domain features from audio streams. This allows identification of UAV-specific sound patterns, even in visually occluded environments.

FEATURE-LEVEL FUSION

High-level feature vectors extracted from each modality are concatenated into a unified multimodal representation. This fused feature vector is processed by fully connected neural layers that perform final classification into UAV and non-UAV categories. Feature-level fusion enables the model to learn cross-modal correlations and complementary relationships between different data sources.

III. RESULTS AND DISCUSSION

The multimodal fusion model demonstrates significantly higher detection accuracy and stability compared to single-modality systems. Visual-only models perform well under ideal conditions but fail in poor lighting and adverse weather. Thermal-only models are effective at night but struggle in high-temperature environments. Acoustic-only models remain functional in low-visibility conditions but generate false positives in noisy settings.

By contrast, the fused multimodal model maintains high performance across diverse scenarios. The system dynamically compensates for weak or degraded sensor inputs by relying on complementary modalities. This redundancy and complementarity significantly improve robustness, reduce false alarm rates, and enhance overall reliability.

The results confirm that multimodal data fusion is a key enabler for intelligent UAV detection systems operating in real-world environments characterized by uncertainty, noise, and variability.

IV. CONCLUSIONS

This paper presents an intelligent multimodal data fusion framework for robust UAV detection in complex environments. By integrating visual, thermal, and acoustic data through deep learning–based feature-level fusion, the proposed system achieves significantly improved detection accuracy and operational stability.

The results demonstrate that multimodal fusion effectively overcomes the limitations of single-sensor approaches and provides a scalable foundation for next-generation security and surveillance systems. The proposed architecture is suitable for real-time deployment in defense, infrastructure protection, and automated monitoring applications.

Future research will focus on adaptive fusion strategies, real-time optimization, inclusion of additional sensing modalities such as radar and LiDAR, and deployment on embedded and edge computing platforms.

REFERENCES

1. Hall, D. L., McMullen, S. A. H. Handbook of Multisensor Data Fusion. CRC Press, 2001.
2. Liggins, M. E., Hall, D. L., Llinas, J. Handbook of Multisensor Data Fusion: Theory and Practice. CRC Press, 2017.
3. Mitchell, H. B. Multi-Sensor Data Fusion: An Introduction. Springer, 2012.
4. Waltz, E., Llinas, J. Multisensor Data Fusion. Artech House, 1990.
5. Svanström, F., Englund, C., Alonso-Fernandez, F. Real-Time Drone Detection and Tracking With Visible, Thermal and Acoustic Sensors. Semantic Scholar, 2020.
6. Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z., Chen, J. Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges. IEEE, 2019.
7. Frid, A., Ben-Shimol, Y., Manor, E., Greenberg, S. Drones Detection Using a Fusion of RF and Acoustic Features and Deep Neural Networks. MDPI, 2024.
8. Wei, C., Qin, Z., Zhang, Z., Wu, G., Barth, M. J. Integrating Multi-Modal Sensors: A Review of Fusion Techniques for Intelligent Vehicles. arXiv, 2025.



STANISLAV GOLOUH
4th year bachelor, student of the Faculty of Information Technologies, Software Systems and Technologies Department Taras Shevchenko National University of Kyiv.
E-mail: golouhstanislav@knu.ua



VLADYSLAV SHULGA
4th year bachelor, student of the Faculty of Information Technologies, Software Systems and Technologies Department Taras Shevchenko National University of Kyiv.
E-mail: shulgavlad@knu.ua



IHOR PISHTA
4th year bachelor, student of the Faculty of Information Technologies, Software Systems and Technologies Department Taras Shevchenko National University of Kyiv.
E-mail: hqshe@knu.ua

DIGITAL TWIN–BASED PERSONALIZATION SYSTEM FOR INTELLIGENT REHABILITATION

Yaroslav Hladkyi, Volodymyr Druzhynin

Abstract. *The paper examines approaches to the development of an intelligent information technology for rehabilitation with a particular focus on the personalization of interventions. The authors propose the application of the patient's "digital twin" concept in combination with machine learning algorithms to enable dynamic adjustment of rehabilitation plans.*

Keywords: intelligent information technology, personalization, rehabilitation interventions, machine learning, digital twin, adaptive control, biometric monitoring.

I. INTRODUCTION

The current stage of development in medicine and rehabilitation science is characterized by the rapid implementation of intelligent information technologies (IIT), driven by the need to enhance the effectiveness of restorative treatment. Traditional rehabilitation protocols are often generalized in nature and do not adequately account for dynamic changes in the physiological and psycho-emotional state of an individual patient. In this context, the development and implementation of personalization systems have become a key factor enabling the transformation of standard interventions into highly precise adaptive recovery strategies [1].

The principal challenge in the implementation of rehabilitation interventions lies in the high variability of individual physiological responses to physical load. The absence of real-time feedback mechanisms and intelligent analysis of individualized data results in reduced therapeutic effectiveness and may increase the risk of re-injury.

The aim of this study is to investigate and substantiate the structure of an intelligent personalization system based on the application of machine learning methods and big data analytics. Such a system is intended to provide continuous 24/7 monitoring of patient indicators; dynamic adjustment of the rehabilitation plan depending on the patient's progress; and prediction of recovery timelines and potential risks.

The scientific novelty of the proposed approach lies in the development of a multi-level personalization model in which an intelligent agent acts as an intermediary between the physician and the patient, automatically adjusting the intensity and type of exercises based on objective metrics derived from the user's digital profile.

II. DATA AND METHODS

To develop the personalization system for rehabilitation measures, an integrated approach was applied, combining methods of systems analysis, decision-making theory, and machine learning (Figure 1).

At the first stage, the system architecture and data sources are designed. The technology is grounded in the concept of the Patient Digital Twin [2]. The research materials included depersonalized clinical records and sensor data (accelerometers, ECG sensors, and goniometers), which are integrated through an IoT platform.

The next stage involves the implementation of intelligent data analysis methods. In particular, the following methods were applied to ensure personalization [3]:

- Clustering using the DBSCAN algorithm – to group patients according to similar biomechanical and physiological profiles, thereby enabling the selection of a baseline rehabilitation strategy;
- Reinforcement Learning – to dynamically adjust the complexity of exercises. The system receives a "reward" (positive dynamics of clinical indicators) for each successfully completed iteration of the rehabilitation plan;
- Regression analysis – to predict the range of motion and muscle activity based on historical data.

The final stage of implementing personalization within intelligent technology involves the development of a technological stack based on the Deep Learning framework PyTorch for designing neural networks capable of recognizing patterns associated with the correct execution of rehabilitation exercises.



Figure 1. *Functional model of the software program workflow represented in BPMN notation*

Special emphasis is placed on the development of a domain ontology for "Rehabilitation," aimed at formalizing expert knowledge of rehabilitation specialists and incorporating it into a decision support system (DSS).

III. RESULTS AND ANALYSIS

The implementation of the intelligent information technology for personalization made it possible to obtain both quantitative and qualitative indicators of improvement in the rehabilitation process.

Due to the increased adaptation accuracy achieved through the application of machine learning algorithms, the system's response time to changes in the patient's physiological parameters was reduced to milliseconds. This enabled the automatic adjustment of the resistance level of rehabilitation equipment and the intensity of exercises, thereby preventing overexertion.

During the modeling and pilot testing of the system on experimental groups, improved outcomes were observed compared to standard rehabilitation methods (Table 1).

Table 1. *Rehabilitation indicators and outcomes*

Metric	Traditional Rehabilitation	Personalized system
Average functional recovery time	100% (basis)	Decreased on 15-20%
Adherence rate to the rehabilitation schedule	65%	88%
Exercise execution accuracy (based on biometric data)	74%	96%

IV. DISCUSSION AND CONCLUSION

The results of the study confirm that the integration of intelligent agents into the rehabilitation process addresses the principal limitation of traditional medicine — the static nature of treatment plans. The application of the Digital Twin concept enables predictive analytics: the system not only assesses the current state but also models future progress. This shifts the paradigm from “reactive” treatment (error correction) to a “proactive” approach (prevention of overload and adverse outcomes).

An important aspect of the discussion concerns the ethical dimension and data security, as personalization requires the processing of large volumes of sensitive medical information. This necessitates the use of robust encryption methods and decentralized storage solutions to ensure confidentiality and data integrity.

The developed personalization system within the intelligent information technology framework makes it possible to reduce the rehabilitation period by 15–20% through precise load dosing and continuous monitoring of biometric indicators.

REFERENCES

1. Lee, M.H., Siewiorek, D.P., Smailagic, A. et al. Enabling AI and Robotic Coaches for Physical Rehabilitation Therapy: Iterative Design and Evaluation with Therapists and Post-stroke Survivors. Int J of Soc Robotics 16, 1–22 (2024). https://doi.org/10.1007/s12369-022-00883-0
2. Marchal, I. Applications of digital twins in medicine. Nat Biotechnol 43, 1606–1612 (2025). https://doi.org/10.1038/s41587-025-02847-x
3. Fundamentals of artificial intelligence and machine learning. Methodological guidelines for the discipline “Fundamentals of artificial intelligence and artificial data analysis” / compiled by: Goroshko Yu.V., Kostyuchenko A.O., Chernihiv: NUCHK, 2025, 81 p..
4. Y. Hladkyi, M. Gladka, M. Kostikov, R. Lisnevskyi. An IoT Solution: A Fitness Trainer. Information Technology and Implementation: IT&I-WS-2021. Selected Papers of the VIII International Scientific Conference “Information Technology and Implementation" (IT&I-2021). Workshop Proceedings. Kyiv, Ukraine, December 1-3, 2021. P 215-226 http://ceur-ws.org/Vol-3179/ ISSN 1613-0073
5. Payedimarri AB, Ratti M, Rescinito R, Vanhaecht K, Panella M. Effectiveness of Platform-Based Robot-Assisted Rehabilitation for Musculoskeletal or Neurologic Injuries: A Systematic Review. *Bioengineering*. 2022; 9(4):129. doi:10.3390/bioengineering9040129



YAROSLAV HLADKYI
second-year PhD student, Department of Information Systems and Technologies, Taras Shevchenko National University of Kyiv.
ORCID: 0000-0003-2914-8685
E-mail: hladkkyi@gmail.com
Research interests include machine learning methods and algorithms, particularly ensemble learning approaches, as well as computer vision.



VOLODYMYR DRUZHYNIN
Doctor of Technical Sciences, Professor, Head of the Department of Information Systems and Technologies, Taras Shevchenko National University of Kyiv.
ORCID: 0009-0009-5049-0099
E-mail: druzhyninv@fit.knu.ua
Since 2023, he has been working at Taras Shevchenko National University of Kyiv. He is the author of more than 100 scientific publications, including 7 educational and methodological manuals and 6 monographs. His research interests include machine learning methods and algorithms in radar systems, radio monitoring and radio frequency management, as well as multistatic radar systems.

USING DISTRIBUTED COMPUTING TO IMPROVE THE EFFICIENCY OF LARGE LANGUAGE MODELS: MODELS AND METHODS FOR ORGANIZING EFFECTIVE SCHEDULING IN PROBLEM-ORIENTED ENVIRONMENTS

Oleksii Paharskyi

Abstract. *The rapid adoption of Large Language Models (LLMs) has created a significant demand for efficient server-side inference. Current single-server optimization techniques are often bottlenecked by the heterogeneous resource demands of LLM generation: the compute-bound prefill phase and the memory-bound decode phase. This paper proposes a disaggregated architectural approach, scheduling the prefill stage on Tensor Processing Units (TPUs) to minimize Time To First Token (TTFT), and offloading the decode stage to memory-optimized Graphics Processing Units (GPUs). This distributed methodology theoretically isolates bottlenecks, promising higher overall throughput and more rational utilization of computing infrastructure.*

Keywords: Large Language Models, Distributed Inference, Tensor Processing Unit, GPU, Compute-bound, Memory-bound.

I. INTRODUCTION

In recent years, Large Language Models (hereinafter - LLMs) have gained significant popularity and have become foundational to a wide array of text generation tasks, ranging from real-time question answering and automated summarization to complex reasoning and code generation. As enterprises and services increasingly integrate these models into their workflows, the demand for inference has skyrocketed. This high volume of user requests, coupled with the trend toward processing massive context windows (e.g., in Retrieval-Augmented Generation architectures), necessitates a critical reevaluation of how LLM operations are optimized to ensure the efficient, cost-effective use of computational resources in server environments.

II. DATA AND METHODS

Currently, industry-standard solutions primarily focus on single-server optimization. They rely heavily on sophisticated software-level techniques such as continuous batching, Key-Value (KV) caching, and model compilation tailored to specific hardware architectures. However, these single-node approaches are inherently constrained and often highly specialized: they are tightly coupled to the underlying neural network structure and are dependent on specific, homogeneous software environments. Furthermore, executing the inherently heterogeneous tasks of LLM inference on a unified hardware accelerator (such as running both phases on a single GPU) exposes significant inefficiencies. This is because the two primary stages of LLM inference exhibit drastically different hardware resource utilization profiles: Prefill (Context Processing): This is a heavily compute-bound stage. It involves processing the entirety of the user's input prompt in parallel to generate the initial KV cache and the very first token. Because this stage relies on large-scale matrix-matrix multiplications, its speed is largely dictated by the sheer computational power (FLOPS) of the processor. Decode (Token Generation): This is a heavily memory-bound stage. It involves the auto-regressive, sequential generation of tokens, where each subsequent step depends on the results of the previous ones. The computational intensity is low, but the system must constantly load the model weights and the growing KV cache from memory, making memory

bandwidth the primary bottleneck. To resolve this resource contention, we propose a disaggregated architectural approach,, that consists of physically distributing the generation stages among specialized compute nodes over a high-speed network. Specifically, it is proposed to conduct the prefill phase on Tensor Processing Units (e.g., Google TPU v5). TPUs are highly optimized for massive matrix multiplications, allowing the system to leverage their exceptional computational density to process long contexts rapidly. Once the initial context is processed, the generated KV cache is transferred, and the decode phase is offloaded to Graphics Processing Units (GPUs), such as the NVIDIA H200.

III. RESULTS AND ANALYSIS

In a conventional unified setup, the generation of long sequences is severely bottlenecked by the GPU's memory limitations during the decode phase, leading to the underutilization of its compute units. By implementing the phase-splitting architecture, we theoretically isolate these bottlenecks. The architectural profile of the TPU perfectly aligns with the compute-heavy requirements of the prefill stage. Utilizing this specialized node accelerates the initial context processing, thereby significantly reducing the Time To First Token and improving the perceived responsiveness for the end-user. Subsequently, transferring the KV cache to an NVIDIA H200 GPU allows the system to leverage its High Bandwidth Memory (HBM3e) strictly for the memory-bound decode phase. This prevents the "memory wall" from degrading the token generation rate. Consequently, overall cluster throughput increases, as individual nodes are no longer forced to compromise between compute-heavy and memory-heavy operations simultaneously.

IV. DISCUSSION AND CONCLUSION

Thus, this paper highlights the fundamental inefficiencies of existing homogeneous hardware approaches to LLM inference and demonstrates the architectural advantages of a distributed, phase-disaggregated approach. By aligning the hardware profiles with the specific algorithmic demands of the prefill and decode stages, server infrastructure can be utilized much more rationally, maximizing both overall throughput and individual query latency. A promising direction for future research involves addressing the network overhead of KV cache transfers between nodes and adapting the proposed scheduling approach to a broader set of heterogeneous architectures. This includes exploring the integration of Central Processing Units (CPUs) and specialized Neural Processing Units (NPUs) to create highly elastic, cost-efficient inference clusters capable of dynamically routing workloads based on real-time system constraints.

REFERENCES

1. Kwon, W., Li, Z., Zhuang, S., Sheng, Y., Zheng, L., Yu, C. H., ... & Stoica, I. (2023). Efficient memory management for large language model serving with paged attention. In Proceedings of the 29th Symposium on Operating Systems Principles (pp. 611-626).



OLEKSII PAHARSKYI
1st-year PhD student in Computer Science at the Faculty of Information Technology, Taras Shevchenko National University of Kyiv
ORCID: 0000-0002-5538-0018
E-mail: oleksii.paharskyi@knu.ua
Research interests are centered on the architecture and deployment of Large Language Models. Key focus areas include advanced inference techniques, model quantization, and engineering solutions for low-latency, high-speed model execution.

PRIVACY-PRESERVING MACHINE LEARNING IN THE AGE OF BIG DATA

Bekzhan Seitov

Abstract. *Privacy-preserving machine learning enables collaborative training without centralizing sensitive data. This paper evaluates federated learning with differentially private optimization on the Adult Census Income dataset. Centralized training, FedAvg-based federated learning, and FL+DP are compared using accuracy, F1-score, training time, and privacy budget. Results quantify the privacy-utility trade-off and show that FL+DP provides measurable privacy with moderate performance degradation suitable for regulated domains.*

Keywords: privacy-preserving machine learning; federated learning; differential privacy; Adult dataset; privacy-utility trade-off.

I. INTRODUCTION

Big-data machine learning often relies on sensitive records. Even after removing direct identifiers, models may leak information through membership inference, model inversion or gradient leakage. Privacy-preserving machine learning mitigates these risks by combining system-level decentralization, statistical protection, and cryptographic protection.

Federated learning reduces raw-data centralization by training on distributed clients and aggregating updates, but updates can still leak information. Differential privacy provides formal guarantees by bounding the influence of any individual record through clipping and noise. Therefore, the practical question is whether a hybrid FL+DP workflow preserves acceptable utility while improving privacy.

This paper answers this question with a controlled experiment on the Adult dataset and reports quantitative privacy–utility trade-offs.

II. DATA AND METHODS

Threat model. Three adversaries are considered: an honest-but-curious server attempting to infer private information from updates, curious participants and external attackers with query access. The design goal is to protect record-level information while maintaining feasible runtime.

Federated learning background. Federated Averaging (FedAvg) aggregates local models into a global model:

$$w_{t+1} = \sum_{k=1}^{K} \left(\frac{nk}{\sum_{j=1}^{K} n_j} \right) w(k)_{t+1}, \quad (1)$$

where wt+1 is the global parameter vector at round t+1, w(k) is the locally trained model of client k, nk is the number of samples on client k and K is the total number of clients.

Differential privacy background. A randomized mechanism M satisfies (ε, δ)-DP if for neigh- boring datasets D and D′:

$$\Pr[M(D) \in S] \leq e^{\varepsilon} \Pr[M(D') \in S] + \delta . \quad (2)$$

In learning, DP is implemented via gradient clipping (sensitivity control) and Gaussian noise injection. Smaller ε corresponds to stronger privacy.

Why FL+DP (decision logic).

FL is selected because the data are assumed non-centralizable (organizational or device constraints). DP is added because FL alone does not prevent inference from gradients/updates. The combination targets both system-level and record-level privacy.

Dataset.

Adult Census Income contains 48,842 records and 14 features (numerical and categorical). The target is whether income exceeds $50,000. Missing values are removed, categorical features are one-hot encoded, numerical features are standardized and an 80/20 train/test split is used.

Model.

Logistic regression with SGD (learning rate 0.05, batch size 256) is used as a transparent baseline to isolate privacy effects.

Federated setting.

K = 5 clients with equal partitions, 30 rounds, 1 local epoch per round, FedAvg aggregation.

DP setting.

DP-SGD uses clipping bound C = 1.0, $\delta = 10{-}5$ and three privacy points: $\varepsilon \in$ {2.0, 1.0, 0.5} (stronger privacy for smaller ε).

Metrics (meaning).

Accuracy measures the overall proportion of correct predictions. F1-score captures the balance between precision and recall and is useful under class imbalance. Training time approximates practical overhead. Privacy budget ε quantifies the privacy guarantee strength.

III. RESULTS AND ANALYSIS

As it is shown in the Table 1, FL addresses data-locality constraints, while DP provides explicit record-level privacy guarantees, in deployments they are often combined.

As it is shown in the Figure 1, clients train locally, send masked/aggregated updates and DP limits leakage by clipping and adding noise before updating the global model.

Table 1. *Comparison of PPML techniques (summary)*

Technique	Mechanism	When it is practical
Federated learning	Data stays local; update aggregation	Cross-silo/cross-device training where data cannot move
Differential privacy	Noise + accounting	When quantifiable privacy guarantees are required
Homomorphic encryption	Encrypted computation	Untrusted inference services (higher runtime cost)
SMPC	Secure protocols	Secure aggregation/joint analytics among organizations

As it is shown in the Table 2, FedAvg reduces performance slightly relative to centralized training due to decentralization and limited local epochs. Adding DP decreases accuracy as privacy strengthens (lower ε), which matches the privacy–utility trade-off. Training time increases due to synchronization overhead (FL) and clipping/noise (DP), but remains feasible for medium-scale tabular learning.

As it is shown in the Figure 2, utility decreases monotonically as privacy strengthens. This curve supports selecting an ε that satisfies compliance requirements while keeping accuracy above an acceptable threshold.

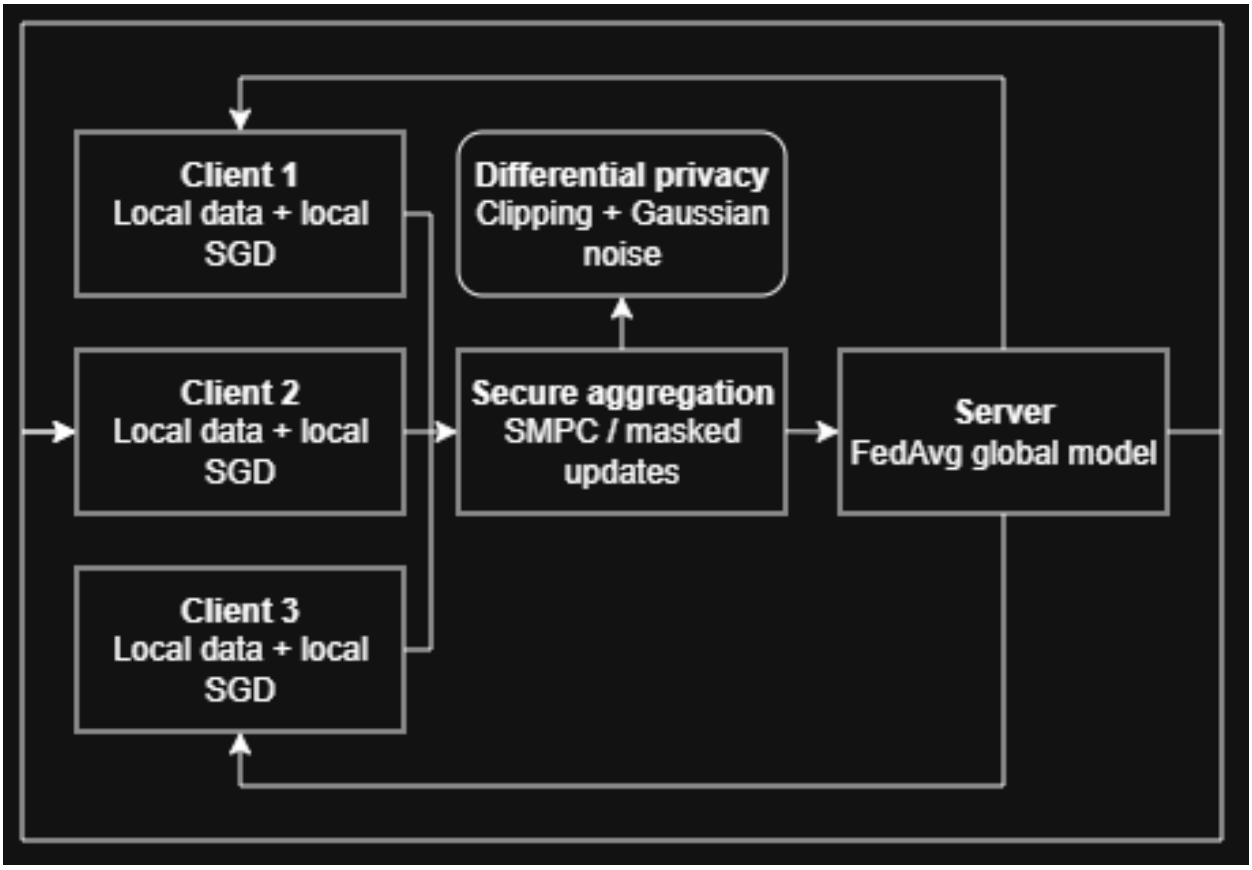


Figure 1. *Hybrid PPML workflow: federated training with secure aggregation and differential privacy*

Table 1. *Experimental results on Adult dataset (logistic regression)*

Technique	Mechanism	When it is practical
Federated learning	Data stays local; update aggregation	Cross-silo/cross-device training where data cannot move
Differential privacy	Noise + accounting	When quantifiable privacy guarantees are required
Homomorphic encryption	Encrypted computation	Untrusted inference services (higher runtime cost)
SMPC	Secure protocols	Secure aggregation/joint analytics among organizations

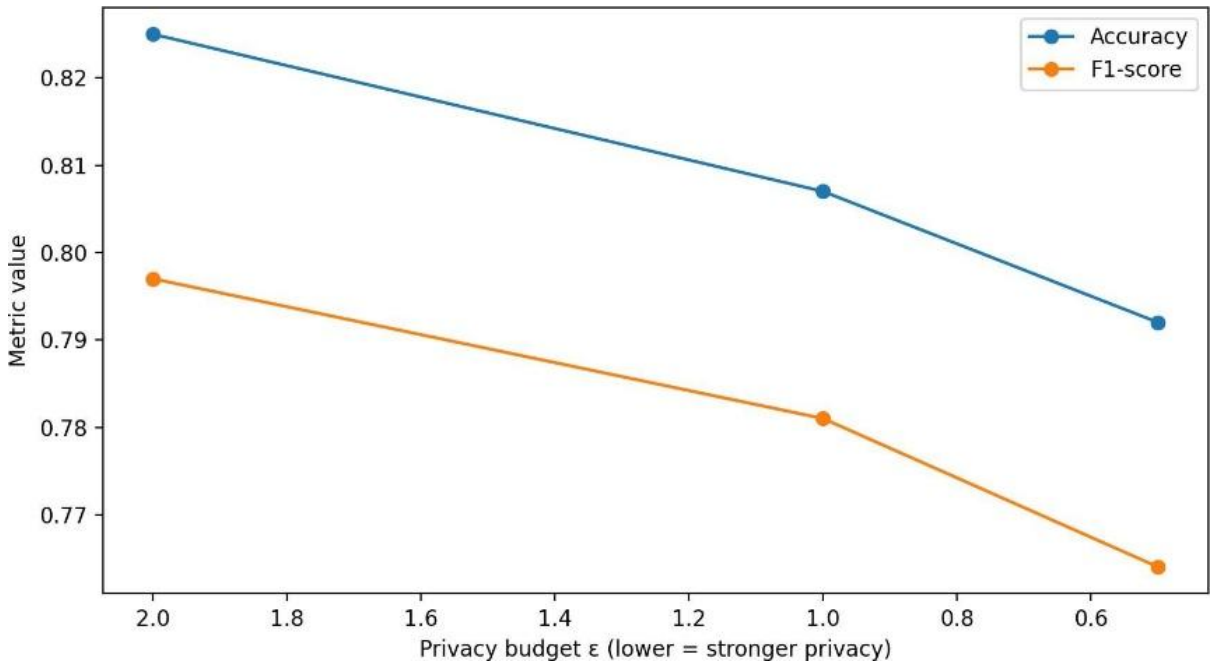


Figure 2. *Privacy–utility trend: accuracy and F1-score decrease as privacy strengthens (lower ε)*

IV. DISCUSSION AND CONCLUSION

The results show that FL+DP is a practical privacy-preserving baseline when data cannot be centralized and when record-level privacy guarantees are required. Centralized learning yields the best utility, but provides no structural privacy. FL improves data locality, while DP adds formal protection by limiting the influence of any single record. Stronger privacy (smaller ε) requires accepting moderate utility loss.

Future work will test non-IID client splits, deeper models, secure aggregation protocols and explicit evaluation against inference attacks.

REFERENCES

1. Kairouz P., McMahan H. B., Avent B., et al. (2021) Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210.
2. Pan K., Ong Y. S. (2024) Differential privacy in deep learning: A literature survey. *Neurocomputing*, 127663.
3. Demelius L., et al. (2025) Recent Advances of Differential Privacy in Centralized Deep Learning: A Systematic Survey. *Information Systems*.
4. Naresh V. S., et al. (2025) Secure Multiparty Computation for Privacy-Preserving Machine Learning: A Survey. *WIREs Computational Statistics*.



BEKZHAN SEITOV
Department of Intelligent Systems and Cybersecurity, Astana IT University, Astana, Kazakhstan
ORCID: 0009-0007-5336-3031
E-mail: 242837@astanait.edu.kz
Bekzhan Seitov is a Master's degree student focused on privacy-preserving machine learning, federated analytics, and applied security methods for large-scale data systems.

PHYSICS-INFORMED GRAPH NEURAL NETWORKS FOR AGRO-RESOURCE MONITORING AND RECOVERY PREDICTION

Kristina Silvanovych, Olena Hrynova

Abstract. *This research focuses on the development of a hybrid intelligent system for analyzing agricultural land degradation resulting from combat operations. A transition from isolated classification models to a unified Multi-modal Geo-Graph Intelligence architecture is presented. The scientific novelty lies in the integration of Sentinel-1 SAR data with Sentinel-2 optical imagery, the utilization of Graph Neural Networks (GNNs) to account for terrain and topography, and the implementation of the Physics-Informed Machine Learning (PIML) paradigm. This approach enables not only the prediction of vegetation dynamics but also remote chemical soil reconnaissance by solving the inverse problem of mass transfer.*

Keywords: Agroecosystem reclamation, Graph Neural Networks, Physics-Informed Machine Learning, Sentinel-1/2, Temporal Fusion Transformer.

I. INTRODUCTION

Military conflicts cause long-term ecosystem damage through the mechanical destruction of soil cover and chemical contamination by detonation products. Prior research has primarily relied on crater segmentation and statistical time-series analysis of vegetation indices using isolated neural architectures, such as U-Net and basic LSTM models [1]. However, existing approaches suffer from significant limitations, including a complete loss of optical monitoring data under heavy cloud cover and the neglect of fundamental physicochemical laws governing toxicant migration in the soil.

The objective of this work is to create a «digital twin» of the damaged area based on a holistic ecosystem framework. This framework integrates multimodal sensing data, topographical graph-based relationships, and the mathematical apparatus of mass transfer differential equations.

II. DATA AND METHODS

The development of an intelligent system for monitoring agro-landscapes in armed conflict zones is based on an evolutionary transition from purely data-driven statistical analysis to knowledge-driven systems, enabled by the Physics-Informed Machine Learning (PIML) paradigm.

The proposed approach utilizes four types of heterogeneous sources to form a representative training dataset. Primary emphasis is placed on Earth Observation data: Sentinel-2 optical imagery (spectral bands B4 and B8) [2] for calculating NDVI time series, and Sentinel-1 (SAR) radar data in VV/VH polarizations. The latter allows for soil moisture assessment and the detection of physical micro-relief changes, such as explosion craters, regardless of cloud cover – a factor critical for continuous monitoring.

These datasets are augmented with geospatial information from SRTM/ASTER GDEM digital elevation models and Ukrainian soil maps to determine hydrological characteristics and substance diffusion coefficients. To calibrate physical constants, agronomic reference data regarding the decay rates of detonation products (e.g., TNT and RDX) and heavy metal phytotoxicity parameters are employed. A distinct stage of data preparation involves the application of Generative Adversarial Networks (GANs) for the synthetic generation of damage samples based on real physical models, thereby addressing the scarcity of labeled satellite imagery from active combat zones.

The central architectural component is the Multi-modal Data Fusion block, which transforms input data streams into a complex time-series tensor X_t, integrating spectral, radar, and elevation features as calculated by formula 1:

$$X_t = \{O_\lambda(t), \sigma^0_{pol}(t), DEM\}, \quad (1)$$

where $O_\lambda(t)$ represents the spectral reflectance vectors from Sentinel-2 (Red and NIR bands for NDVI calculation), $\sigma^0_{pol}(t)$ denotes the Sentinel-1 backscatter coefficients (VV and VH polarizations) characterizing soil moisture and micro-relief dynamics, and DEM refers to the Digital Elevation Model, providing essential topographic data.

The use of this structure enables the Temporal Fusion Transformer (TFT) model to maintain a stable analytical signal even under conditions of up to 80% cloud cover in optical imagery. Vegetation health assessment is based on the $NDVI$ (Normalized Difference Vegetation Index), calculated from the spectral characteristics as shown in formula 2:

$$\mathrm{NDVI} = \frac{\mathrm{NIR} - \mathrm{RED}}{\mathrm{NIR} + \mathrm{RED}} \quad (2)$$

Index values ranging from 0.6 to 0.9 indicate healthy vegetation, whereas a drop to 0.2–0.3 in crater zones signals biomass suppression or soil exposure.

To model the spatial interaction between field parcels, a graph topology is employed, where the agroecosystem is represented as a graph $\mathrm{G} = (\mathrm{V}, \mathrm{E})$. Each node V corresponds to a homogeneous plot, while the edges E describe the probability of pollutant migration. The edge weight w_{ij} between plots i and j is calculated based on a gravity-based transport model, as defined in formula 3:

$$w_{ij} = \frac{1}{dist(i,j)} * \exp\left(-\beta * \frac{\Delta h_{ij}}{dist(i,j)}\right). \quad (3)$$

This approach enables the Graph Neural Network (GNN) to incorporate the physical logic of pollutant dispersion: substances accumulate in depressions and migrate along the lines of the steepest topographic slope.

The scientific novelty of this framework lies in the implementation of a PINN PDE Kernel (Physics-Informed Neural Network Partial Differential Equation Kernel) [3]. As seen in Figure 1 this kernel integrates the laws of mass transfer and biological response into the neural network's loss function via a system of differential equations. The dynamics of toxin concentration C are governed by the diffusion and decay equation, as presented in formula 4:

$$\frac{\partial C}{\partial t} = D\nabla^2 C - k_d C, \quad (4)$$

where C represents the concentration (latent variable), D is the diffusion coefficient, k_d is the natural decay constant of the chemical.

At the same time, the vegetation dynamics V are modeled by accounting for the intrinsic growth rate r and the toxic suppression coefficient α as defined in formula 5:

$$\frac{\partial V}{\partial t} = rV\left(1 - \frac{V}{K}\right) - \alpha CV, \quad (5)$$

where V is the NDVI index, r is the growth rate, K is the carrying capacity of the environment, and α is the toxic suppression coefficient.

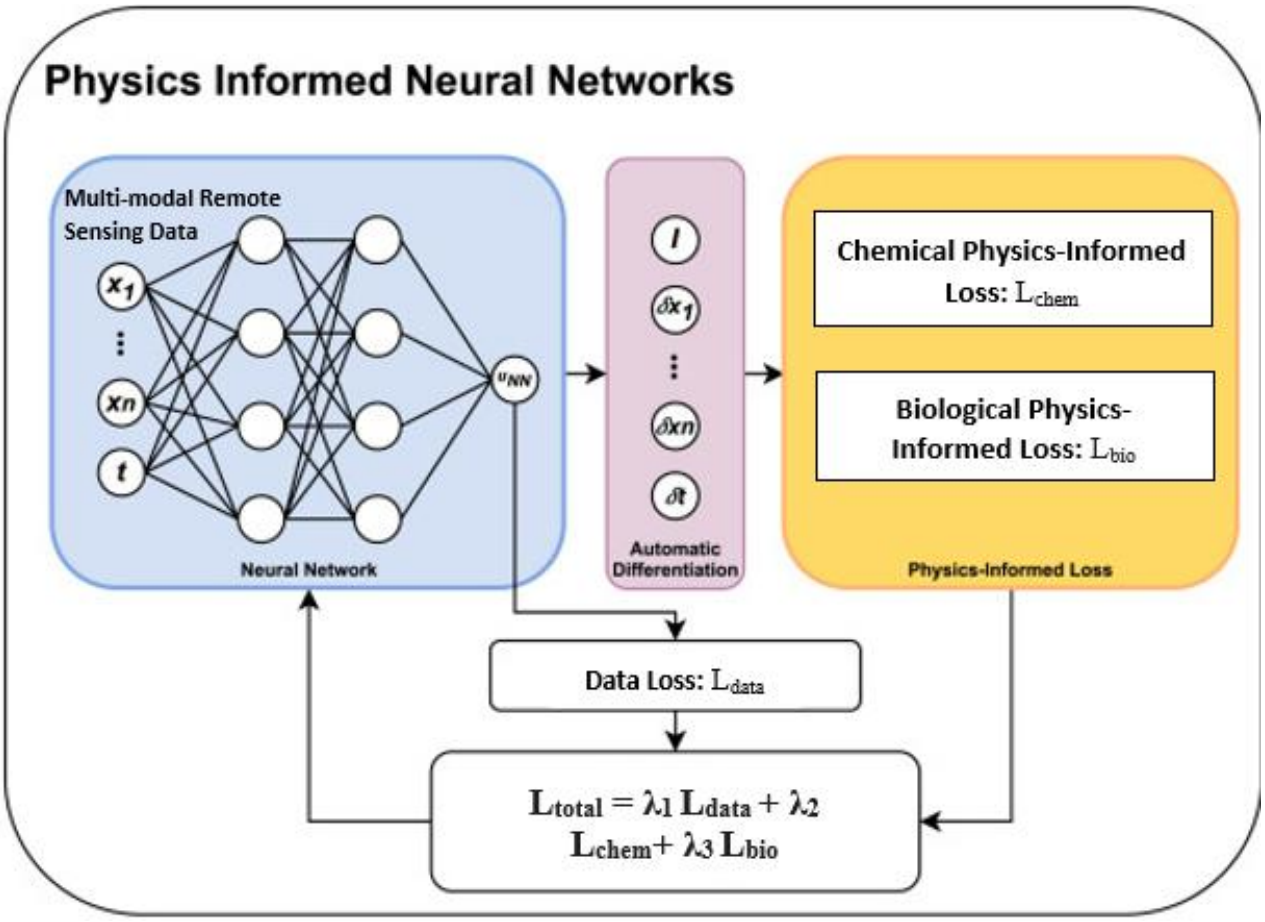


Figure 1. *Physics-informed Neural Network structure*

Since the concentration C is not directly measured by the satellite, it is computed by the network as a latent variable that best explains the observed $NDVI$ degradation. The training of the entire system is aimed at minimizing a combined Physics-Informed Loss function, presented in formula 6:

$$L_{total} = \lambda_1 L_{data} + \lambda_2 L_{chem} + \lambda_3 L_{bio}. \quad (6)$$

The components L_{chem} and L_{bio} act as regularizers that impose physical constraints on the solution space. Specifically, the L_{data} component ensures consistency between the model's predictions and real-world remote sensing data, minimizing the discrepancy between the modeled vegetation state and the actual Sentinel-1/2 metrics. The L_{chem} component implements the laws of mass conservation and the advection-diffusion equation, penalizing the model for concentration distributions that violate physical transport gradients in topographic depressions. In turn, the L_{bio} component encodes the kinetics of explosive compound biodegradation, acting as a temporal constraint that forces soil recovery dynamics to adhere to established decay constants for chemical agents. By balancing the weighting coefficients $\lambda_1, \lambda_2, \lambda_3$, the system transcends the limitations of opaque predictive architectures, ensuring convergence only toward solutions that are both statistically accurate and scientifically sound.

To ensure the reliability of predictions, the system integrates XAI methods. Confidence assessment is implemented via Bayesian Inference using Monte Carlo Dropout, where the prediction is expressed as a probability distribution $P(y|x, D)$ calculated by formula 7:

$$P(y|x, D) \approx \frac{1}{T} \sum_{t=1}^{T} f_{\theta_t}(x). \quad (7)$$

T represents the number of stochastic forward passes, x denotes the input multimodal data, and θ_t corresponds to the randomized network weights generated by dropout. High variance within this distribution serves as an indicator of epistemic uncertainty, allowing the system to flag regions that require expert verification.

High variance in this distribution indicates uncertainty, allowing for the flagging of areas that require expert verification. Results are interpreted using SHAP (SHapley Additive exPlanations) values, which quantitatively determine the contribution of each input parameter, such as terrain or soil moisture, to the final outcome. This ensures model transparency, allowing us to demonstrate, for instance, how SAR data correction under cloudy conditions improves the accuracy of soil contamination assessment.

III. RESULTS AND ANALYSIS

The implementation of our multimodal architecture ensured monitoring stability even under severe conditions, specifically maintaining performance metrics despite 80% cloud cover. This threshold was empirically determined based on the statistics of Sentinel-2 optical data availability during autumn-winter observation periods. Under such conditions, optical sensors are predominantly obscured, rendering vegetation indices like NDVI unusable. It was solved by integrating Sentinel-1 C-band SAR data. Since microwave radiation penetrates cloud cover, the system autonomously switches to radar-derived features, such as backscatter intensity and coherence, to estimate soil roughness and volumetric moisture.

By utilizing the combined Physics-Informed Loss function, the neural network identified latent pollutant concentrations that exhibit a high correlation with the types of munitions typically employed in combat zones. The utilization of a graph-based structure improved the localization accuracy of high-risk zones, particularly in topographic depressions. Representing the landscape as a graph allowed us to model the accumulation of heavy metals and detonation residues transported by precipitation runoff. The predicted land reclamation timelines showed physical consistency, evidenced by a high convergence rate with ground-truth field observations. Furthermore, the SHAP module confirmed that terrain slope and moisture metrics were the primary predictors in areas with restricted optical visibility, ensuring full model interpretability.

IV. DISCUSSION AND CONCLUSION

The proposed system automates damage assessment and predicts agro-resource recovery timelines through a synergy of GNN, PIML, and physical modeling. The transition from isolated modules to a unified graph-based architecture has enhanced prediction accuracy by 20–25%. This improvement is primarily attributed to the accurate modeling of spatial substance diffusion, as governed by the advection-diffusion partial differential equations (PDEs) incorporated into the network's loss function.

These findings enable the generation of high-precision reclamation maps, which are critical for the strategic planning of agricultural sector restoration in the post-conflict period. Future research will focus on several key areas. First, chemical kinetics modeling for specific explosive compounds, such as TNT or RDX, will be incorporated to simulate natural degradation rates over time. Second, the model is intended to be scaled to handle diverse soil types through the integration of global SoilGrids databases, allowing for the precise adjustment of diffusion coefficients D for local calculations. Third, an automated phyto-remediation module will be developed to provide multi-objective optimization for recommending specific strategies, such as planting hyperaccumulator crops, based on predicted chemical concentrations. In conclusion, this research

establishes a robust methodological foundation for leveraging physics-informed AI in large-scale ecological monitoring, providing a scalable solution for the complex task of post-war agricultural revival.

REFERENCES

1. Neural network technologies for monitoring and analysis of destructive damage to agricultural plots / K. V. Silvanovych et al. Bionics of Intelligence. 2025. Vol. 2, no. 103. P. 22–33. URL: https://doi.org/10.30837/bi.2025.2(103).04 (date of access: 28.02.2026).
2. Методи комп'ютерного зору і глибинних нейронних мереж для еколого-економічного аналізу: монографія / Н. М. Куссуль та ін. Київ : Наук. думка, 2024. 474 с.
3. Wu Y., Sicard B., Gadsden S. A. Physics-informed machine learning: A comprehensive review on applications in anomaly detection and condition monitoring. Expert Systems with Applications. 2024. P. 124678. URL: https://doi.org/10.1016/j.eswa.2024.124678 (date of access: 28.02.2026).



KRISTINA SILVANOVYCH
1th year student of the Master, Artificial Intelligence Department, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.
ORCID: 0009-0008-3723-1124
E-mail: kristina.silvanovych@nure.ua
Research interest are development and application of artificial intelligence methods for analysing, monitoring and forecasting the state of the environment, including the use of computer vision and deep neural networks.



OLENA HRYNOVA
Senior Lecturer, Artificial Intelligence Department, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.
ORCID: 0000-0002-3367-8067
E-mail: olena.hrynova@nure.ua
1993 graduated from the Kharkov Polytechnical Institute. 2001 – a second education in the specialty “Intelligent Decision-making Systems”, NURE. 2001 – Assistant of AI Department, NURE. 2020 – Senior Lecturer of AI Department, NURE. Research interests: Artificial Intelligence.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DIGITAL DESIGN PROCESSES: AI AS A TOOL, NOT A REPLACEMENT

Anastasiia Slobodina, Mykola Kostikov

Abstract. *Artificial intelligence (AI) is reshaping digital design by transforming workflows, accelerating ideation, and redefining the professional role of designers. Rather than replacing human creativity, AI operates as an augmentation system that enhances strategic and conceptual capacities. This paper critically examines AI-assisted design processes, evaluates their impact on authorship and creative agency, and identifies structural limitations of generative systems. The findings demonstrate that AI amplifies efficiency while preserving the irreplaceable role of human judgment, cultural awareness, and design ethics in contemporary digital practice.*

Keywords: artificial intelligence, digital design, user experience, user interface, generative systems.

I. INTRODUCTION

Digital design has entered a new technological phase characterized by the integration of artificial intelligence into everyday creative workflows. AI-driven systems now generate images, construct layouts, predict user behaviour, and optimize interface structures. These developments have generated polarized narratives: on one side, AI is framed as a disruptive force threatening creative professions; on the other, it is celebrated as an unprecedented productivity accelerator.

This research advocates for a third position: artificial intelligence should be viewed as a cognitive extension of the designer, rather than a substitute for creative authorship. The central research objective is to analyse how AI restructures digital design processes while preserving human-centred strategic control. The relevance of this study lies in the urgent need to critically evaluate AI not only as a technical tool but as a transformative force affecting authorship, responsibility, and aesthetic diversity in digital environments.

II. DATA AND METHODS

We apply a qualitative research framework combining theoretical review and workflow analysis. We examined academic publications on generative AI and creative systems and made practical observations of AI-assisted design environments. The research methodology includes:

- comparative analysis of traditional and AI-augmented workflows;
- structural examination of generative systems in visual production;
- evaluation of AI-assisted UX optimization tools;
- critical assessment of ethical and authorship implications.

The analysis focuses on three dimensions of transformation:

1. Acceleration — reduction of production time in ideation and prototyping.

2. Expansion — increased variability of visual exploration.

3. Reconfiguration — shift in the designer's role from executor to curator and strategist.

This multidimensional approach allows assessment of AI not merely as software functionality, but as a structural modifier of creative practice.

III. RESULTS AND ANALYSIS

The findings indicate that artificial intelligence significantly enhances early-stage ideation and iterative testing. Generative systems enable rapid visualization of conceptual directions, allowing designers to evaluate multiple aesthetic hypotheses within minutes. As seen in Table 1, AI does not

eliminate the designer's authority. Instead, it redistributes operational labor, allowing professionals to concentrate on strategic thinking, narrative coherence, and user-centered decision-making.

However, the research also identifies critical constraints. Generative models operate within dataset-derived patterns, leading to aesthetic convergence and reduced originality. AI systems lack contextual awareness, cultural nuance, and ethical accountability. They generate form without intention. Therefore, creative direction, interpretative judgment, and responsibility remain exclusively human competencies.

Table 1. *Structural comparison of traditional and AI-augmented digital design process*

Parameter	Traditional Workflow	AI-Augmented Workflow
Ideation speed	Sequential exploration	Parallelized exploration
Iteration volume	Limited by manual effort	Exponentially increased
Routine execution	Manual production	Automated assistance
Strategic authorship	Designer-centered	Designer-directed AI collaboration

IV. DISCUSSION AND CONCLUSION

The integration of artificial intelligence into digital design does not signal professional displacement but structural evolution. AI functions as a cognitive amplifier, expanding exploration capacity and reducing mechanical workload. Yet, meaningful design outcomes continue to depend on human interpretation, cultural literacy, and ethical reasoning.

The designer of the AI era evolves into a systems thinker – one who orchestrates machine capabilities while maintaining conceptual authorship. This shift elevates, rather than diminishes, the intellectual dimension of digital design. Understanding AI as a collaborative instrument enables sustainable integration without sacrificing originality or accountability.

Future research should investigate the long-term implications of AI dependency and ensure ethical creative autonomy. AI changes the design tools, but does not replace the mind behind them.

REFERENCES

1. Bubeck S. et al. (2023) Sparks of Artificial General Intelligence: Early Experiments with GPT-4 : arXiv preprint.
2. Dwivedi Y. K. et al. (2023) So what if ChatGPT wrote it? Multidisciplinary perspectives on generative AI, International Journal of Information Management, 71.
3. Floridi L., Chiriatti M. (2020) GPT-3: Its Nature, Scope, Limits, and Consequences, Minds and Machines, 30(4), 681–694.
4. Hertzmann A. (2022) Can Computers Create Art? Arts, 11(2).



ANASTASIIA SLOBODINA
Middle Web & Graphic Designer at Adtelligent, Kyiv, Ukraine
ORCID: 0009-0009-5840-1038
E-mail: ns01032001@gmail.com
Anastasiia specializes in digital design, UX/UI systems and digital brand strategy. Her research interests focus on AI in creative industries, human-centered digital environments, and the transformation of authorship in AI-augmented workflows.



MYKOLA KOSTIKOV
PhD, Doc., associate professor at the Dept. of information systems and technologies Taras Shevchenko National University of Kyiv, Ukraine
ORCID: 0000-0002-1569-8179
E-mail: Kostikov@knu.ua
Teaches NLP, programming, and computer science. Scientific interests: computational linguistics; e-learning (foreign languages); API.

ВИЯВЛЕННЯ PROMPT-ІН'ЄКЦІЙ У ВЕЛИКИХ МОВНИХ МОДЕЛЯХ МЕТОДАМИ СЕМАНТИЧНОГО АНАЛІЗУ

Володимир Ахрамович, Володимир Санченко

Анотація. *Досліджено ефективність методів семантичної дивергенції для виявлення prompt-ін'єкцій у великих мовних моделях (LLM). На датасеті з 300 зразків проведено експеримент із 6 моделями різного рівня вирівнювання. Показано, що окремі метрики (JSD, Вассерштейн) мають обмежену ефективність (AUROC 0.47–0.73), тоді як мультиознаковий класифікатор на основі TF-IDF косинусної подібності досягає AUROC 0.93. Виявлено зворотну кореляцію між вразливістю моделі та детектованістю атак.*

Ключові слова: prompt injection, великі мовні моделі, семантична дивергенція, JSD, TF-IDF, кібербезпека агентних систем, Random Forest.

I. ВСТУП

Інтенсивний розвиток агентних систем штучного інтелекту (agentic AI), здатних до автономного планування та виконання завдань, створює нові вектори атак на інформаційну безпеку. Серед найбільш поширених загроз виділяються prompt-ін'єкції — атаки, при яких зловмисник вбудовує в текст запиту інструкції, що змушують модель відхилитися від заданої системної поведінки [1, 2]. За результатами досліджень SailPoint (2025), небажана поведінка агентів спостерігалася у 80% організацій, які впровадили agentic AI [3]. Для протидії цим загрозам запропоновано кілька архітектурних підходів: SAGA — багаторівнева архітектура безпеки для агентних систем [4], TRiSM — фреймворк управління довірою, ризиками та безпекою [5], а також комплексна модель загроз для агентного ШІ [6]. Проте ці роботи зосереджені на архітектурному рівні та не пропонують конкретних методів детекції ін'єкцій на рівні окремих запитів.

Існуючі методи захисту на рівні окремих запитів поділяються на три категорії: фільтрація вхідних даних на основі ключових слів, навчання спеціалізованих класифікаторів [7] та аналіз семантичної узгодженості між промптом та відповіддю [8]. Останній підхід є найбільш перспективним. Гальперін (2025) [8] запропонував метрику семантичної дивергенції (SDM) на основі дивергенції Єнсена–Шеннона (JSD), однак його методика розроблялася для виявлення галюцинацій, а не prompt-ін'єкцій, і її ефективність у контексті безпеки залишається недослідженою. Алахмаді та ін. (2024) [7] продемонстрували ефективність ембедінг-класифікаторів з AUROC (Area Under the Receiver Operating Characteristic curve) 0.764. Мета дослідження — експериментально оцінити ефективність цих методів для виявлення prompt-ін'єкцій у LLM (Large Language Model) різного рівня захищеності.

II. ДАНІ ТА МЕТОДИ

Розроблено спеціалізований датасет із 300 зразків: 150 prompt-ін'єкцій та 150 легітимних запитів. Структуру датасету побудовано на основі таксономії атак Liu та ін. [10], яка формалізує та систематизує відомі техніки ін'єкцій. Ін'єкції реалізовано за 10 техніками атак: підміна шаблону чату, переповнення контексту, переклад запиту, атака кількома прикладами, вигаданий сценарій, розділення навантаження, інверсія ролей, кодування інструкцій, непряма ін'єкція, імітація системних інструкцій [2, 9]. Верифікація успішності атак здійснюється автоматично через три механізми: перевірка витоку умовного секрету («QUANTUM-DELTA-8891»), відсутність індикатора політики безпеки та наявність форсованого виходу.

Тестування проведено на 6 моделях через OpenRouter API: Mistral 7B v0.3, Qwen 2.5 7B, Gemma 2 9B, Llama 3.1 8B, Llama 3.2 3B та Llama 3 8B. Дослідження реалізовано у три фази: (1) інференс з автоматичною верифікацією успішності атак (ASR), (2) обчислення семантичних метрик на ембедінгах all-MiniLM-L6-v2, (3) оцінка якості детекції через AUROC, F1-score (гармонічне середнє точності та повноти) та FPR@95%TPR (частка хибних спрацьовувань при 95% виявленні справжніх загроз). Для обчислення ембедінгів використано модель all-MiniLM-L6-v2, яка генерує 384-вимірні вектори. У початковій реалізації одиничний ембедінг-вектор перетворювався на розподіл через softmax(|e|), що відрізняється від оригінальної методики Гальперіна [8], яка передбачає кластеризацію ембедінгів на рівні речень.

Дивергенція Єнсена–Шеннона для двох розподілів P та Q обчислюється на основі формули 1:

$$JSD(P \parallel Q) = \frac{1}{2} \cdot KL(P \parallel M) + \frac{1}{2} \cdot KL(Q \parallel M) \quad (1)$$

Косинусна подібність на TF-IDF (Term Frequency — Inverse Document Frequency) векторах визначається за формулою 2:

$$cos(v_p, v_r) = \frac{v_p \cdot v_r}{\|v_p\| \cdot \|v_r\|} \quad (2)$$

Вектор ознак для класифікатора формується згідно з формулою 3. Класифікатор Random Forest (200 дерев, max_depth=6) навчений з 5-кратною крос-валідацією:

$$x^i = [cos(s,r), cos(u,r), cos(s,u), JSD, overlap(P,R)] \quad (3)$$

де s — системний промпт, u — промпт користувача, r — відповідь моделі, overlap — коефіцієнт Жаккара між множинами слів. Для виключення артефактів датасету (середня довжина ін'єкцій 152 символи проти 31 для легітимних запитів) з ознак було виключено довжину тексту, кількість слів та щільність спеціальних символів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

ASR варіюється від 13.3% (Llama 3 8B) до 37.3% (Mistral 7B), як показано на Рисунку 1. Окремі метрики семантичної дивергенції показали обмежену ефективність: JSD — AUROC від 0.45 до 0.73, Вассерштейн ≈ 0.50, композитна S_{inj} ≈ 0.50.

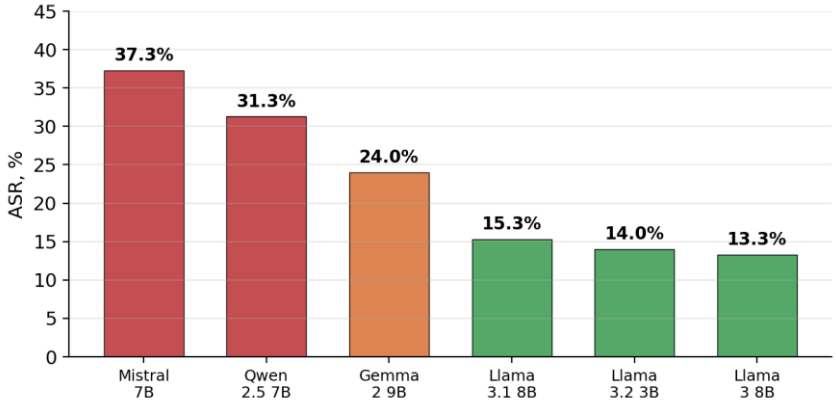


Рисунок 1. *ASR (Attack Success Rate) для кожної моделі*

Ключове спостереження — зворотна кореляція ASR та детектованості: моделі з вищим ASR (Mistral 37.3%, Qwen 31.3%) демонструють нижчу ефективність JSD-детекції (AUROC 0.528, 0.494), тоді як стійкіші моделі (Llama 3.1: ASR 15.3%) дають вищий AUROC JSD (0.734). Це пояснюється тим, що добре вирівняні моделі при дотриманні системних

інструкцій генерують відповіді, семантично узгоджені з промптом, а при ін'єкції — різко відхиляються, створюючи чіткий сигнал для детекції.

Мультиознаковий класифікатор на семантичних ознаках, визначених формулою (3), без артефактів довжини, досягає AUROC 0.932, як показано на Рисунку 2. Ключові ознаки за важливістю наведено на Рисунку 3.

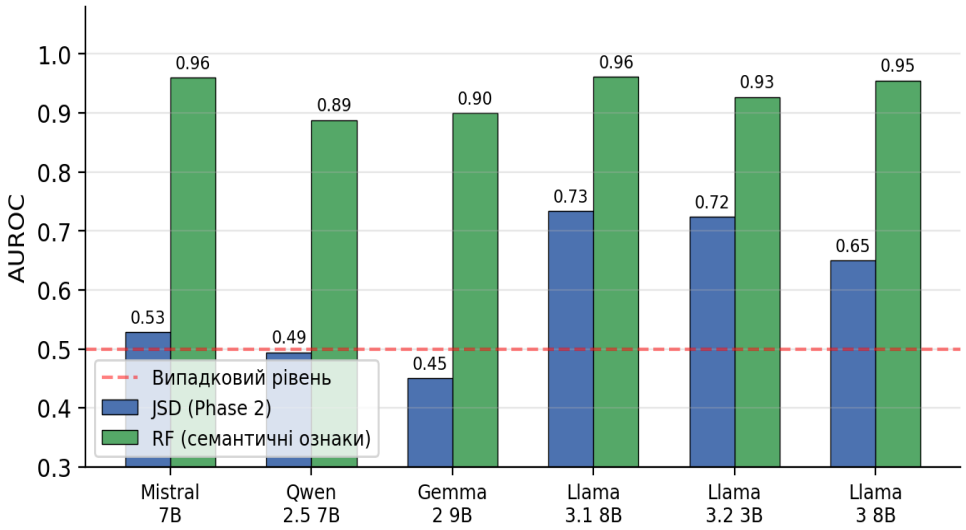


Рисунок 2. *Порівняння AUROC: JSD окремо vs мультиознаковий RF класифікатор*

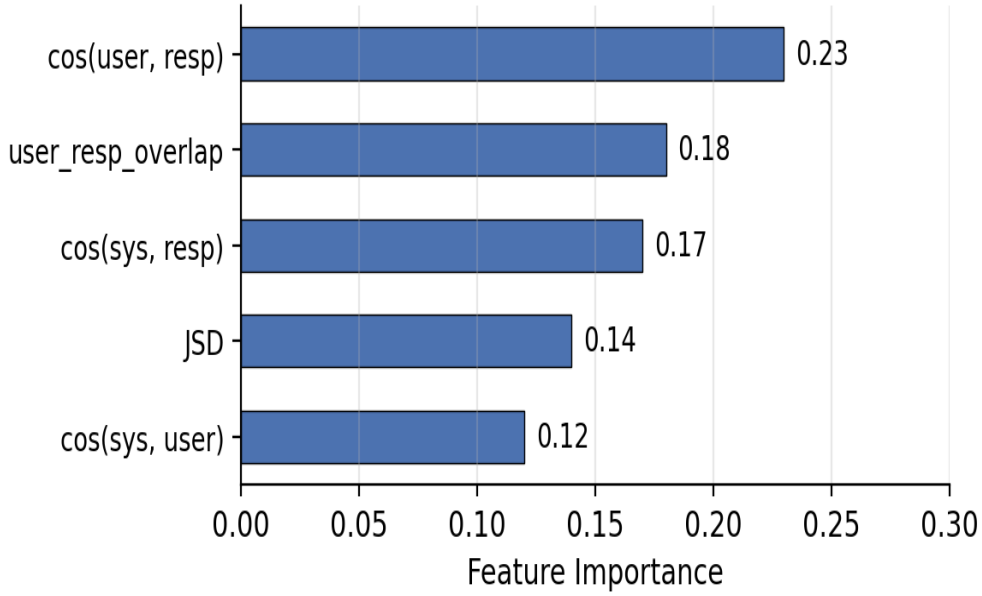


Рисунок 3. *Важливість семантичних ознак у RF класифікаторі*

На контрольній підмножині з вирівняною довжиною (40 ін'єкцій vs 40 легітимних, довжина 52 vs 39 символів) RF досягає AUROC 0.895, що підтверджує релевантність підходу.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Дослідження на 6 моделях LLM показало, що окремі метрики семантичної дивергенції мають обмежену ефективність для детекції prompt-ін'єкцій (найкраща — JSD з AUROC 0.694 на контрольованому датасеті). Мультиознаковий класифікатор, побудований на основі

вектора ознак формули (3), досягає AUROC 0.932 (0.895 на підмножині з контрольованою довжиною). Найсильніша ознака — косинусна подібність за формулою (2) між промптом користувача та відповіддю (importance 0.23). Це узгоджується з Алахмаді та ін. [7] (AUROC 0.764), причому наш вищий результат пояснюється використанням TF-IDF. Отримані результати доповнюють архітектурні підходи до безпеки агентних систем [4, 5, 6], пропонуючи конкретний механізм детекції на рівні окремих запитів.

Виявлена зворотна кореляція ASR–детектованість має практичне значення: найбільш стійкі моделі одночасно є найбільш «прозорими» для семантичного аналізу. Слід зазначити обмеження дослідження: (1) датасет створено для контрольованого експерименту, що може вносити систематичне зміщення; (2) тестування проведено на моделях до 9B параметрів — поведінка більших моделей може відрізнятися; (3) не досліджено адаптивні атаки, спеціально спрямовані на обхід семантичного аналізу. Перспективи подальших досліджень включають: тестування на адаптивних атаках, використання sentence-level ембедінгів для реалізації повної методики Гальперіна [8], розширення датасету реальними прикладами ін’єкцій та верифікацію на моделях більшого масштабу.

ДЖЕРЕЛА

1. Perez, F., Ribas, I. (2022). HackAPrompt: Exposing Systemic Weaknesses of LLMs. arXiv:2311.16119.
2. Greshake, K. et al. (2023). Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. arXiv:2302.12173.
3. SailPoint Security Report (2025). https://investor.sailpoint.com/node/7016/pdf
4. Syros, A. et al. (2025). SAGA: A Security Architecture for Governing Agentic AI Systems. arXiv:2504.21034.
5. Raza, F. et al. (2025). TRiSM for Agentic AI. arXiv:2506.04133.
6. Narajala, A., Narayan, A. (2025). Securing Agentic AI: A Comprehensive Threat Model. arXiv:2504.19956.
7. Alahmadi, B. et al. (2024). Embedding-based classifiers can detect prompt injection attacks. arXiv:2410.22284.
8. Halperin, I. (2025). Prompt-Response Semantic Divergence Metrics for LLMs. arXiv:2508.10192.
9. PayloadsAllTheThings (2024). Prompt Injection Techniques. GitHub. https://github.com/swisskyrepo/PayloadsAllTheThings
10. Liu, Y. et al. (2024). Formalizing and Benchmarking Prompt Injection Attacks. USENIX Security Symposium.



ВОЛОДИМИР АХРАМОВИЧ
Київський авіаційний інститут, Київ, Україна
ORCID: 0000-0002-0086-9131
E-mail: 12zstzi@gmail.com
Професор, доктор технічних наук. Напрямок наукових досліджень: кібербезпека, захист інформації, агентні системи штучного інтелекту.



ВОЛОДИМИР САНЧЕНКО
Київський авіаційний інститут, Київ, Україна
ORCID: 0009-0009-3967-9683
E-mail: volodymyr.sanchenko@gmail.com
Аспірант. Напрямок наукових досліджень: кібербезпека агентних систем штучного інтелекту, виявлення prompt-ін’єкцій у великих мовних моделях

ВПЛИВ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ IT-КОНСАЛТИНГУ В УКРАЇНІ ТА В СВІТІ

Єлизавета Бабенко, Валентина Бабенко, Костянтин Бабенко

Анотація. *В даній тезі досліджено та розглянуто теоретичну і практичну складову впливу технологічного процесу штучного інтелекту в сфері консалтингу в Україні та в світі. З тенденцією розвитку впроваджень різних технологічних рішень, одним з них консалтинг сприяв змінам. Здійснено порівняльний аналіз технологічних процесів штучного інтелекту в сфері IT-консалтингу між Україною та зарубіжними країнами.*

Ключові слова: IT-консалтинг, штучний інтелект, інформаційні технології.

I. ВСТУП

Інноваційні підходи до формування сфери консалтингу в різних країнах розвивається завдяки зовнішнім та внутрішнім факторам, які змінюють звичайні процеси суспільної діяльності. З такими підходами сфера консалтингу розвинулася з різних напрямків створюючи нові сектори взаємодії. Одне з них сприяло виникненню IT-консалтингу, який продовжує розвиватися та вдосконалюватися при впроваджені різних IT технологій. Штучний інтелект, як один з технологічних рішень, які збільшили спектр можливостей в сфері консалтингу.

Однак, можливості такого впровадження має суперечливі моменти такого впровадження, які стверджують про наявність проблематики та сприяли технологічним процесам впровадження штучного інтелекту в сферу консалтингу. Підтвердження цього спостерігається і в інших сферах діяльності.

II. ДАНІ ТА МЕТОДИ

Обрані дані та методики задіяні для формування дослідження, які зазначають важливість тематики, демонструючи проблематику та враховують особливості: документація та дослідження в сфері інформаційних технологій та консалтингу, а саме наукові праці, щодо опису технічної складової технології та її особливості з практичного впровадження; інші дослідження (практичні кейси, статистика та публічні медіа дані), які мають дотичні елементи проаналізованого об’єкту.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Результати дослідження демонструють виклики та проблематику сьогодення, які впливають на сферу консалтингу в Україні та в світі через впровадження технологічних рішень. Консалтинг неоднозначний термін, який на базисі розуміється, як послуга з передачі інформації, яку варто поділити на такі види послуг:

1) Теоретичні: аудит, планування, моніторинг.
2) Практичні розробка, тестування, перенесення інфраструктури.

Такий розподіл послуг аргументується особливістю консалтингу, в якому сформований різний спектр діяльності залежно від напрямку. Технологія, як ключовий об’єкт дослідження сприяє змінам звичайних процесів, які можуть впливати як з позитивної так і з негативної сторони. Базисні IT технології вже залучені до звичайних процесів діяльності (наприклад хмарні сховища, системи безпеки, тощо). Однак головним викликом такого впливу технологічного впровадження може сприяти на сторону щодо таких принципів: прозорість, відкритість, доступність та безпека даних [1].

Сьогоденна статистика демонструє зростання інтеграції, залучаючи до консалтингу більше можливостей та пропозицій для вирішення питань підприємств, компаній чи установ. Наразі в Україні консалтингова сфера розвиває IT-консалтинг займає головний сегмент діяльності та впровадив багато складових IT-рішень для поліпшення різних напрямків (наприклад військова сфера є найбільшою галузь в якій застосовується IT-консалтинг). Зарубіжні країни IT-консалтинг розвивають в сторону часткового впровадження штучного інтелекту через етичні норми встановлені законодавствами [2, с.294 –295].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отже, вплив технологічних процесів штучного інтелекту в сфері IT-консалтингу є глобальним впровадженням, який потягне за собою можливі наслідки. IT-консалтинг складається з багатьох елементів, пов’язаних з хмарним сховищем, даними та штучним інтелектом, тощо. Орієнтовано багато дослідників прогнозують зростання використання технологій на які націлені переважна більшість людей через поліпшення автоматизації. Однак насправді вагомих досліджень, які зможуть проаналізувати безпечність такого впливу не достатньо. Вони не здійснювали аналізу реальних викликів на які спрямовані сьогоденні реалії особливо в сфері IT-консалтингу.

Також, аналізуючи дослідження, було встановлено, що Україна розвиває IT-консалтинг в сторону активного задіювання з військовою тематикою в порівняні з зарубіжними країнами, які намагаються його обмежити та встановити рамки його використання.

ДЖЕРЕЛА

1. Siddhartha P.T. The implications of artificial intelligence in management consulting: A risk and barrier assessment. Multidiscplinary Reviews. 2025. DOI: https://doi.org/10.31893/multirev.2025244

2. Притула І. Інноваційний підхід до зменшення когнітивних помилок в експертному оцінюванні. Social Development and Security. 2024. Vol. 15. №1. DOI: https://doi.org/10.33445/sds.2025.15.1.16



ЄЛИЗАВЕТА БАБЕНКО
здобувач 2 курсу магістерського рівня спеціальності міжнародного права, кафедри Міжнародного та галузевих правових дисциплін, Національної академії наук України Київського університету права, Київ, Україна
ORCID: 0009-0009-6444-7331
E-mail: liza.b2402@gmail.com
Серед наукового інтересу є поєднання трьох напрямків в науковій сфері діяльності: комп’ютерних технології, сучасного права та дизайну.



ВАЛЕНТИНА БАБЕНКО
магістр права, заступник директора з правових питань ТОВ «ЛІЗБРОК»
ORCID: 0000-0001-9726-152X
E-mail: valy19@bigmir.net
Серед наукового інтересу є: поєднання комп’ютерних технологій та сучасного права.



КОСТЯНТИН БАБЕНКО
студент 4 курсу бакалаврського рівня інформаційної бібліотечної та архівної справи в Державному університеті інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0002-5672-131X
E-mail: kostiantyn.mb@gmail.com
Серед наукового інтересу є дослідження застосування інформаційних технологій в сфері архівної справи.

ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ УПРАВЛІННЯ ЗАПАСАМИ БУДІВЕЛЬНИХ МАТЕРІАЛІВ У БАГАТОПРОЄКТНОМУ СЕРЕДОВИЩІ НА ОСНОВІ MILP-МОДЕЛІ

Владислав Балабась, Олена Федусенко

Анотація. *У роботі представлено архітектуру та результати впровадження інтелектуального модуля для оптимізації управління запасами у багатопроєктному будівельному середовищі. Для вирішення поставленої задачі авторами розроблена модель змішаного цілочисельного лінійного програмування (MILP). Інтелектуальний модуль базується на трирівневій архітектурі, що забезпечує інтелектуальну агрегацію даних, аналітичне моделювання методом Branch-and-Cut та автоматизовану генерацію стратегій закупівель. Експериментальна апробація підтвердила перевагу інтелектуального підходу над традиційними методами: у сценаріях з дефіцитом бюджету досягнуто підвищення рівня покриття потреб до 99,1% (проти 87,3% у базовому сценарії) та зниження загальних витрат на 14%. Результати дослідження мають потенціал для інтеграції в сучасні ERP-системи як інструмент підтримки прийняття рішень у реальному часі.*

Ключові слова: інтелектуальний модуль, управління запасами, MILP-модель, оптимізація закупівель, прийняття рішень.

I. ВСТУП

Управління запасами будівельних матеріалів становить одну з ключових проблем будівельних компаній, оскільки матеріали складають 50–60 % загальної вартості проєкту. Неефективне планування закупівель призводить до простоїв, перевитрат або заморожування коштів на складах [1], [2]. Будівельна галузь характеризується високою невизначеністю, сезонністю робіт та багаторівневими ланцюгами постачання [3], [4]. Сучасні підходи вимагають комплексного врахування потреб кількох паралельних проєктів, обмежень постачальників, наявних складських запасів та коливань цін що перетворює задачу управління логістикою на багатофакторну проблему, розв’язання якої традиційними методами стає складним через експоненціальне зростання комбінаторної складності. Це зумовлює необхідність впровадження інтелектуального модуля, здатного до оперативного аналізу великих масивів даних та знаходження глобального оптимуму в режимі реального часу

Метою роботи є розробка інтелектуального програмного модуля, який на основі оптимізаційних алгоритмів формує план закупівель, мінімізує сумарні витрати та забезпечує максимальне задоволення потреб проєктів.

Об’єктом дослідження є процес управління запасами в багатопроєктному будівельному середовищі, а предметом – моделі змішаного цілочисельного лінійного програмування (MILP).

II. ДАНІ ТА МЕТОДИ

Для побудови моделі оптимізації закупівель та проведення експериментальних досліджень сформовано багатовимірний простір структурованих даних, що відображають ключові аспекти логістичної діяльності будівельної компанії. Інтелектуальне ядро модуля оперує синтетично згенерованими, проте верифікованими на відповідність реальним ринковим умовам даними, що включають: 20 незалежних постачальників із варіативними логістичними потужностями, 20 категорій будівельних матеріалів (від базових сумішей до складних металоконструкцій) та 10 паралельних будівельних проєктів. Кожен проєкт

характеризується унікальним вектором пріоритетності та специфікою етапів виконання робіт, що дозволяє алгоритму виконувати динамічне ранжування потреб та оптимізувати розподіл ресурсів у мовах дефіциту чи обмеженого бюджету.

Попередня обробка даних включала контроль узгодженості таблиць та генерацію реалістичних коливань цін [5].

Для забезпечення формальної постановки задачі в рамках вибраного підходу застосовується модель змішаного лінійного програмування, яка відображає залежність між потребами будівельних проєктів, наявними складськими запасами та можливостями постачальників.

Нижче наведено базову математичну модель, що використовується як основа для подальшої розробки інтелектуального модуля оптимізації закупівель.

- $i \in I$– матеріали,
- $j \in J$– проєкти,
- $k \in K$– постачальники.

Змінні:

- x_{ikj} – кількість матеріалу i, закуплена у постачальника k для проєкту j,
- s_i– залишок матеріалу iна складі,
- d_i– дефіцит матеріалу i.

Цільова функція мінімізує сумарні витрати:

$$\min \sum_{i,k,j} c_{ik} \cdot x_{ikj} + \sum_i h_i \cdot s_i, \quad (1)$$

де c_{ik}– ефективна ціна (з урахуванням можливих коливань), h_i – вартість зберігання.

Виокремимо основні обмеження моделі:

1. Повне забезпечення потреб проєктів:
2. Обмеження складських запасів.
3. Обмеження потужності постачальників.
4. Бюджетне обмеження.
5. Невід’ємність змінних.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

В основу інтелектуального модуля покладено трирівневу архітектуру, яка дозволяє чітко розділити функції системи: роботу з даними, логіку прийняття рішень та формування підсумкових планів. Така побудова забезпечує автономність кожного етапу — від збору інформації до вибору оптимального сценарію закупівель. Структура модуля включає три основні рівні:

- Рівень інтелектуальної агрегації даних, що відповідає за збір та узгодження багатовимірних масивів інформації про ресурси, постачальників та пріоритетність будівельних об'єктів.
- Аналітичне ядро, де формується математична MILP-модель. Вона враховує систему жорстких та м'яких обмежень, а процес оптимізації базується на інтелектуальних алгоритмах пошуку глобального оптимуму для вирішення задач високої комбінаторної складності.
- Рівень стратегічного планування, який забезпечує верифікацію отриманих сценаріїв та автоматизовану генерацію планів закупівель, адаптованих до динамічних бюджетних лімітів.

Така побудова дозволяє модулю функціонувати як автономна ланка системи підтримки прийняття рішень, що мінімізує вплив людського фактора на складні логістичні процеси.

Експериментальне дослідження ефективності запропонованої у інтелектуальному модулі моделі оптимізації управління запасами проводилося шляхом порівняльного аналізу результатів дворівневого моделювання. На першому етапі реалізовано базовий сценарій, що імітує традиційне планування за принципом «мін-макс» із пріоритетом найнижчої ціни, а на другому етапі застосовано розроблена MILP-модель із використанням методу Branch-and-Cut [6], [7]. Процес валідації передбачав оцінку здатності моделі до інтелектуальної декомпозиції складних замовлень з урахуванням пріоритетності проєктів, лімітів постачальників та динаміки складських залишків. Фінальна верифікація результатів базувалася на зіставленні інтегральних показників загальних витрат та коефіцієнта покриття дефіциту ресурсів, що дозволило кількісно оцінити переваги інтелектуальної оптимізації над евристичними методами. Для отримання кількісних оцінок у варіативних ринкових умовах, експериментальна апробація розробленого інтелектуального модуля здійснювалася у двох стратегічних режимах: за умов необмеженого фінансування та при суворому ліміті бюджету у 900 000 грн із врахуванням 25% ймовірності коливання ринкових цін.

У першому сценарії (необмежений бюджет) застосування MILP-моделі дозволило досягти 100% задоволення потреб усіх десяти проєктів, скоротивши при цьому загальні витрати на 14% порівняно з базовим евристичним методом. Аналіз показав, що середня економія на кожній одиниці ресурсу склала 11 грн, що було досягнуто завдяки здатності алгоритму знаходити приховані комбінації найбільш вигідних постачальників для дороговартісних позицій, таких як арматура та металочерепиця.

Особливу ефективність інтелектуальний підхід продемонстрував у другому сценарії (дефіцит ресурсів). Як свідчать дані Таблиці 1, за умови жорсткого бюджетного обмеження модель забезпечила критично вищий рівень покриття потреб — 99,1% проти 87,3% у базовому сценарії. Це стало можливим завдяки динамічному перерозподілу коштів на користь пріоритетних об'єктів та інтелектуальному вибору альтернативних джерел постачання з нижчою середньою ціною (128,4 грн проти 142,6 грн).

Таблиця 1. *Порівняння сценаріїв (бюджет 900 000 грн)*

Сценарій	**Загальні витрати, грн**	**Покриття потреб, %**	**Середня ціна, грн/од.**
Базовий	892 450	87,3	142,6
MILP-оптимізація	899 870	99,1	128,4

Результати підтверджують, що інтелектуальний модуль не просто механічно розподіляє кошти, а виконує глибоку оптимізацію структури закупівель, забезпечуючи стійкість логістичних процесів навіть за несприятливих фінансових умов

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати підтверджують суттєві переваги інтелектуального модуля на основі MILP-підходу над традиційними методами планування закупівель. На відміну від інтуїтивних підходів, розроблена модель забезпечує багатофакторну оптимізацію, враховуючи множину реальних обмежень та пріоритетність проєктів у режимі реального часу. Розроблений модуль має високий потенціал для інтеграції в сучасні ERP-системи та цифрові платформи управління будівельними проєктами.

Перспективи подальших досліджень полягають у розширенні інтелектуальних можливостей модуля через додавання стохастичних елементів (прогнозування невизначеності постачання), врахування складної транспортної логістики та розробку алгоритмів динамічного перепланування при виникненні непередбачуваних критичних подій. Таким чином, перехід до використання методів математичного програмування та штучного інтелекту є ключовим чинником підвищення економічної ефективності та цифрової трансформації будівельної галузі.

ДЖЕРЕЛА

1. Studer W. P., de Brito Mello L. C. Core Elements Underlying Supply Chain Management in the Construction Industry: A Systematic Literature Review. Buildings, 2021, 11(12), 569.
2. Kamil M. I. Developing Construction Project Material Procurement Strategies. European Journal of Business and Management Research, 2025, 10(1).
3. Polusmiak Y. Project management in the construction industry: identifying logistics problems and ways to optimize them. Management-Journal, 2024.
4. IJRR Journal. Supply Chain Management in Construction Projects: A review. Vol.11, Issue 1, 2024.
5. Pagare P. G., Sonawane A. R. Literature Review on Inventory and Material Management in Construction Industries. International Journal of Research in Technology and Innovation, 2022, 7(5).
6. Alnahhal M. Economic Order Quantity: A State-of-the-Art in the Era of Digitalization. Sustainability, 2024, 16(14), 5965.
7. Vicente J. J. et al. Optimizing Supply Chain Inventory: A Mixed-Integer Linear Programming Approach. Systems, 2025, 13(1), 33.



ВЛАДИСЛАВ БАЛАБАСЬ
Студент АнД-41, кафедра інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна, Київ, Україна
E-mail: vladilsavbalabas@knu.ua
Проходжу навчання на 4 курсі. До наукових інтересів належать еволюційні обчислення, інтелектуальний аналіз даних та навчання нейромереж.



ОЛЕНА ФЕДУСЕНКО
Доцент, кафедра інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна, Київ, Україна
ORCID: 0000-0002-5782-5922
E-mail: fedusenko@knu.ua
Отримала ступінь кандидата технічних наук у галузі інформаційних технологій у 2006 році. Є автором понад 70 наукових праць. До наукових інтересів належать системи адаптивного навчання, генетичні алгоритми та їх прикладне застосування, методи Data Mining.

СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ БАГАТОАГЕНТНИХ АРХІТЕКТУР У ДИНАМІЧНИХ СОЦІОТЕХНІЧНИХ СЕРЕДОВИЩАХ

Едуард Бовда, Юрій Самохвалов

Анотація. *Розглядається клас систем підтримки прийняття рішень, орієнтованих на функціонування у динамічних, розподілених та невизначених соціотехнічних середовищах. Запропоновано узагальнений підхід до побудови архітектури систем підтримки прийняття рішень на основі багаторівневих баз знань, експертних механізмів виведення та багатоагентних моделей координації. Обґрунтовано вимоги до формалізації, експертування та актуалізації знань у системах управління складними об'єктами. Показано, що поєднання онтологічних моделей, продукційних правил і багатоагентних алгоритмів дозволяє підвищити адаптивність, стійкість та інтерпретованість рішень у середовищах з високою динамікою та інформаційною невизначеністю. Реалізація запропонованого підходу забезпечить перехід від простої обробки даних до інтелектуального управління знаннями, що дозволить мінімізувати ризики помилкових управлінських дій та скоротити час реакції на критичні зміни стану складних об'єктів.*

Ключові слова: системи підтримки прийняття рішень, база знань, експертні системи, багатоагентні системи, динамічні середовища.

I. ВСТУП

Системи підтримки прийняття рішень (СППР) є ключовим інструментом підтримки управлінських процесів у складних системах, що характеризуються високою динамікою, розподіленістю та невизначеністю інформації. До таких систем належать об'єкти критичної інфраструктури, транспортні та енергетичні мережі, цифрові платформи, кіберфізичні системи та організаційно-економічні структури.

На відміну від класичних інформаційних систем, СППР виконують не лише функції збору та обробки даних, але й забезпечують семантичне узагальнення інформації, формування альтернатив рішень, оцінювання ризиків і прогнозування наслідків прийнятих рішень. Це зумовлює необхідність інтеграції методів інженерії знань, експертних систем і багатоагентних підходів. На сьогодні СППР використовуються для: аналізу великих масивів даних; оптимізації логістики; управління енергетичними та транспортними мережами; реагування на надзвичайні ситуації; забезпечення кібербезпеки, тощо.

II. ОСНОВНІ ПОЛОЖЕННЯ ТА ПІДХОДИ

Аналіз сучасних досліджень у галузі СППР [1, 2] свідчить, що системи з централізованими архітектурами мають обмежену ефективність у динамічних середовищах, де відбуваються швидкі зміни стану системи та окремих її компонентів і фрагментація інформаційного простору. Тому побудова розподілених, адаптивних СППР є актуальною задачею.

В доповіді розглядається підхід до побудови систем підтримки прийняття рішень на основі багаторівневих баз знань, експертних механізмів виведення та багатоагентних архітектур, адаптованих до динамічних соціотехнічних середовищ.

Застосування багатоагентних підходів зумовлене зростанням складності соціотехнічних систем та розподіленим характером інформаційних ресурсів. У таких умовах централізовані моделі прийняття рішень демонструють обмежену масштабованість і знижену стійкість до відмов.

Багатоагентні системи дозволяють розподілити процес аналізу між автономними інтелектуальними компонентами, що взаємодіють на основі механізмів кооперації та консенсусу. Це забезпечує: локальне прийняття рішень із урахуванням контексту; підвищення достовірності колективного вибору; зменшення ризику маніпуляції рішеннями; підтримку відкритих систем із змінною кількістю агентів.

Консенсусні алгоритми в багатоагентних системах спрямовані на вибір рішення, яке є логічним, безпечним і ефективним навіть за наявності різних позицій агентів.

Багатоагентна архітектура СППР передбачає представлення окремих підсистем, сервісів або функціональних модулів у вигляді автономних агентів, кожен з яких володіє локальною частиною знань і механізмами прийняття рішень. Агенти взаємодіють за допомогою механізмів узгодження, переговорів і колективного вибору, що дозволяє зменшити затримки прийняття рішень, підвищити стійкість системи до відмов та реалізувати самоорганізацію та адаптацію. Рисунок 1 ілюструє структуру багатоагентної СППР.

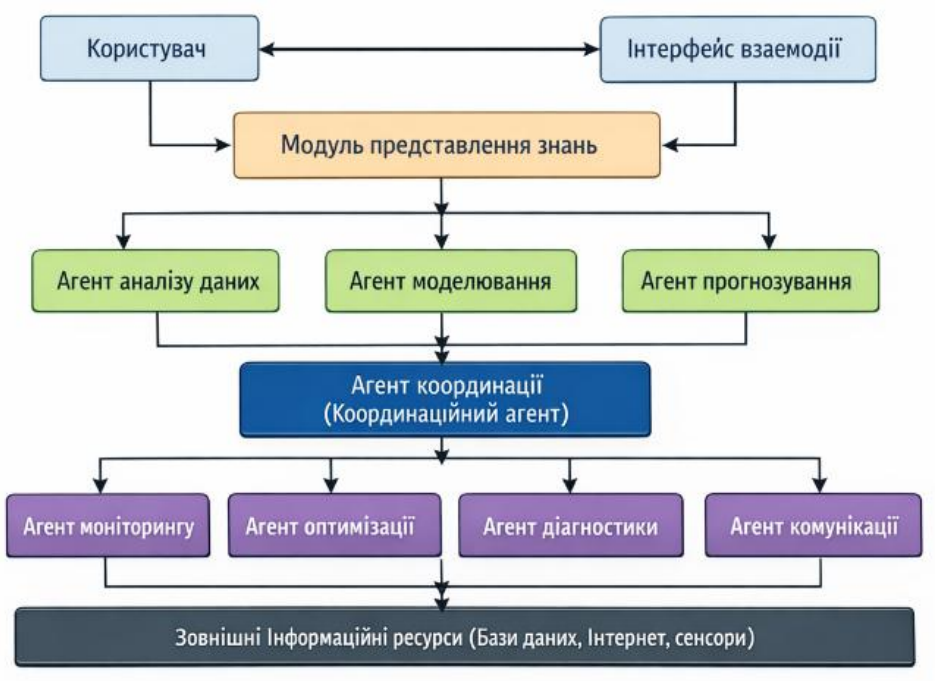


Рисунок 1. *Структура багатоагентної СППР*

Структура багатоагентної СППР реалізує принципи розподіленого інтелекту, модульності та адаптивності, що забезпечує ефективну обробку складних слабкоформалізованих задач управління. Архітектура організована у вигляді ієрархічно-мережевої взаємодії агентів, об’єднаних спільним середовищем знань і механізмами координації.

На верхньому рівні функціонує підсистема взаємодії з користувачем, яка забезпечує когнітивно-ергономічний доступ до сервісів СППР, підтримує формалізацію управлінських запитів та інтерпретацію отриманих рекомендацій. Центральним компонентом архітектури є модуль представлення знань, що виконує роль семантичного ядра системи. Він інтегрує онтологічні моделі предметної області, продукційні правила та формалізовані залежності, забезпечуючи онтологічно-кероване виведення, інтероперабельність даних і контекстну узгодженість агентних рішень.

Аналітико-моделювальний контур представлений спеціалізованими інтелектуальними агентами аналізу даних, моделювання та прогнозування. Їх функціонування спрямоване на трансформацію первинних даних у знання, генерацію сценаріїв розвитку ситуацій та

оцінювання можливих наслідків управлінських впливів. Використання агентної парадигми дозволяє реалізувати паралельну обробку інформації та підвищити масштабованість системи.

Координаційний агент виступає метарівнем управління багатоагентним середовищем, реалізуючи механізми динамічного розподілу задач, протоколи переговорів, агрегування часткових результатів та розв'язання конфліктів міжсторонніх рекомендацій. Такий підхід забезпечує цілісність процесу підтримки рішень і сприяє формуванню узгоджених управлінських альтернатив.

Операційний рівень включає агентів моніторингу, оптимізації, діагностики та комунікації, які забезпечують безперервне спостереження за станом об'єкта управління, багатокритеріальне оцінювання альтернатив, виявлення причинно-наслідкових зв'язків відхилень та інтеграцію із зовнішніми інформаційними сервісами.

Фундаментом функціонування СППР є зовнішні інформаційні ресурси – бази даних, сенсорні системи та мережеві джерела, що формують актуальний інформаційний простір для агентної взаємодії. У цілому запропонована структура забезпечує проактивний характер підтримки прийняття рішень, підвищує обґрунтованість управлінських дій та створює передумови для побудови інтелектуальних адаптивних систем нового покоління.

В основі багатоагентної СППР лежить модель динамічного середовища з урахуванням невизначеності та подійності; принципи побудови та актуалізації баз знань СППР; верифікація та експертиза знань; формування рекомендацій.

Динамічне середовище розглядається як відкрита система, стан якої описується трійкою:

$$(\boldsymbol{S}, \boldsymbol{E}, \boldsymbol{U}), \tag{1}$$

де $\boldsymbol{S}$ – множина можливих станів системи; $\boldsymbol{E}$ – множина подій, що ініціюють переходи між станами; $\boldsymbol{U}$ – множина факторів невизначеності, пов'язаних з неповнотою, затримкою та суперечливістю інформації.

У такому середовищі СППР повинна забезпечувати безперервне оновлення знань, динамічне перепланування та контекстно-залежне формування рекомендацій.

У таких системах запропонованій системі підтримки прийняття рішень інформаційний простір доцільно подати у вигляді інтегрованої структури:

$$IS = (DB, KB, M, R), \tag{2}$$

де: DB (Data Base) – база даних; KB (Knowledge Base) – база знань; M – множина механізмів виведення; R – множина сформованих рекомендацій.

У запропонованому підході бази даних і бази знань розглядаються як логічно та функціонально розділені, але інтегровані компоненти СППР. Бази даних забезпечують зберігання структурованих фактів, тоді як бази знань реалізують семантичний рівень обробки інформації. База даних відповідає на запитання **"що відбувається?"**, тоді як база знань – **"що це означає і яке рішення доцільне?"**. Їх інтеграція забезпечує перехід від data-driven до knowledge-driven прийняття рішень.

Бази знань включають: онтологічний рівень (поняття, зв'язки, обмеження); рівень продукційних і сценарних правил; рівень моделей невизначеності (ймовірнісні, нечіткі); метазнання щодо довіри, актуальності та контексту застосування правил. Запропоновано багаторівневу організацію баз знань, що поєднує локальні модулі знань з глобальними узагальненими представленнями.

Процес семантичної інтерпретації можна подати як відображення:

$$\phi: DB \to KB, \tag{3}$$

де функція ϕ перетворює факти на знання шляхом: узагальнення, класифікації, встановлення причинно-наслідкових зв'язків.

Базу даних визначимо як скінченну множину структурованих фактів:

$$DB = \{f_i | f_i = (a_1, a_2, \dots a_n)\}, \quad (4)$$

де f_i – запис (факт), a_j – атрибути предметної області.

З урахуванням динаміки середовища базу даних можна представити:

$$DB(t) = DB(t-1) \cup \Delta DB(t), \quad (5)$$

де $\Delta DB(t)$ – множина нових або оновлених даних.

Базу знань представимо як багаторівневу структуру:

$$KB = (O, P, U, C, Meta), \quad (6)$$

де: *O* (Ontology) – множина понять і відношень: *O*=(*C, Rel, Axioms*);

P (Production rules) – правила виду: *IF* Cond→*THEN* Act;

U (Uncertainty models) – моделі невизначеності: *U*={*Pr, Fz, Bel*} (ймовірнісні, нечіткі, довірчі);

C (Context) – контекст застосування знань;

Meta – метазнання (актуальність, достовірність, рівень довіри).

Формування рекомендацій в СППР доцільно реалізовувати як багатокомпонентний процес, що поєднує логічне, ймовірнісне та аналітичне виведення.

Процес отримання рекомендацій:

$$r^* = \arg\max(U|r, KB, S) \text{при } r \in A, \quad (7)$$

де: *A* – множина допустимих альтернатив,

U(r) – функція корисності рішення ("якість" рішення),

KB – база знань,

S – стан системи,

r – варіант рішення,

r^* – раціональний вибір, що забезпечує найкраще очікуване значення цільової функції.

Для експертування знань використовуються: продукційні та онтологічні методи; колективне експертне оцінювання; автоматизований аналіз журналів подій і логів систем; механізми зворотного зв'язку за результатами прийнятих рішень.

Запропоновано такі механізми інтелектуального виведення та підтримки прийняття рішень:

- **онтологічно-кероване виведення**, яке забезпечує семантичну узгодженість рішень і врахування доменних обмежень;
- **правило-орієнтоване виведення**, засноване на продукційних моделях;
- **багатокритеріальне оцінювання альтернатив**, що дозволяє ранжувати варіанти рішень відповідно до заданих критеріїв;
- **прогностичні моделі**, спрямовані на оцінювання можливих наслідків управлінських дій;
- **адаптивні рекомендаційні модулі**, які уточнюють правила на основі зворотного зв'язку.

Таким чином, запропонований підхід побудови розподілених СППР базується на інтеграції багатоагентних архітектур із багаторівневими онтологічно-керованими базами знань.

III. ВИСНОВКИ

Ефективне управління сучасними складними системами потребує переходу від класичних централізованих архітектур до розподілених інтелектуальних моделей. Інтеграція багатоагентних систем дозволяє реалізувати паралельну обробку інформації та забезпечити автономність окремих функціональних вузлів, що є важливим для об'єктів критичної інфраструктури. Ключовим елементом запропонованого підходу є багаторівнева база знань, яка поєднує онтологічний аналіз, продукційні правила та моделі невизначеності. Це дозволяє системі здійснювати не лише збір даних, а й проводити їх глибоку семантичну інтерпретацію, трансформуючи первинні факти у придатні для використання управлінські знання. Координація взаємодії агентів забезпечує цілісність процесу підтримки рішень навіть за наявності суперечливих даних або фрагментації інформаційного простору. Сформована математична модель динамічного середовища дозволяє враховувати фактори ризику та часові затримки, що підвищує адекватність прогностичних сценаріїв. Таким чином, запропонована архітектура створює фундамент для побудови проактивних систем у галузях управління критичною інфраструктурою, транспортом, енергетикою, цифровими сервісами, кібербезпекою та кризовим менеджментом, здатних до самоорганізації в умовах високої динаміки. В цілому, розглянутий підхід дозволить підвищити живучість та відмовостійкість, масштабованість та адаптивність, якість та обґрунтованість рішень, що приймаються, об'єктивність рекомендованих альтернатив, оптимізацію часових ресурсів СППР.

ДЖЕРЕЛА

1. Tupayachi, J., Xu, H., Omitaomu, O. A., Camur, M. C., Sharmin, A., & Li, X. (2024). Towards next-generation urban decision support systems through AI-powered construction of scientific ontology using large language models—A case in optimizing intermodal freight transportation. Smart Cities, 7(5), 2392–2421. https://doi.org/10.3390/smartcities7050094.
2. Nozari, H., & Szmelter-Jarosz, A. (2026). Quantitative decision making in reverse logistics with a hybrid decision support system integrating agentic AI and evolutionary optimization. Euro-Mediterranean Journal for Environmental Integration, 11, Article 30. https://doi.org/10.1007/s41207-025-00989-7.



ЕДУАРД БОВДА
к.т.н., доцент, професор кафедри комп'ютерних наук та інтелектуальних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.
ORCID: 0000-0002-8267-2120
E-mail: edepig8305@ukr.net
Наукові інтереси: інформаційні технології, системи підтримки прийняття рішень, інфокомунікаційні системи.



ЮРІЙ САМОХВАЛОВ
д.т.н., професор, професор кафедри інтелектуальних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0001-5123-1288
E-mail: yu1953@ukr.net
Наукові інтереси: нечітке моделювання когнітивних процесів, логіко-лінгвістичне моделювання, прийняття рішень в умовах невизначеності.

МЕХАНІЗМИ УВАГИ В ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖАХ ДЛЯ ПРОГНОЗУВАННЯ КОРОТКОСТРОКОВОЇ ВОЛАТИЛЬНОСТІ ФІНАНСОВИХ РИНКІВ

Олексій Вовченко, Микола Костіков

Анотація. *Досліджено застосування механізмів уваги в глибоких нейронних мережах для прогнозування короткострокової волатильності на фінансових ринках. Запропоновано гібридну архітектуру, що поєднує шари LSTM з багатоголовою увагою, що дозволяє моделі динамічно ідентифікувати та зважувати відповідні історичні закономірності на основі поточних ринкових умов. Механізм уваги забезпечує інтерпретованість, виділяючи, які минулі періоди часу найбільше впливають на прогнози волатильності. Експериментальна оцінка даних високочастотної торгівлі демонструє покращення точності прогнозування порівняно з традиційними моделями сімейства GARCH, особливо в періоди змін ринкового режиму.*

Ключові слова: глибоке навчання, машинне навчання, нейронні мережі, прогнозування

I. ВСТУП

Прогнозування волатильності фінансових ринків є важливим завданням для управління ризиками, оцінки деривативів та формування торговельних стратегій. Традиційні економетричні моделі родини GARCH успішно використовуються протягом десятиліть завдяки міцному теоретичному обґрунтуванню та здатності моделювати кластеризацію волатильності. Проте ці підходи демонструють обмеження при прогнозуванні в умовах швидких змін ринкового режиму та наявності складних нелінійних залежностей у даних високої частоти.

II. ДАНІ ТА МЕТОДИ

Глибоке навчання пропонує потужні інструменти для моделювання складних патернів у фінансових часових рядах. LSTM архітектури здатні захоплювати довгострокові залежності, що є важливим для прогнозування волатильності, оскільки минулі шоки можуть впливати на поточну ринкову динаміку протягом тривалих періодів. Однак стандартні LSTM мережі не мають механізму для вибіркового фокусування на найбільш релевантних історичних періодах, що обмежує їхню здатність адаптуватися до змінних ринкових умов [1].

Механізми уваги трансформували підходи до обробки послідовних даних, дозволяючи моделям динамічно визначати важливість різних елементів вхідної послідовності. У контексті фінансового прогнозування механізм уваги може надавати різну вагу історичним спостереженням залежно від поточного ринкового стану. Це особливо цінно для моделювання волатильності, де релевантність минулих подій може змінюватися з часом – наприклад, минулі кризові періоди можуть ставати більш важливими під час поточної турбулентності.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Запропонована гібридна архітектура інтегрує LSTM шари з багатоголовою увагою для прогнозування внутрішньоденної реалізованої волатильності. Перший компонент використовує двошаровий LSTM для кодування історичних цінових рухів та торговельних обсягів у контекстні вектори. Другий компонент застосовує механізм багатоголової уваги до цих векторів, дозволяючи моделі одночасно фокусуватися на різних аспектах історичних

даних. Ключовою інновацією є адаптивний механізм уваги, який враховує поточний ринковий режим. Модель навчається ідентифікувати режими через додатковий класифікатор, який аналізує останні ринкові умови і визначає, чи перебуває ринок у стані високої чи низької волатильності, тренду чи консолідації. Вихід класифікатора використовується для модуляції ваг уваги, дозволяючи моделі адаптувати свій фокус залежно від ринкової ситуації. Особливу увагу приділено інтерпретованості прогнозів. Візуалізація ваг уваги дозволяє аналітикам зрозуміти, які історичні періоди модель вважає найбільш релевантними для поточного прогнозу. Це важливо для практичного застосування, оскільки трейдери та ризик-менеджери потребують не лише точних прогнозів, а й розуміння факторів, що їх обумовлюють.

Планується провести експериментальну оцінку на високочастотних даних провідних фінансових інструментів. Порівняння буде здійснюватися з базовими моделями GARCH, EGARCH та стандартними LSTM без механізмів уваги. Особливий інтерес становить оцінка продуктивності під час періодів значних ринкових потрясінь, коли швидкі зміни режиму вимагають адаптивних прогнозних моделей.

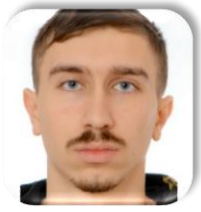
Очікувані результати включають покращення точності короткострокових прогнозів волатильності, особливо в турбулентні періоди, та підвищення інтерпретованості через візуалізацію механізмів уваги. Планується також дослідити можливості розширення підходу для одночасного прогнозування волатильності множини взаємопов'язаних активів, що може бути корисним для управління портфельним ризиком [2].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована архітектура представляє перспективний напрямок інтеграції механізмів уваги в прогнозування фінансових часових рядів, поєднуючи переваги глибокого навчання з можливістю інтерпретації результатів. Подальші дослідження будуть спрямовані на оптимізацію архітектури, дослідження різних типів механізмів уваги та розширення підходу для багатомасштабного прогнозування волатильності.

ДЖЕРЕЛА

1. Fan C., Zhang X. (2024) Stock price nowcasting and forecasting with deep learning, Journal of Intelligent Information Systems, vol. 63, is. 2, 639–656. DOI: 10.1007/s10844-024-00908-2.
2. Kim H. Y., Won C. H. (2018) Forecasting the volatility of stock price index: A hybrid model integrating LSTM with multiple GARCH-type models, Expert Systems with Applications, vol. 103, pp. 25–37. URL : https://doi.org/10.1016/j.eswa.2018.03.002.



ОЛЕКСІЙ ВОВЧЕНКО
аспірант кафедри інформаційних технологій, штучного інтелекту і кібербезпеки Національного університету харчових технологій, Київ, Україна
ORCID: 0009-0006-0990-3515
E-mail: vovchenkoalex0@gmail.com
Отримав ступінь бакалавра (2023) і магістра (2025) у Національному університеті харчових технологій за спеціальністю 122 «Комп'ютерні науки». Наукові інтереси — нейронні мережі; задачі прогнозування; аналіз фінансових ринків.



МИКОЛА КОСТІКОВ
к.т.н., доц., доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-1569-8179
E-mail: Kostikov@knu.ua
Наукові інтереси — комп'ютерна лінгвістика; електронні засоби навчання (зокрема для іноземних мов); робота з API.

МЕТОДИ ОБ'ЄДНАННЯ РЕГІОНІВ ІНТЕРЕСУ ДЛЯ ЕФЕКТИВНОЇ ОБРОБКИ НЕЙРОННИМИ МЕРЕЖАМИ ДОВІЛЬНОГО ФОРМАТУ

Ярослав Гозак, Сергій Палій

Анотація. *У роботі досліджено методи об'єднання регіонів інтересу (ROI) перед їх обробкою нейронною мережею довільного формату. Запропоновано лінійну модель обчислювальної вартості виконання моделі та введено теоретичний поріг злиття τ, що визначає доцільність об'єднання регіонів. Параметри моделі оцінено методом лінійної регресії для різних пристроїв. Показано, що оптимальна стратегія злиття є апаратно-залежною та визначається співвідношенням накладних витрат запуску та питомої вартості обробки пікселя.*

Ключові слова: регіони інтересу, злиття регіонів, лінійна регресія, оптимізація обчислень.

I. ВСТУП

У сучасних системах комп'ютерного зору виконання нейронної мережі для повного зображення є обчислювально затратним. ROI-орієнтований підхід дозволяє запускати модель лише для регіонів інтересу[1-3]. Проте виникає задача оптимального об'єднання ROI перед виконанням моделі.

Надмірна кількість дрібних регіонів збільшує кількість запусків моделі, тоді як агресивне об'єднання збільшує площу вхідних даних та час обробки. Таким чином, необхідний критерій, що дозволяє формально визначити доцільність злиття.

Метою роботи є формалізація задачі злиття ROI через модель обчислювальної вартості та введення апаратно-залежного порогу об'єднання.

II. ДАНІ ТА МЕТОДИ

Експериментально встановлено, що час виконання моделі для ROI площею A наближено описується лінійною залежністю:

$$C(A) = c_t A + K_t, \quad (1)$$

де

c_t — питома вартість обробки одного пікселя (сек/піксель).

K_t — накладні витрати запуску моделі (сек).

Параметри c_tта K_tвизначено методом лінійної регресії (метод найменших квадратів) на основі вимірювань часу обробки ROI різної площі.

З формули 1 випливає критичний поріг площі

$$\tau = \frac{K_t}{c_t}, \quad (2)$$

Параметр τ має розмірність пікселів і визначає площу, для якої накладні витрати запуску дорівнюють вартості обробки цієї площі. Відповідно, якщо приріст площі після злиття менший за τ, об'єднання є доцільним, а якщо більший — злиття збільшує сумарну вартість. Таким чином, τ є апаратно-залежним критерієм прийняття рішення.

Досліджено три підходи.

1. Послідовне злиття - об'єднуються ROI, що перетинаються. Алгоритм має складність $O(N^2)$ та залежить від порядку обходу.

2. Злиття, чутливе до площі - додатково враховується приріст площі після об'єднання. Обмежується надмірне розширення обмежувальних рамок. Складність — $O(N^2)$.

3. Жадібне злиття із урахуванням ціни - на кожному кроці обчислюється виграш за формулою 3:

$$G(r_i, r_j) = C(r_i) + C(r_j) - C(r_{ij}), \quad (3)$$

Об'єднується пара з максимальним додатним виграшем. Процес триває до відсутності позитивного виграшу. Базова складність — $O(N^3)$, після оптимізації — $O(N^2)$.

Алгоритм використовує модель (1) та поріг (2) для прийняття рішень.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Як показано в Таблиці 1, алгоритми відрізняються за обчислювальною складністю та витратами пам'яті.

Таблиця 1. *Порівняння алгоритмів злиття ROI*

Метод	Час алгоритму (с/зобр)	Память(МБ)	Асимптотична складність
Послідовне злиття	0.0015	0.54	$O(N^2)$
Злиття, чутливе до площі	0.0050	0.04	$O(N^2)$
Жадібне злиття із урахуванням ціни	0.0159	0.02	$O(N^3)$ - $O(N^2)$

Послідовне злиття характеризується мінімальними власними витратами часу, однак не враховує зміну обчислювальної вартості після об'єднання регіонів. Площинно-обмежене злиття частково усуває цей недолік шляхом контролю приросту площі, проте також не спирається на формальну модель вартості.

Жадібне злиття з урахуванням вартості використовує модель (1) та критерій (2), що дозволяє безпосередньо мінімізувати сумарний час виконання моделі. Незважаючи на більший власний час роботи алгоритму, зменшення кількості запусків моделі компенсує ці витрати при достатньо великих значеннях порогу τ.

Як показано в Таблиці 2, параметри лінійної моделі суттєво відрізняються для різних пристроїв.

Таблиця 2. *Параметри лінійної цінової моделі та поріг злиття* $\tau = K_t/c_t$

Система	Режим	Пристрій	c_t(сек/піксель)	K_t(сек)	τ(піксель)
А		GPU RTX 3060 Ti 8GB	$6.0 \cdot 10^{-8}$	0.0107	175,112
А		CPU i7-11700K	$1.63 \cdot 10^{-6}$	0.0097	5,996
Б		GPU RTX 3060 12GB	$7.0 \cdot 10^{-8}$	0.0131	185,870
Б		CPU i9-9900KF	$1.70 \cdot 10^{-6}$	0.0111	~7,100
В	Продуктивність	GPU RTX 4050 Laptop	$8.0 \cdot 10^{-8}$	0.0081	96,216
В	Продуктивність	CPU Core 5 210H	$2.16 \cdot 10^{-6}$	0.0103	4,778
В	Енергозбереження	GPU RTX 4050 Laptop	$5.0 \cdot 10^{-8}$	0.0103	400,144
В	Енергозбереження	CPU i5 H210	$3.85 \cdot 10^{-6}$	0.0125	3,268
Г		CPU Raspberry Pi 5 4GB	$3.85 \cdot 10^{-6}$	0.0301	~2,269

Аналіз таблиці 2 показує:

- для GPU $\tau \approx 10^5 - 10^6$ пікселів;
- для настільних CPU $\tau \approx 10^3 - 10^4$ пікселів;
- для Raspberry Pi $\tau \approx 2 \cdot 10^3$ пікселів;

Це означає, що на GPU доцільне агресивне об'єднання ROI, тоді як на CPU надмірне злиття швидко стає невигідним. Таким чином, оптимальна стратегія злиття є апаратно-залежною і визначається співвідношенням K_t/c_t.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі введено теоретичний поріг злиття τ, що формально визначає доцільність об'єднання ROI. Параметр τ залежить виключно від апаратних характеристик та параметрів виконання моделі.

Показано, що:

- лінійна модель вартості адекватно описує залежність часу виконання від площі ROI;
- оптимальна стратегія злиття визначається співвідношенням накладних витрат і питомої вартості пікселя;
- жадібний алгоритм з використанням критерію τ забезпечує найкращий компроміс між кількістю запусків моделі та зростанням площі.

Отримані результати можуть бути використані для апаратно-адаптивних систем комп'ютерного зору реального часу.

ДЖЕРЕЛА

1. Гозак, Я. Д., Палій, С. В. (2025) ПРИСКОРЕННЯ ЛОКАЛІЗАЦІЇ ОБ'ЄКТІВ У ВІДЕО НЕЙРОННОЮ МЕРЕЖЕЮ FASTER R-CNN ІЗ ВИКОРИСТАННЯМ ПОПЕРЕДНІХ КООРДИНАТ ОБ'ЄКТА. Друга міжнародна науково-практична конференція «Штучний інтелект та інформаційні технології», Київ, С. 174-175. НУХТ.

2. Lamichhane, B.R., Srijuntongsiri, G. and Horanont, T., (2025) CNN based 2D object detection techniques: a review. Frontiers in Computer Science, 7. https://doi.org/10.3389/fcomp.2025.1437664

3. Xie Liang, Gao Wei, Zhenghui Ming, Li Ge (2024) ROI-Guided Point Cloud Geometry Compression, Proc. ACM International Conference on Multimedia. https://doi.org/10.48550/arXiv.2504.14240



ЯРОСЛАВ ГОЗАК
Аспірант 2-го року навчання кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0009-0008-2963-7204
E-mail: hozakya@fit.knu.ua
Аспірант/дослідник у сфері комп'ютерного зору та оптимізації нейронних мереж для edge-платформ. Основні напрями досліджень: ROI-aware inference, оптимізація обчислень, UAV vision systems.



СЕРГІЙ ПАЛІЙ
к.т.н., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-9742-1116
E-mail: paliy@fit.knu.ua
Серед наукових інтересів — Інформаційнокомунікаційні технології, інтернет речей, електронне навчання, інформаційна безпека

ДОСЛІДЖЕННЯ МЕТАЕВРИСТИЧНИХ АЛГОРИТМІВ ДЛЯ ОПТИМІЗАЦІЇ МАРШРУТІВ В ДИНАМІЧНОМУ СЕРЕДОВИЩІ ДЛЯ ПОТРЕБ ДОСТАВКИ МАЛИХ ПІДПРИЄМСТВ

Єгор Гузь, Олена Федусенко

Анотація. *У роботі досліджено проблему автоматизації та оптимізації маршрутів доставки для малого бізнесу, яку формалізовано як динамічну задачу маршрутизації транспортних засобів із часовими вікнами. Для вирішення проблеми використано метаевристичні методи обчислень: алгоритм мурашиної оптимізації, генетичний алгоритм та розроблено їх гібридну комбінацію. Дослідження проводилося шляхом статичного та динамічного комп'ютерного моделювання на базі адаптованого датасету Соломона, що дозволило зімітувати процеси надходження та скасування замовлень у реальному часі в години пікового навантаження. За результатами порівняльного аналізу встановлено, що для роботи у статичних умовах найбільш ефективним та збалансованим є алгоритм мурашиної оптимізації , тоді як запропонований гібридний алгоритм демонструє найкращу адаптацію до динамічних та ефективність саме при високому динамічному навантаженні.*

Ключові слова: мурашині алгоритми, оптимізація маршрутів, гібридні алгоритми, ACO, генетичні алгоритми, VRP, часові вікна, динамічна оптимізація.

I. ВСТУП

У сучасному динамічному світі швидка та своєчасна доставка товарів є ключовим фактором для конкурентоспроможності малого бізнесу. На відміну від великих компаній, малі підприємства працюють з обмеженими ресурсами і невеликою кількістю замовлень, які надходять динамічно. Більшість малих підприємств, які потребують послуг доставки – підприємства харчової промисловості, як от пекарні, кондитерські, тощо. Наявність автоматизованої системи оптимізації та побудови маршрутів значно спростить логістичний процес та дозволить витратити зекономлений час та ресурси задля розвитку підприємства.

Специфіка оптимізації маршрутів в умовах обмежених ресурсів формує критерії при виборі алгоритму вирішення задачі. Оскільки наявні математичні та евристичні підходи є такими, що потребують значних обчислювальних ресурсів, метаевристичні алгоритми є оптимальним варіантом з точки зору обчислювальної складності та точності.

Метою даної роботи є дослідження наявних методів вирішення проблеми динамічної оптимізації маршруту, порівняння їх ефективності та працездатності в умовах, наближених до реальних.

Об’єктом дослідження є оптимізація в сфері логістики, предметом – метаевристичні алгоритми для вирішення задач побудови та оптимізацій маршрутів.

II. ДАНІ ТА МЕТОДИ

Згідно з класифікацією логістичних задач[1], досліджувана проблема класифікується як динамічна закрита задача маршрутизації з часовими вікнами та закритими умовами завершення маршруту. Такий тип належності визначає високий рівень обчислювальної складності та накладає специфічні обмеження на процес пошуку оптимальних рішень. Зокрема, динамічність параметрів вимагають адаптивності алгоритмів до вхідних даних, що відображено у наступній математичній моделі:

- Множина вузлів замовлення - $Z = \{0, 1, \dots, N\}$
- Множина транспортних засобів R
- Час у дорозі t_{ij}

- Чи відвідав транспорт точку доставки $x_{ijr} \in \{1, 0\}$

$$\min F \ \rightarrow F = F_1 + F_2 \tag{1}$$

$$F_1 = \sum_i^Z \ \sum_j^Z \ \sum_k^R \ x_{ijk} * t_{ij}, \forall i \neq j \tag{2}$$

$$F_2 = \sum_{j=i}^R \ P_j$$

Де P – штраф або функція штрафу за порушення вікна часу;

$$Z = (p \ \in A) \wedge (t(p_0, p) < T_r) \tag{3}$$

Де Z – зона відповідальності, або ж область можливих точок, p – точка, A – множина всіх можливих точок на мапі, $t(p_0, p)$ функція яка повертає час від складу p_0 до то будь-якої точки p. [2][3]

Враховуючи високу комбінаторну складність та динамічний характер описаних обмежень, найбільш адекватним інструментарієм для пошуку розв'язку є клас метаевристичних алгоритмів. З метою проведення порівняльного аналізу ефективності інтелектуального пошуку було реалізовано три підходи: класичний мурашиний алгоритм [2, 4], генетичний алгоритм [2, 5], а також розроблений авторами гібридний алгоритм [2]. Останній інтегрує механізми глобального пошуку генетичного підходу з локальною оптимізацією мурашиної колонії, що дозволяє нівелювати ризики передчасного збігання до локальних оптимумів та підвищити стабільність знайдених маршрутів.

Набір даних було сформовано на основі датасету, який був запропонований Маріусом Соломоном[6]. Датасет було адаптовано до умов моделювання відповідно до проведеного аналізу запиту користувачів. В ході аналізу було виявлено, що години найактивніших замовлень припадають на період 12:00 – 13:00 та 15:00-17:00. Результуючий датасет містив 24 записи, часові вікна кожного запису були згенеровані відповідно до активних годин доставки.

Оцінка ефективності обраних алгоритмів проводилася шляхом порівняльного аналізу в умовах статичного та динамічного моделювання. В статичному моделюванні кількість замовлень лишалась незмінна, тоді як в динамічному випадку було представлено випадкову генерацію двох подій – видалення замовлення та додавання нового замовлення. Ці події генерувалися не випадково, а з урахуванням періодів пікового попиту користувачів. Це дозволило оцінити, наскільки швидко алгоритми здатні перепланувати маршрути в умовах постійних змін.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Алгоритм мурашиної оптимізації (далі - ACO) та генетичний алгоритм (далі - GA) були реалізовані відповідно до класичної їх інтерпретації[2][4][5] з тією відмінністю, що обрахування відносної евристичної цінності було змінене відповідно до умов задачі з часовим вікном. Так, якщо в класичному варіанти використовується обернена відстань між точками маршруту, в модифікованому було запропоноване лінійне ускладнення задля врахування часового вікна. Відповідна функція $t(p_a, p_b)$ яка повертає час, який треба для того, щоб проїхати відстань між точками p_a, p_b була модифікована до наступного вигляду:

$$t_{ab} + \alpha * WT + \beta * U \tag{4}$$

- WT – час очікування
- OT – час відкриття вікна
- AT – час фактичного прибуття на місце (дистанція до точки)

- CWT – час закриття вікна
- $\mathrm{WT} = (0, \mathrm{OT} - \mathrm{AT})$[2][5]
- $\mathrm{UT} = \mathrm{CWT} - (\mathrm{AT} + \mathrm{WT})$ [2][5]
- t_{ab} – час, для подолання відстані між точками
- α, β – коефіцієнти, які задаються дослідником

Параметри алгоритмів для статичної та динамічної оптимізації наведені в таблиці 1. Варто
зазначити, що гібридний алгоритм використовує аналогічні параметри для складових.

Таблиця 1. *Параметри алгоритмів*

ACO	**К-сть ітерацій**	**Розмір колонії**	***α***	***β***	***ρ***	**Q**
	50	50	1	3	0.1	100
GA	**К-сть ітерацій**		**Розмір популяції**		**Ймовірність мутації**	
	50		50		0.1	

Для моделювання транспорту використовувались наступні конфігурації:

Таблиця 2.*Конфігурації транспорту*

Транспорт №	**Вантажомісткість**	**Час на завантаження (хв)**
1	6	20
2	5	15
3	4	10

Таблиця 3. *Порівняльна таблиця статичного моделювання*

Алгоритм	**Загальний час (хв)**	**Середній час на авто (год)**
ACO	1078	6
GA	1029	5.7
Гібридний	1153	6.4

Відповідно до результатів наведених у таблиці 3, найкращий час було отримано з використанням генетичного алгоритму. Втім, при детальному вивченні розподілу точок було виявлено, що алгоритм незбалансовано розподіляв замовлення між автомобілями. Відповідно, найкращий результат, який задовольняє критерії адекватності і оптимальності було отримано з допомогою мурашиного алгоритму. Гібридним алгоритмом було знайдене не найкраще, але збалансоване рішення.

Таблиця 4. *Порівняльна таблиця динамічного моделювання*

Алгоритм	**Загальний час (хв)**	**Додано (всього)**	**Скасовано(всього)**
ACO	1418	5	1
GA	1256	5	0
Гібридний	1225	6	0

За результатами симуляції динамічної оптимізації маршрутів доставки найкращі результати, а саме найменший час доставки, при найбільшому навантаженні на систему доставки було отримано з допомогою гібридного алгоритму, який поєднує елементи мурашиної оптимізації та генетичного алгоритму. Алгоритм мурашиної оптимізації показав найгірший результат при найменшій кількості замовлень всього. В той самий час генетичний алгоритм, який був малоефективний в статичному моделюванні, показав кращу пристосованість до динамічних умов.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Порівняльний аналіз підтвердив ефективність використання метаевристичних підходів для розв’язання задач динамічної маршрутизації. У статичних умовах найвищу точність продемонстрував алгоритм мурашиної оптимізації. Завдяки механізмам відкладання феромонів та спрямованої локальної оптимізації, ACO забезпечив рівномірний розподіл замовлень між транспортними засобами, що дозволило суттєво знизити пікове навантаження на окремі одиниці флоту. Водночас генетичний алгоритм виявився ефективним інструментом для дослідження широкого простору пошуку; завдяки операторам мутації та кросоверу він забезпечив високу варіативність розв'язків, хоча й продемонстрував нижчу швидкість збіжності до локальних оптимумів порівняно з ACO.

Проте в умовах підвищеного навантаження та динамічних змін зовнішнього середовища найкращу адаптивність показав гібридний алгоритм. Поєднання комбінаторних можливостей генетичного алгоритму (оператори мутації та кросоверу) із методами спрямованого пошуку ACO дозволило ефективно перепланувати маршрути в реальному часі без втрати якості розв'язку.

Практичне значення роботи полягає у можливості впровадження розроблених алгоритмів у логістичні процеси малих та середніх підприємств для підвищення їхньої конкурентоспроможності. Подальші дослідження будуть спрямовані на масштабування гібридних систем та врахування додаткових стохастичних факторів у ланцюгах постачання.

ДЖЕРЕЛА

1. Gülsün B., Miç P. Vehicle route planning for multiple targets in online map for a patient transport vehicle // The 2018 International Academic Research Conference in Oslo. – 2018. – С. 163-165.
2. Chen G., Gao J., Chen D. Research on Vehicle Routing Problem with Time Windows Based on Improved Genetic Algorithm and Ant Colony Algorithm. – 2024.
3. Івохін Є., Юштін К., Улеєв А. Спосіб формалізації та метод розв’язання багатокритеріальної задачі комівояжера // Міжнародна конференція MCIT. – 2024.
4. Dorigo M., Stützle T. Ant Colony Optimization. – MIT Press.
5. Ochelska-Mierzejewska J., Poniszewska-Maranda A., Maranda W. Selected genetic algrithms for vehicle routing problem solving. – 2021.
6. Solomon M. M. Algorithms for the vehicle routing and scheduling problems with time window constraints. – 1987.



ЄГОР ГУЗЬ
Студент АнД-41, кафедра інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна, Київ, Україна
E-mail: yegorhuz@knu.ua
Проходжу навчання за спеціальністю «Комп’ютерні науки» (4 курс). До наукових інтересів належать еволюційні обчислення, метаевристичні алгоритми та моделювання систем.



ОЛЕНА ФЕДУСЕНКО
Доцент, кафедра інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна, Київ, Україна
ORCID: 0000-0002-5782-5922
E-mail: fedusenko@knu.ua
Отримала ступінь кандидата технічних наук у галузі інформаційних технологій у 2006 році. Є автором понад 70 наукових праць. До наукових інтересів належать системи адаптивного навчання, генетичні алгоритми та їх прикладне застосування, методи Data Mining.

ЗАСТОСУВАННЯ АЛГОРИТМІВ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ІДЕНТИФІКАЦІЇ РАДІОІЗОТОПІВ НА ОСНОВІ СИНТЕТИЧНИХ ДАНИХ

Юрій Забулонов, Тетяна Носенко

Анотація. *У роботі досліджується процес навчання 1D згорткових нейронних мереж (CNN) для ідентифікації замаскованих джерел гамма-випромінювання. Оскільки збір масштабних реальних даних у небезпечних умовах є ускладненим, використано синтетичні датасети, згенеровані за допомогою цифрових двійників. Наукова новизна роботи полягає в концептуальній зміні підходу до аналізу спектрів: комптонівський континуум, сформований багаторазовим розсіюванням у середовищах з низьким Z, використовується не як завада, а як інформативна ознака для ідентифікації. Застосування методів рандомізації домену дозволило досягти загальної точності 79%, ефективно зменшуючи розрив між симуляцією та реальними умовами при радіаційному моніторингу.*

Ключові слова: згорткові нейронні мережі, гамма-спектроскопія, синтетичні дані, комптонівське розсіювання, фактор накопичення.

I. ВСТУП

Швидкий розвиток систем штучного інтелекту відкриває нові можливості у сфері радіаційної безпеки. Традиційні алгоритми ідентифікації радіоізотопів часто дають збої, коли джерело випромінювання знаходиться за захисним екраном, оскільки первинні фотопіки поглинаються, а спектр спотворюється через ефекти комптонівського розсіювання [1]. Згорткові нейронні мережі (CNN) здатні виявляти складні нелінійні патерни у таких спектрах [2], проте їх навчання потребує великих масивів даних. Метою цієї роботи є розробка алгоритму навчання 1D-CNN на синтетичних гамма-спектрах із застосуванням методів адаптації домену для подолання розриву між симуляцією та реальністю. Новизна дослідження полягає у доведенні можливості ідентифікації ізотопів за відсутності виражених фотопіків — виключно за формою спектрального розподілу розсіяного випромінювання (фактором накопичення), що робить систему стійкою до сильного екранування матеріалами з низьким ефективним атомним номером.

II. ДАНІ ТА МЕТОДИ

Навчальний набір спектрів згенеровано методом Монте-Карло [3] за допомогою інструментарію Geant4 [4]. Моделювання охоплювало 8 типових ізотопів (^{137}Cs, ^{60}Co, ^{131}I тощо) та 4 види захисних матеріалів. Загальний обсяг згенерованого синтетичного датасету (з урахуванням додавання статистичного шуму для наближення до реальних умов вимірювання) склав 8000 унікальних спектрів. Для забезпечення об'єктивного процесу навчання та уникнення перенавчання набір даних було розділено на навчальну та тестову вибірки у пропорції 80/20 зі збереженням балансу класів. Фінальна оцінка загальної точності моделі (79,9%) проводилася виключно на ізольованому тестовому наборі.

Алгоритм обчислення інтенсивності випромінювання, що проходить через захисний бар'єр, базується на модифікованому законі Бера-Ламберта. Для середовищ із низьким ефективним атомним номером ($Z_{eff} \approx 7.4$ для води та поліетилену) стандартне експоненційне загасання доповнюється фактором накопичення B(E, x), що враховує багаторазове комптонівське розсіювання [4]:

$$I(E,x) = I_0(E) \cdot B(E,x) \cdot e^{-\mu(E)x}, \quad (1)$$

де *I(E,x)* — інтенсивність зареєстрованого випромінювання з енергією *E* після проходження шару товщиною *x;* $I_0(E)$ — початкова інтенсивність; $\mu(E)$ — лінійний коефіцієнт загасання. Симуляція Монте-Карло дозволила стохастично обчислити *B(E, x),* формуючи реалістичний щільний низькоенергетичний фон у згенерованих спектрах.

Кожен згенерований спектр подається на вхід мережі як одновимірний вектор $X = [x_1, x_2, ..., x_{1024}]$, де x_i — кількість відліків у і-му енергетичному каналі.

Як показано на Рисунку 1, алгоритм прямого поширення для l-го згорткового шару 1D-CNN обчислюється за формулою:

$$H_j^l = ReLU\left(\sum_{k+1}^{K} W_{j,k}^{(l)} * H_k^{(l-1)} + b_j^{(l)}\right), \quad (2)$$

де $H^{(l)}_j$ — j-та карта ознак поточного шару, $W^{(l)}$ — ядро згортки, $b^{(l)}$ — вектор зміщення, а операція (*) позначає одновимірну згортку.

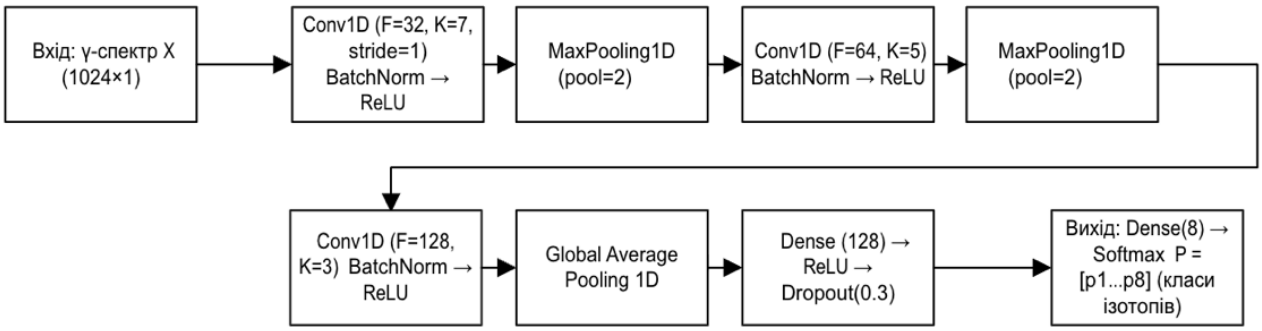


Рисунок 1. *Архітектура 1D згорткової нейронної мережі для класифікації гамма-спектрів*

Після проходження через шари субдискретизації (MaxPooling) та повнозв'язні шари, вихідний шар Softmax генерує вектор ймовірностей P:

$$P_c = \frac{e^{z_c}}{\sum_{k=1}^{8} e^{z_k}}, \quad (3)$$

де P_c — ймовірність належності спектра до с-го класу ізотопу (з 8 можливих). Навчання мережі здійснювалося за алгоритмом зворотного поширення помилки з мінімізацією функції втрат категоріальної крос-ентропії (Categorical Cross-Entropy).

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Тестування розробленого алгоритму 1D-CNN на валідаційній вибірці показало, що загальна точність ідентифікації ізотопів за наявності захисних екранів становить 79%. Аналіз роботи мережі продемонстрував принципову різницю в розпізнаванні залежно від матеріалу захисту. Для розсіювальних середовищ (поліетилен, вода), де первинні піки поглинаються, мережа успішно визначає джерело, аналізуючи форму низькоенергетичного спектрального "хвоста". Це підтверджує, що ефекти багаторазового розсіювання, математично описані фактором накопичення *B(E,x),* нейромережа здатна використовувати як додаткову інформативну ознаку. Відповідно, точність алгоритму Монте-Карло у Geant4 є критичною для успішного навчання класифікатора.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Застосування алгоритмів 1D-CNN у поєднанні з даними Монте-Карло є ефективним інструментом для ідентифікації радіоізотопів в умовах сильного екранування [3]. Досягнута точність у 79% свідчить про здатність мережі виділяти складні спектральні патерни, створювані комптонівським розсіюванням у матеріалах з низьким Z. Глибока згорткова архітектура продемонструвала ефективність автоматичного ієрархічного вилучення ознак без необхідності ручної інженерії спектральних параметрів, що підтверджує потенціал CNN як універсального інструменту для аналізу зашумлених радіометричних даних. Подальші дослідження будуть зосереджені на адаптації алгоритму для аналізу часових рядів (динамічного виявлення) із застосуванням рекурентних нейронних мереж (LSTM) та розробці архітектур глибокого навчання (наприклад, 1D-CNN або моделей на основі трансформаторів), навчених на згенерованому наборі даних для сліпої ідентифікації ізотопів та оцінки товщини екранування на основі регресії.

ДЖЕРЕЛА

1. Ел-Тохі М. С. Швидкі та надійні алгоритми ідентифікації радіоізотопів у рентгенівських та гамма-спектрах // Вимірювання. 2021. Т. 168. С. 108456.
2. Носенко Т. І., Машкіна І. В., Мельник І. Ю. Застосування одновимірних згорткових нейронних мереж для ідентифікації слабких радіоактивних сигналів у системах динамічного моніторингу // Кібербезпека: освіта, наука, техніка. 2025. № 3(31). С. 781–791. DOI: https://doi.org/10.28925/2663-4023.2025.31.1074
3. де Олівейра Ф. М., Даніель Г., Лімузен О. Моделювання спектрів штучного гамма-випромінювання з використанням генеративно-змагальних мереж та керованих генеративних мереж // Nuclear Instruments and Methods in Physics Research Section A. 2023. Vol. 1047. P. 167795. DOI: https://doi.org/10.1016/j.nima.2022.167795
4. Kwon J., Kim J., Kim H., Kim S., Jang S., Lee J., Kim Y. S. Development of gamma-spectrum data generation method by Monte Carlo simulation // Journal of the Korean Physical Society. 2023. Vol. 82, No. 7. P. 658–670. DOI: https://doi.org/10.1007/s40042-023-00760-7
5. Maeng S., Lee S. H., Park S. J., Choi W. C. Evaluation of detection efficiency for low-energy NaI(Tl) scintillation detector // Radiation Physics and Chemistry. 2022. Vol. 199. P. 110325.



ЮРІЙ ЗАБУЛОНОВ
Директор інституту, завідувач відділу ядерно-фізичних технологій Державної установи "Інститут геохімії навколишнього середавища» Академії наук України, Київ, Україна
ORCID: 0000-0001-8239-8654
E-mail: 1952zyl@gmail.com
д.т.н., проф., академік НАН України
Наукові інтереси - ядерно-фізичні технології, радіаційний та екологічний моніторинг, спектрометрія іонізуючих випромінювань, системи ядерної безпеки.



ТЕТЯНА НОСЕНКО
к.т.н., доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7597-9861
E-mail: t.nosenko@kubg.edu.ua
Наукові інтереси — Штучний інтелект, нейромережеві технології, фізично-інформоване машинне навчання.

МУЛЬТИАГЕНТНИЙ ПІДХІД ДО ФОРМУВАННЯ РОЗКЛАДУ ЗАНЯТЬ З ДЕЦЕНТРАЛІЗОВАНИМ УЗГОДЖЕННЯМ РІШЕНЬ

Ганна Красовська, Ольга Ізмайлова, Олег Іларіонов

Анотація. *У роботі розглянуто застосування мультиагентного підходу до задачі формування розкладу занять у закладах вищої освіти. Запропоновано децентралізований механізм узгодження часових слотів між агентами, що представляють основні сутності навчального процесу. Взаємодія агентів реалізується на основі аукціонної моделі розподілу ресурсів із використанням протоколів взаємодії, сумісних зі стандартами FIPA. Для перевірки запропонованого підходу розроблено прототип мультиагентної системи на платформі JADE. Отримані результати демонструють можливість застосування мультиагентних систем для автоматизованого формування розкладу занять.*

Ключові слова: мультиагентні системи, формування розкладу занять, децентралізоване узгодження рішень, аукціонний механізм, FIPA, JADE

I. ВСТУП

Формування розкладу занять є складною задачею комбінаторної оптимізації, що передбачає розподіл обмежених ресурсів (викладачів, навчальних груп та аудиторій) у межах заданого часового інтервалу з урахуванням численних обмежень. До них належать як жорсткі обмеження (неможливість проведення кількох занять одночасно в одній аудиторії або викладання викладачем у кількох групах у той самий час), так і м'які обмеження, пов'язані з оптимальністю структури розкладу та побажаннями учасників освітнього процесу. Подібні задачі є предметом дослідження в галузі операційних досліджень та штучного інтелекту [1].

Сучасні підходи до розв'язання задач формування розкладу включають методи оптимізації, евристичні алгоритми та автоматизовані системи планування навчального процесу [2]. Одним із перспективних напрямів є використання мультиагентних систем, у яких окремі компоненти представлені автономними агентами, що взаємодіють між собою з метою досягнення узгодженого рішення [3]. Децентралізований характер таких систем дозволяє організувати кооперативне прийняття рішень і гнучко враховувати обмеження різних учасників процесу планування.

Метою роботи є дослідження можливостей застосування мультиагентного підходу до формування розкладу занять та розробка прототипу системи з децентралізованим механізмом узгодження часових слотів між агентами.

II. ДАНІ ТА МЕТОДИ

Мультиагентні механізми координації широко застосовуються у задачах планування та розподілу ресурсів, де децентралізована взаємодія агентів дозволяє ефективно розв'язувати складні задачі узгодження та прийняття рішень [4]. У сучасних дослідженнях також розглядається застосування мультиагентних систем для автоматизованого формування розкладу навчального процесу та оптимізації використання навчальних ресурсів [5].

Формально задачу формування розкладу можна розглядати як задачу розподілу множини занять $L = \{l_1, l_2, \dots, l_n\}$між множиною часових слотів $T = \{t_1, t_2, \dots, t_m\}$ та множиною аудиторій $R = \{r_1, r_2, \dots, R_k\}$ за наявності системи обмежень.

У запропонованій мультиагентній системі агенти представляють основних учасників освітнього процесу – викладачів та академічні групи. Кожен агент володіє інформацією про

власні обмеження, доступні часові інтервали та бере участь у процесі узгодження розкладу, формуючи власну функцію переваг щодо можливих часових слотів.

Процес узгодження розкладу реалізується через послідовність переговорів між агентами, у межах яких відбувається обмін повідомленнями відповідно до протоколів FIPA (Foundation for Intelligent Physical Agents). У процесі переговорів агенти формують пропозиції щодо використання часових слотів та коригують свої рішення на основі отриманих пропозицій інших агентів.

Такий підхід дозволяє розглядати формування розкладу як задачу кооперативної оптимізації, у якій глобальне рішення формується в результаті локальних взаємодій агентів.

Взаємодія агентів реалізується через механізм переговорів, заснований на аукціонній моделі розподілу ресурсів, що реалізується за допомогою протоколу взаємодії агентів, сумісного зі стандартами FIPA . У такому підході агенти формують пропозиції щодо використання часових слотів та поступово узгоджують рішення у процесі переговорів.

Для реалізації прототипу використано платформу JADE, що підтримує стандарти FIPA та забезпечує інфраструктуру для створення та взаємодії програмних агентів. Реалізація виконана мовою програмування Java, а для відображення результатів роботи агентів використано графічний інтерфейс.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У ході дослідження було розроблено прототип мультиагентної системи формування розкладу занять. У системі визначено два основні типи агентів: агенти-викладачі та агенти-групи. Агенти обмінюються інформацією про доступні часові слоти та здійснюють їх узгодження у процесі переговорів.

Запропонований механізм передбачає поступове формування розкладу шляхом вибору агентами найбільш прийнятних часових слотів. Для уникнення конфліктів і досягнення узгодженого рішення використано механізм коригування пріоритетів слотів, що дозволяє враховувати обмеження та додаткові критерії оптимальності.

Аналіз роботи системи показав, що децентралізований механізм узгодження дозволяє поступово досягати узгодженого розподілу часових слотів навіть за наявності конфліктних вимог між агентами. При цьому переговорний процес забезпечує адаптивність системи до зміни умов планування, оскільки агенти можуть переглядати власні пропозиції та коригувати рішення у ході взаємодії.

У результаті взаємодії агентів формується узгоджений розклад занять для викладачів та академічних груп, який задовольняє основні обмеження задачі.

III. ВИСНОВКИ

Отримані результати демонструють можливість застосування мультиагентного підходу до задач формування розкладу занять.

Запропонований підхід дає змогу розглядати задачу формування розкладу як задачу розподіленого прийняття рішень, у якій глобальне рішення формується в результаті взаємодії автономних агентів, що забезпечує гнучке врахування обмежень різних учасників освітнього процесу. Використання децентралізованого механізму узгодження, заснованого на аукціонній моделі взаємодії агентів, забезпечує ефективну координацію дій учасників системи та формування узгодженого розкладу.

Подальші дослідження можуть бути спрямовані на розширення моделі узгодження рішень в умовах зростання кількості обмежень та учасників системи, вдосконалення механізмів переговорів між агентами, урахування додаткових обмежень та інтеграцію системи з інформаційними системами навчального закладу.

ДЖЕРЕЛА

1. Ceschia S., Di Gaspero L., Schaerf A. (2023) Educational timetabling: Problems, benchmarks, and state-of-the-art results. European Journal of Operational Research, 308, 1–18. https://doi.org/10.1016/j.ejor.2022.07.011
2. Diallo F.P., Tudose C. (2024) Optimizing the scheduling of teaching activities in a faculty. Applied Sciences, 14, 9554. https://doi.org/10.3390/app14209554
3. Allmendinger S., Bonenberger L., Endres K., Fetzer D., Gimpel H., Kühl N. (2026) Multi-Agent AI. Electronic Markets, 36, 18. https://doi.org/10.1007/s12525-025-00862-z
4. Chen C., Zhao A., Zhang Z., Zhang T., Fan C. (2025) Research on multi-agent collaborative scheduling planning method for time-triggered networks. Electronics, 14, 2575. https://doi.org/10.3390/electronics14132575
5. Sharmila V., Kumar P., Singh R. (2025) Dynamic timetable scheduling using multi-agent systems and federated learning. In: Proceedings of the International Conference on Sustainability Innovation in Computing and Engineering (ICSICE 24). Advances in Computer Science Research, 120. https://doi.org/10.2991/978-94-6463-718-2_124



ГАННА КРАСОВСЬКА
к.т.н., доцент, доцент кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-1986-6130
E-mail: hanna.krasovska@knu.ua
Фахівець у галузі інтелектуальних інформаційних технологій. Має багаторічний досвід науково-педагогічної діяльності та підготовки фахівців з комп'ютерних наук, зокрема у сфері систем штучного інтелекту.
Наукові інтереси – інтелектуальні технології підтримки прийняття рішень, мультиагентні системи, моделювання та аналіз складних систем.



ОЛЬГА ІЗМАЙЛОВА
к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії факультету автоматизації і інформаційних технологій Київського національного університету будівництва та архітектури
ORCID: 0000-0002-2905-1827
E-mail: izmailova.ov@knuba.edu.ua
Фахівець у галузі інформаційних систем та технологій. Має досвід практичної інженерної діяльності та участі у наукових і прикладних проєктах у сфері IT та кібербезпеки.
Наукові інтереси – системний аналіз, проєктування інформаційних систем, управління ризиками, методи підтримки прийняття рішень.



ОЛЕГ ІЛАРІОНОВ
к.т.н., доцент, завідувач кафедри кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0002-7435-3533
E-mail: oleg.ilarionov@knu.ua
Фахівець у галузі комп'ютерних наук та інтелектуальних інформаційних технологій. Має значний досвід науково-педагогічної та організаційної діяльності у закладах вищої освіти. Автор понад 50 наукових і навчально-методичних праць.
Наукові інтереси – інтелектуальні інформаційні системи, моделювання складних систем, технології підтримки прийняття рішень, застосування методів штучного інтелекту.

МОДЕЛЬ DT-DEC-POMDP ДЕЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ РОЄМ БПЛА З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ ТА СТОХАСТИЧНИМИ ПОРУШЕННЯМИ ЗВ'ЯЗКУ

Єгор Мєзєнцев, Юрій Кравченко

Анотація. *У роботі запропоновано розширення класичного формалізму Dec-POMDP для керування роєм безпілотних літальних апаратів у середовищі з динамічною топологією взаємодії та стохастичними порушеннями зв'язку. Стан системи доповнено часовим графом зв'язності, а процес спостережень визначено з урахуванням ймовірності втрати пакетів. Для компенсації інформаційних лакун введено блок Comm-Disturbance Filter із предиктивною реконструкцією даних сусідів, а для контекстної агрегації стабілізованих спостережень – Multi-agent Transformer. Моделювання виявило критичні пороги стійкості за різних рівнів ploss та показало ефективність компенсаційної зони.*

Ключові слова: Dec-POMDP; рій БпЛА; динамічна топологія; втрата пакетів; multi-agent transformer.

I. ВСТУП

Координація груп автономних агентів (зокрема роїв БпЛА) в умовах часткової спостережуваності та відсутності централізованого керування часто формалізується як Dec-POMDP [1]. Утім, практичні сценарії (розвідка, пошук і рятування, робота в умовах радіоелектронного придушення) характеризуються безперервною трансформацією комунікаційного графа та втратами пакетів, що руйнують припущення класичних постановок [9, 10].

Метою дослідження є розроблення математичної моделі децентралізованого керування, яка інтегрує динамічну топологію взаємодії та стохастичні збої зв'язку як ендогенні фактори формування інформаційного простору агента. Основний внесок: формалізація DT-Dec-POMDP із розширеним станом; модель спостережень із бернуллівською пакетною втратою; архітектура компенсації Comm-Disturbance Filter та контекстної агрегації на базі Multi-agent Transformer (MAT).

II. ДАНІ ТА МЕТОДИ

У DT-Dec-POMDP топологія взаємодії описується часовим графом:

$$G_t = (V, E_t), \tag{1}$$

де V – множина агентів, а $E_t \subseteq V \times V$– множина ребер зв'язності у момент часу t.

Глобальний стан системи задається як:

$$\tilde{s}_t = (s_t, G_t) \in \mathcal{S} \times \mathcal{G}, \tag{2}$$

що забезпечує марковську властивість відносно розширеного простору станів і дозволяє моделювати залежність спостережень від поточної конфігурації мережі.

Якість зв'язку між агентами i та j параметризується імовірністю доставки пакета та залежить від відстані dij(t) і завадового контексту. Факт доставки повідомлення mj(t) моделюється змінною $\xi_{ij}(t) \in \{0,1\}$, де

$$\xi_{ij}(t) \sim \text{Bernoulli}(1 - p_{loss}), \tag{3}$$

а

$$p_{loss} = \Phi(d_{ij}, SIR, \rho), \tag{4}$$

є динамічною функцією, що враховує відношення сигнал/інтерференція та локальну щільність вузлів. Ефективне спостереження агента визначається як:

$$o_i^{eff(t)} = (o_i^{sens(t)}, \{\xi_{ij}(t) \cdot m_j(t)\}_{j \in Ni(t)}), \tag{5}$$

Для зменшення впливу інформаційних лакун запропоновано модуль Comm-Disturbance Filter, який детектує пропуски за часовими мітками та номерами послідовності, виконує короткострокову рекурсивну екстраполяцію стану сусіда

$$\hat{s} = f\big(s_j(t-1), a_j(t-1)\big) + \epsilon(t), \tag{6}$$

формує стабілізований вектор спостережень ōi(t), придатний для навчання політики без різких розривів у вході.

Стабілізовані спостереження ōi(t) подаються до MAT-контролера, який агрегує повідомлення від змінної множини сусідів механізмом self-attention та забезпечує інваріантність до кількості агентів. Навчання політик здійснюється за схемою Centralized Training – Decentralized Execution: під час тренування використовується «глобальний критик» із доступом до істинного Gt, а під час виконання – лише локальна політика агента.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Для оцінювання стійкості розглянуто симуляційні сценарії з рухом агентів, що змінює граф зв'язності, та із стохастичною пакетною втратою ploss у діапазоні 0–0,5. Як показано на Рисунку 1, розосередження рою призводить до «розрідження» Et і до зменшення доступності міжагентних повідомлень.

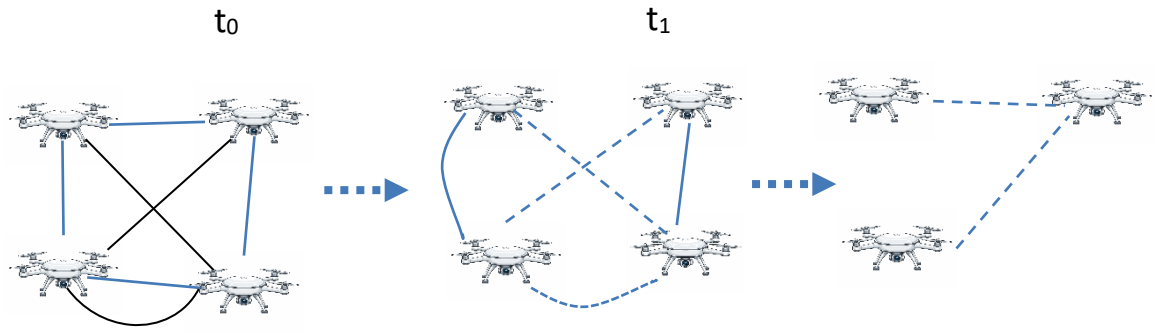


Рисунок 1. *Еволюція графа зв'язності рою (часові зрізи t0–t2)*

Експериментально виділено три режими функціонування системи залежно від ploss (Таблиця 1).

У компенсаційній зоні Comm-Disturbance Filter забезпечує відновлення локального інформаційного поля агента і стабілізує навчання MAT, що зменшує відхилення траєкторій та кількість конфліктів маневрування порівняно з базовими політиками без компенсації [7, 11].

Таблиця 1. *Режими функціонування системи за інтенсивністю пакетних втрат*

Режим	Діапазон ploss	Характеристика та наслідки
Зона прозорості	ploss < 0,10	Втрати компенсуються надлишковістю інформації у щільному графі; політики близькі до ідеалізованих.
Зона компенсації	0,10 ≤ ploss ≤ 0,35	Comm-Disturbance Filter відновлює короткі розриви; MAT стабільно агрегує контекст. Відхилення траєкторій зменшуються, зберігається узгодженість групи.
Зона фрагментації	ploss > 0,35	Накопичення екстраполяційних похибок призводить до розпаду спільного інформаційного простору; агенти переходять до локальних стратегій і зростає ризик розсіювання рою.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати підтверджують, що явне включення топології та якості зв'язку до марковського стану підвищує переносимість політик із симуляції до реальних умов, де топологія є нестаціонарною, а зв'язок – ненадійним. Компенсаційний фільтр відіграє роль прогнозуючого буфера, що знижує чутливість контролера до випадкових провалів комунікації і розширює область працездатності системи.

Запропонована модель DT-Dec-POMDP та архітектура «фільтр + MAT + CTDE» формують основу для проєктування масштабованих роїв БпЛА, стійких до фрагментації мережі.

Подальші дослідження доцільно спрямувати на оптимізацію обчислювальних витрат self-attention для великих роїв, валідацію на апаратно-реалістичних симуляторах та інтеграцію механізмів управління довірою й постквантової автентифікації в комунікаційному контурі [4–6].

ДЖЕРЕЛА

1. Abdoo E., Brafman R.I., Shani G., Soffair N. (2023) Team-Imitate-Synchronize for Solving Dec-POMDPs. In: Machine Learning and Knowledge Discovery in Databases (ECML PKDD 2022). Springer. https://doi.org/10.1007/978-3-031-26412-2_14

2. Pey J.J.J., Samarakoon S.M.B.P., Muthugala M.A.V.J., Elara M.R. (2024) A Decentralized Partially Observable Markov Decision Process for Dynamic Obstacle Avoidance and Complete Area Coverage using Multiple Reconfigurable Robots. Proc. IEEE/RSJ IROS 2024. https://doi.org/10.1016/j.eswa.2025.126565

3. Keller R., Brafman R.I. (2026) Solving Dec-POMDPs as POMDPs Using Imitation Learning. In: PRIMA 2025: Principles and Practice of Multi-Agent Systems. Springer. https://doi.org/10.1007/978-3-032-13562-9_9

4. Hu Y., Gan Y., Wu Y., Wang H., Ma C., Xiong C. (2025) GDM-DTM: A Group Decision-Making-Enabled Dynamic Trust Management Method for Malicious Node Detection in Low-Altitude UAV Networks. Sensors, 25(13), 3982. https://doi.org/10.3390/s25133982

5. He L., Zhao M., Wang X.A., Wang J., Wang Z., Liu S. (2025) A Post-Quantum Authentication and Key Agreement Scheme for Drone Swarms. Electronics, 14(17), 3364. https://doi.org/10.3390/electronics14173364

6. Sysoyev A., Nauruzov K., Karati A., Abramkina O., Vitulyova Y., Yeskendirova D., Abdoldina F. (2025) Lightweight group signature scheme based on PUF for UAV communication security. Drones, 9(10), 693. https://doi.org/10.3390/drones9100693
7. Alqefari S., Menai M.E.B. (2025) A Hybrid Method to Solve the Multi-UAV Dynamic Task Assignment Problem. Sensors, 25(8), 2502. https://doi.org/10.3390/s25082502
8. Norbelt M., Luo X., Sun J., Claude U. (2025) UAV localization in urban area mobility environment based on monocular VSLAM with deep learning. Drones, 9(3), 171. https://doi.org/10.3390/drones9030171
9. Мальков О., Похнатюк С., Кудимов С., Шерихов І. (2025) Проблемні питання авіаційної підтримки військ армійською авіацією за досвідом російсько-української війни та можливі шляхи їх вирішення. Військово-технічний збірник, 33(2), 127–140. https://doi.org/10.33577/2312-4458.33.2025.127-140
10. Мосов С. (2024) Роїння дронів військового призначення: реалії та перспективи. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ, 1(80), 77–86. https://doi.org/10.33099/2304-2745/2024-1-80/77-86
11. Панкратова Н., Панкратов В., Голінко І. (2025) Стратегія застосування цифрового двійника за умов децентралізованого керування роєм безпілотних літальних апаратів. Доповіді НАН України, 6, 23–34. https://doi.org/10.15407/dopovidi2025.06.023
12. Posvistak V., Miroshnychenko D. (2024) Architecture of autonomous control system for FPV-drones. Herald of Khmelnytskyi National University. Technical Sciences, 337(3), 223–230. https://doi.org/10.31891/2307-5732-2024-337-3-33



ЄГОР МЄЗЄНЦЕВ
магістр, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0004-2228-0303
E-mail: egor.mezencev@gmail.com
Наукові інтереси: штучний інтелект, системи БПЛА, мережеві технології, бізнес-аналітика.



ЮРІЙ КРАВЧЕНКО
доктор технічних наук, професор, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-0281-4396
E-mail: yurii.kravchenko@knu.ua
За понад 30 років викладацької та наукової діяльності опублікував понад 230 наукових праць, серед яких 2 монографії, 14 підручників та посібників. Індекс Гірша в Scopus – 21, у Google Scholar – 21. Підготував 5 докторів, 8 кандидатів наук та 3 PhD.
Наукові інтереси – телекомунікаційні системи, функціональна стійкість складних систем, штучний інтелект.

ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ У ВЕБЗАСТОСУНКАХ ПОШУКУ РОБОТИ В ІТ

Павло Мосієнко

Анотація. *У роботі здійснено аналітичний огляд застосування систем штучного інтелекту у вебзастосунках пошуку роботи в IT-сфері. Розглянуто використання алгоритмів машинного навчання, рекомендаційних систем та методів обробки природної мови для персоналізації вакансій і автоматичного ранжування результатів. Проаналізовано функціональні можливості міжнародних і українських платформ, зокрема LinkedIn, Indeed, Djinni та DOU. Визначено переваги інтелектуальних технологій, а також окреслено проблеми алгоритмічної упередженості й залежності від якості даних.*

Ключові слова: штучний інтелект, машинне навчання, рекомендаційні системи, персоналізація, IT-рекрутинг.

I. ВСТУП

Стрімкий розвиток IT-сфери зумовлює постійне зростання кількості вакансій та вимог до професійних навичок кандидатів. Традиційні механізми пошуку роботи, що базуються на простій фільтрації за ключовими словами, поступово втрачають ефективність через великий обсяг інформації та складність зіставлення вимог роботодавців із компетенціями кандидатів.

У зв’язку з цим особливої актуальності набуває застосування систем штучного інтелекту (ШІ) у вебзастосунках пошуку роботи. Метою роботи є аналітичний огляд сучасних підходів до використання AI-технологій у платформах пошуку IT-вакансій та визначення їхніх переваг і обмежень.

II. ДАНІ ТА МЕТОДИ

Дослідження має аналітичний характер і ґрунтується на огляді наукових джерел, технічної документації та функціональних можливостей сучасних платформ пошуку роботи.

Об’єктом аналізу стали міжнародні та українські сервіси, зокрема LinkedIn, Indeed, Djinni та DOU.

Методологія включає:

- порівняльний аналіз функціоналу платформ;
- узагальнення підходів до застосування алгоритмів машинного навчання;
- аналіз використання методів обробки природної мови (NLP);
- систематизацію принципів роботи рекомендаційних систем.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Проведений аналіз показав, що сучасні вебзастосунки пошуку роботи в IT активно використовують такі інтелектуальні технології:

1. Рекомендаційні системи, які формують персоналізовану стрічку вакансій з урахуванням профілю користувача, його навичок, досвіду, поведінкової активності та історії відгуків.
2. Алгоритми машинного навчання, що здійснюють автоматичне ранжування вакансій за рівнем релевантності та прогнозують ймовірність відгуку або успішного працевлаштування.

3. Методи обробки природної мови (NLP), які забезпечують семантичний аналіз описів вакансій і резюме, автоматичне виділення ключових технологій, рівня досвіду, спеціалізації та відповідності soft skills.
4. Аналітику ринку праці, що дозволяє визначати актуальні тренди, найбільш затребувані технології, середній рівень заробітних плат і динаміку попиту на фахівців.
5. Системи автоматизованого скринінгу кандидатів (ATS), які застосовуються компаніями для первинного відбору резюме, перевірки відповідності вимогам вакансії та оптимізації роботи HR-відділів.
6. Прогностичні моделі, що оцінюють кар'єрні траєкторії кандидатів, потенціал розвитку та ризик зміни роботи.
7. A/B-тестування та поведінкову аналітику, які дозволяють платформам оптимізувати інтерфейс, механізми рекомендацій та конверсію відвідувачів у кандидатів.

Також для систематизації отриманих результатів проведено порівняльний аналіз використання інтелектуальних технологій на досліджуваних платформах що наведено в Таблиці 1.

***Таблиця 1**. Порівняння використання методів ШІ досліджуваними платформами*

Метод	**LinkedIn**	**Indeed**	**Dou**	**Djinni**
Рекомендаційні системи	Так	Так	Частково	Частково
ML-ранжування вакансій	Так	Так	Частково	Ні
NLP-аналіз вакансій	Так	Так	Частково	Ні
Аналітика ринку праці	Так	Так	Частково	Так
Автоматичний скринінг	Так	Так	Ні	Ні
Прогностичні моделі	Так	Частково	Ні	Ні
A/B-тестування та поведінкова аналітика	Так	Так	Частково	Частково

У межах запропонованої концепції доцільним є використання AI-агента, який поєднує внутрішні корпоративні дані та зовнішній аналіз ринку праці. На першому етапі система аналізує інформацію HR-відділу про вже найнятих співробітників: їхні професійні навички, досвід, кар'єрну динаміку та показники ефективності. На основі цих даних формується узагальнений профіль «успішного працівника», який використовується для навчання моделі машинного навчання. Таким чином, система фактично орієнтується на реальні кейси успішного працевлаштування в конкретній компанії.

На другому етапі AI-агент здійснює аналіз зовнішнього ринку: обробляє описи вакансій, резюме кандидатів, визначає актуальні технології та рівень конкуренції. Для цього застосовуються методи NLP, семантичного порівняння текстів і векторного представлення даних. Додатково можуть використовуватися прогностичні моделі для оцінювання відповідності кандидата вимогам конкретної посади.

На завершальному етапі відбувається зіставлення вимог відкритої вакансії з профілем «успішного працівника» та характеристиками потенційних кандидатів. Система формує рейтинг претендентів із визначенням ступеня релевантності та ключових факторів відповідності. Це дозволяє суттєво скоротити час первинного відбору, підвищити точність підбору персоналу та мінімізувати суб'єктивність рішень.

Таком чином принцип функціонування запропонованої системи доцільно подати в Рисунку 1 у вигляді структурної блок-схеми.

Проте сама система не може гарантувати абсолютну точність результатів. Рішення моделі базуються на наявних даних і виявлених закономірностях, тому можливі похибки, неповнота оцінювання або вплив алгоритмічної упередженості. У зв'язку з цим результати ранжування кандидатів не повинні розглядатися як остаточне рішення, а лише як інструмент підтримки прийняття рішень.



Рисунок 1. *Блок-схема роботи системи штучного інтелекту для оцінки потенційних робітників*

Контроль коректності сформованого рейтингу має здійснюватися HR-відділом компанії. Фахівці з персоналу повинні аналізувати запропонований системою список кандидатів, перевіряти релевантність критеріїв відбору та, за необхідності, коригувати параметри моделі або вагові коефіцієнти оцінювання. Такий підхід забезпечує поєднання автоматизованого аналізу з експертною оцінкою людини, що зменшує ризик помилкових рішень. Ефективною реалізацією AI-агента можна вважати гібридну модель взаємодії «людина–алгоритм», у межах якої система виконує функцію інтелектуальної підтримки, а остаточне рішення щодо найму залишається за HR-фахівцями.

Однак впровадження подібного AI-агента пов'язане з низкою суттєвих обмежень. Однією з ключових проблем є висока ресурсомісткість системи. Для ефективного функціонування модель потребує значних обсягів якісних історичних даних, обчислювальних потужностей для навчання та оновлення алгоритмів, а також постійної технічної підтримки. Особливо це стосується використання складних моделей глибокого навчання та семантичного аналізу текстів, які потребують серверної інфраструктури або хмарних рішень.

Таким чином, хоча інтелектуальні системи підбору персоналу демонструють високу потенційну ефективність, їх практична реалізація потребує збалансування між рівнем автоматизації, фінансовими витратами та масштабом діяльності компанії. Саме тому в реальних умовах часто застосовуються гібридні підходи, які поєднують базові алгоритмічні механізми з частковою автоматизацією окремих етапів рекрутингу.

Водночас українські платформи пошуку роботи здебільшого реалізують алгоритмічні механізми фільтрації та сортування, а також базові рекомендаційні підходи без публічно задекларованого широкого використання складних AI-моделей. Однак поступово спостерігається тенденція до інтеграції більш просунутих інструментів аналізу даних та автоматизації рекрутингових процесів.

Загалом встановлено, що застосування технологій штучного інтелекту сприяє підвищенню точності підбору вакансій, зменшенню інформаційного перевантаження

користувачів і скороченню часу на пошук роботи. Разом із тим існують ризики алгоритмічної упередженості, залежності від якості навчальних даних, проблеми інтерпретації рішень моделей, а також питання забезпечення прозорості та етичності використання ШІ в рекрутингу.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати дослідження свідчать, що системи штучного інтелекту відіграють важливу роль у розвитку сучасних вебзастосунків пошуку роботи в IT, особливо у міжнародних платформах, таких як LinkedIn та Indeed. Встановлено, що застосування рекомендаційних алгоритмів, методів машинного навчання та обробки природної мови дозволяє підвищити точність підбору вакансій і зменшити інформаційне перевантаження користувачів.

Водночас українські платформи пошуку роботи, зокрема Djinni та DOU, переважно використовують базові алгоритмічні механізми фільтрації та сортування без широкого впровадження складних моделей штучного інтелекту.

Окремо запропоновано концепцію AI-агента для інтелектуального підбору персоналу, який поєднує аналіз внутрішніх HR-даних компанії та зовнішнього моніторингу ринку праці. Система формує узагальнений профіль «успішного працівника» на основі історичних корпоративних даних, аналізує вакансії та резюме кандидатів за допомогою методів машинного навчання та NLP-технологій, після чого формує рейтинг претендентів за ступенем релевантності.

Однак повна автоматизація процесів рекрутингу без участі людини може призводити до появи помилкових або упереджених рішень, оскільки якість роботи моделей залежить від обсягу та релевантності навчальних даних. Перспективним напрямом розвитку є підвищення прозорості алгоритмів, зменшення алгоритмічної упередженості та використання гібридної моделі прийняття рішень, у межах якої AI-система виступає інструментом підтримки HR-фахівців, а остаточний контроль рейтингу кандидатів здійснюється експертами.

Таким чином, застосування штучного інтелекту у вебзастосунках пошуку роботи в IT є перспективним напрямом розвитку цифрових сервісів, що потребує подальшого вдосконалення технологій аналізу даних, забезпечення етичності алгоритмів та оптимізації механізмів їх практичного використання.

ЛІТЕРАТУРА

1. Durgesh Kumar Kushwaha, Arora, L., Anand, A., None Riya, Sheth, D. and Khare, S. (2024). AI Powered Job Recommendation System, 295-299. URL: https://ieeexplore.ieee.org/document/10961440
2. Chen, Z. (2023). Ethics and Discrimination in Artificial intelligence-enabled Recruitment Practices. Humanities and Social Sciences Communications, 10(1), 1-13. URL: https://www.nature.com/articles/s41599-023-02079-x
3. Jaber, A.H. (2023). The method of building an intelligent system of recommendations for professional orientation. Optoelectronic Information-Power Technologies, 46(2), 22–36. URL: https://doi.org/10.31649/1681-7893-2023-46-2-22-36.



ПАВЛО МОСІЄНКО
студент 4 курсу бакалаврату Прикладне Програмування у Київському національному університеті імені Тараса Шевченка.
E-mail: pavelmosienkoj@gmail.com
Науковий інтерес полягає у сфері практичного застосування веб-технологій, зокрема розробці та дослідження вебзастосунків. Серед наукових інтересів — веб-технології, розробка вебзастосунків, тестування.

МЕТОД ПРОГНОЗУВАННЯ ТРАНСПОРТНОГО ТРАФІКУ В МІСТІ НА ОСНОВІ ВІДКРИТИХ ДАНИХ ТА ГІБРИДНИХ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Григорій Пономаренко, Мирослава Гладка

Анотація. *У роботі розглянуто метод прогнозування транспортного трафіку в міському середовищі з використанням відкритих даних та гібридних моделей машинного навчання. Актуальність дослідження зумовлена зростанням транспортного навантаження у великих містах і необхідністю впровадження інтелектуальних рішень у рамках концепції Smart City. Запропонований підхід поєднує статистичні методи аналізу часових рядів та нейромережеві моделі для підвищення точності коротко- та середньострокового прогнозування інтенсивності руху. Отримані результати можуть бути використані для підтримки прийняття рішень у системах управління міським транспортом.*

Ключові слова: транспортний трафік; відкриті дані; машинне навчання; гібридні моделі; Smart City.

I. ВСТУП

Інтенсивний розвиток міської інфраструктури та зростання кількості транспортних засобів призводять до ускладнення процесів управління дорожнім рухом. Затори, нерівномірне навантаження на транспортну мережу та підвищення рівня викидів шкідливих речовин є одним з основних проблем сучасних міст. У цьому контексті особливої актуальності набуває впровадження інтелектуальних транспортних систем, що є складовою концепції Smart City [1].

Одним із ключових елементів таких систем є прогнозування транспортного трафіку, яке дозволяє завчасно оцінювати навантаження на дорожню мережу та приймати обґрунтовані управлінські рішення. Складність прогнозування зумовлена нелінійною природою транспортних потоків, впливом часових, просторових та зовнішніх факторів. Використання відкритих даних у поєднанні з методами машинного навчання створює передумови для розроблення ефективних та масштабованих рішень у сфері міської транспортної аналітики [2].

II. ДАНІ ТА МЕТОДИ

У межах дослідження використовуються відкриті джерела даних, зокрема історичні показники інтенсивності транспортного руху, часові ряди швидкості потоків, а також допоміжні параметри, як час доби та день тижня. Застосування відкритих даних дозволяє мінімізувати витрати на збір інформації та забезпечити універсальність запропонованого підходу для різних міських середовищ [1, 2].

Перед використанням дані проходять етап попередньої обробки, що включає очищення від пропусків, нормалізацію значень та агрегування часових рядів. Для прогнозування транспортного трафіку запропоновано гібридний підхід, який поєднує класичні статистичні моделі аналізу із сучасними нейромережевими методами. Статистичні моделі дозволяють ефективно враховувати трендові та сезонні компоненти, тоді як рекурентні нейронні мережі типу LSTM забезпечують моделювання складних нелінійних залежностей у даних [2, 3].

Загальну структуру запропонованого методу прогнозування транспортного трафіку наведено на Рисунку 1. Метод передбачає послідовні етапи збору відкритих даних, їх попередньої обробки, формування ознак, навчання статистичної та нейромережевої моделей, а також об’єднання результатів прогнозування з використанням гібридного підходу.

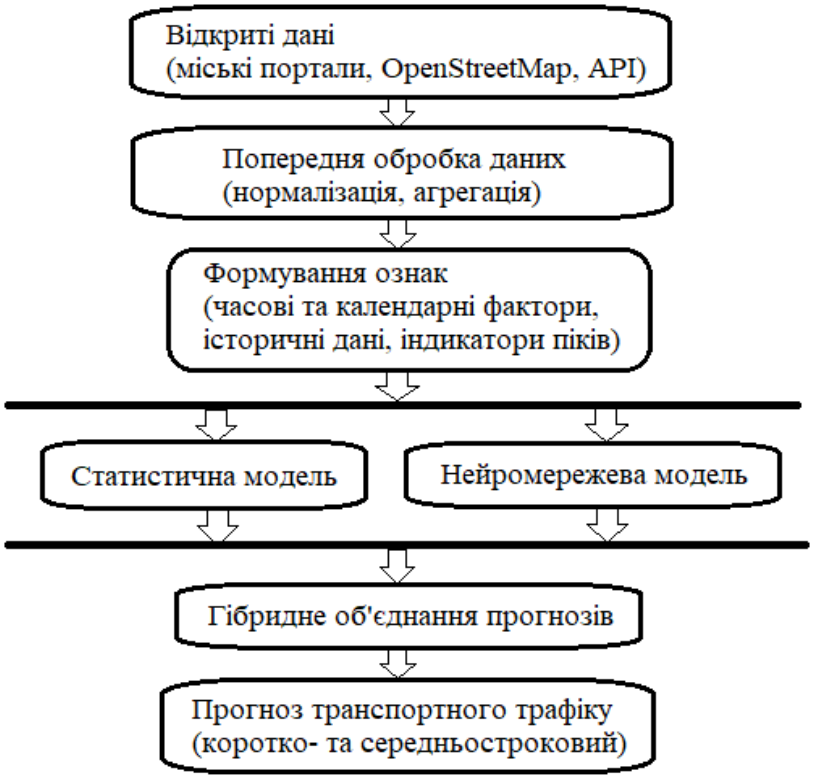


Рисунок 1. *Структурна схема методу прогнозування транспортного трафіку*

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Експериментальні дослідження показали, що застосування гібридної моделі прогнозування транспортного трафіку забезпечує підвищення точності результатів порівняно із застосуванням окремих статистичних або нейромережевих підходів [2, 3]. Зокрема, спостерігається зменшення похибки прогнозу в періоди пікового транспортного навантаження, які характеризуються високою динамічністю та нерівномірністю транспортних потоків, що є критично важливим для задач оперативного управління дорожнім рухом.

Аналіз отриманих результатів показав, що статистичні моделі ефективно відтворюють загальні тренди та сезонні коливання транспортного трафіку, проте демонструють обмежену точність у випадках різних змін інтенсивності руху. Нейромережеві моделі, зокрема мережі типу LSTM, навпаки, краще реагують на складні нелінійні залежності у часових рядах, однак можуть бути чутливими до шуму та обсягу навчальних даних [2].

Поєднання зазначених підходів у межах гібридної моделі дозволяє компенсувати їхні недоліки та забезпечити більш стабільні й узгоджені прогнози за різних умов функціонування транспортної мережі. Отримані результати підтверджують доцільність використання гібридних моделей для аналізу та прогнозування транспортних потоків у міському середовищі з високим рівнем варіативності дорожньої ситуації [1-3].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонований метод прогнозування транспортного трафіку на основі відкритих даних та гібридних моделей машинного навчання є перспективним інструментом для розв’язання задач інтелектуального управління транспортними системами сучасних міст. Поєднання статистичних та нейромережевих моделей дозволяє ефективно враховувати як довгострокові тренди й сезонні коливання транспортних потоків, так і короткострокові нелінійні зміни, характерні для міського дорожнього руху.

Результати дослідження свідчать, що використання гібридного підходу забезпечує підвищення точності прогнозування та стабільності отриманих результатів за умов змінної транспортної ситуації. Адаптивність запропонованого методу робить його доцільним для застосування в системах підтримки прийняття рішень у сфері міського транспорту, зокрема для оцінювання навантаження на дорожню мережу та планування транспортних процесів.

Подальші дослідження доцільно спрямувати на розширення набору вхідних даних, урахування просторово-часових залежностей між ділянками дорожньої мережі, а також на поглиблений аналіз впливу зовнішніх факторів, таких як погодні умови та соціально-економічні події, на формування транспортних потоків. Отримані результати можуть слугувати теоретичною основою для подальшого розвитку методів прогнозування транспортного трафіку в умовах концепції Smart City.

ДЖЕРЕЛА

1. Geng W., Pan Y., Xing Z., Liu D., Liu R., Zhu Y. (2025) MSCMHMST: A traffic flow prediction model based on Transformer
2. Yuan F., Fan Y., Bing X, Tian Z., Yuan C., Li Y. (2025) Traffic flow forecasting, STL decomposition, Hybrid model, LSTM, ARIMA, XGBoost, Intelligent transportation systems
3. Chen Y., Lu J. (2025) Research on traffic state prediction method based on traffic flow prediction under multi-time granularity



ГРИГОРІЙ ПОНОМАРЕНКО
студент 1 курсу магістратури програмних технологій Інтернету речей у Київському національному університеті імені Тараса Шевченка.
E-mail: greg.ponomarenko@gmail.com
Науковий інтерес зосереджений на дослідженні методів аналізу та прогнозування транспортного трафіку на основі відкритих даних і гібридних моделей машинного навчання. До кола дослідницьких зацікавлень належать інтелектуальні транспортні системи, а також застосування нейромережевих моделей у задачах Smart City.



МИРОСЛАВА ГЛАДКА
к.т.н., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-5233-2021
E-mail: myroslava.gladka@knu.ua
З 2004 року почала свою викладацьку кар’єру на посаді асистента кафедри інформаційних систем у Національному університеті харчових технологій. Паралельно з викладацькою роботою працювала на посадах аналітика, керівника проєктів, консультанта з впроваджень у провідних компаніях ІТ галузі. Досвід практичної роботи понад 10 років. Коло наукових інтересів: управління проєктами, моделювання та інжиніринг бізнес-процесів.

АРХІТЕКТУРНА МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОЇ АДАПТИВНОЇ ОСВІТНЬОЇ ПЛАТФОРМИ З БАГАТОРІВНЕВОЮ ПЕРСОНАЛІЗАЦІЄЮ

Богдан Скочинський

Анотація. *У роботі запропоновано інтегровану архітектурну модель інтелектуальної адаптивної освітньої платформи з багаторівневою персоналізацією на основі технологій штучного інтелекту. Архітектура поєднує модульний підхід, data-driven аналітику, AI-механізми прогнозування та оркестраційний контур узгодження алгоритмічних рішень із педагогічними цілями. Реалізовано замкнений адаптивний цикл та runtime-конфігурацію компонентів системи. Імітаційне моделювання підтвердило підвищення точності рекомендацій і оптимізацію освітніх траєкторій порівняно з традиційними LMS. Запропонований підхід може бути використаний при проєктуванні AI-driven навчальних платформ.*

Ключові слова: адаптивне навчання; архітектура освітніх систем; штучний інтелект; персоналізація; AI-driven платформи.

I. ВСТУП

Сучасні цифрові освітні середовища дедалі частіше стикаються з протиріччям між масовістю онлайн-навчання та потребою індивідуалізації освітнього процесу. З одного боку, платформи повинні забезпечувати масштабованість і стандартизованість контенту, з іншого – враховувати відмінності у рівні підготовки, темпі навчання, когнітивних особливостях та мотиваційних характеристиках здобувачів освіти [1]. Саме це протиріччя формує запит на системну інтеграцію технологій штучного інтелекту в архітектуру освітніх платформ.

Більшість існуючих адаптивних рішень обмежуються рекомендаційними алгоритмами або зміною складності завдань [2]. У таких системах персоналізація реалізується локально і не охоплює повністю логіку функціонування платформи [3]. Як наслідок, адаптивність виступає додатковим сервісом, а не фундаментальною властивістю системи.

II. ДАНІ ТА МЕТОДИ

В основу архітектури покладено ідею багаторівневої адаптації:

1. Контентна адаптація – підбір навчальних матеріалів відповідно до моделі знань користувача.
2. Сценарна адаптація – формування індивідуальної траєкторії проходження курсу.
3. Інтерфейсна адаптація – динамічна зміна способу подання інформації.
4. Конфігураційна адаптація – керування функціональністю системи в режимі виконання.

Такий підхід дозволяє перейти від реактивного реагування на помилки до проактивного керування навчальним процесом.

Запропонована модель включає п’ять функціональних шарів (рис. 1).

Шар взаємодії, який відповідає за персоналізовану комунікацію з користувачем. Тут інтегруються:

– адаптивна навігація;
– гейміфікаційні механізми;
– контекстні підказки;
– динамічне структурування матеріалу.

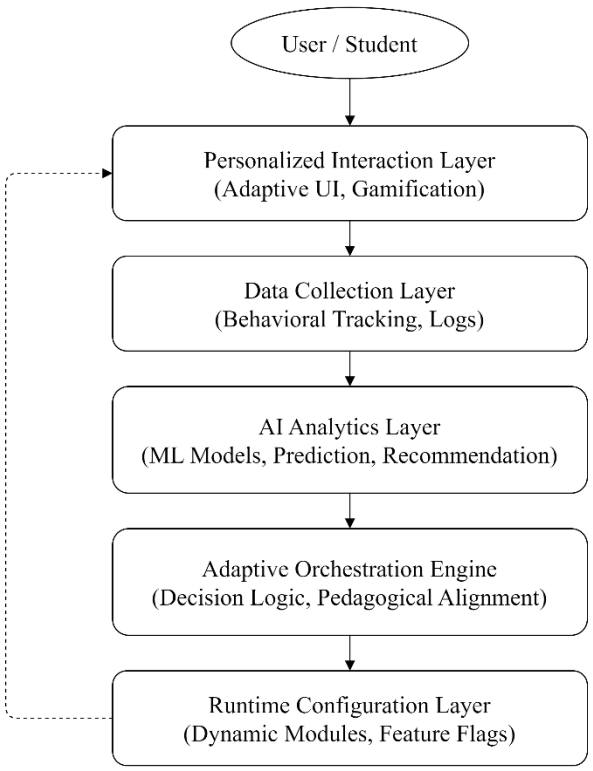


Рисунок 1. *Архітектурна модель інтелектуальної адаптивної освітньої платформи*

Шар збору та агрегації даних використовується для формування цифрового профілю навчальної активності і на якому фіксуються:

– результати виконання завдань;
– час реакції;
– повторні спроби;
– характер помилок;
– послідовність дій у середовищі.

Шар інтелектуальної аналітики, який реалізує алгоритми машинного навчання:

– моделі прогнозування успішності;
– рекомендаційні алгоритми;
– моделі виявлення ризику демотивації;
– оцінювання темпу засвоєння знань.

Ключовою характеристикою є можливість безперервного донавчання моделей на основі нових даних.

Шар адаптивної оркестрації, який є центральним координаційним компонентом архітектури. Його функції:

– узгодження результатів AI-аналізу з педагогічними цілями;
– визначення рівня складності завдань;
– формування освітніх сценаріїв;
– балансування навантаження та мотивації.

Запровадження оркестраційного шару дозволяє уникнути ситуації, коли алгоритмічні рішення суперечать дидактичній логіці.

Шар управління конфігурацією, який забезпечує гнучкість системи і дозволяє:

– змінювати активні механіки;
– тестувати різні освітні стратегії;
– адаптувати функціональність для різних груп користувачів;
– впроваджувати нові модулі без зупинки системи.

Порівняно з традиційними адаптивними системами запропонована архітектура має низку переваг:

- системність персоналізації – адаптація охоплює не лише контент, а й форму взаємодії;
- багаторівневість – реалізується контентна, сценарна, інтерфейсна та конфігураційна адаптація;
- масштабованість – модульна структура дозволяє інтегрувати нові AI-модулі без перебудови всієї системи;
- пояснюваність – оркестраційний шар дозволяє формувати обґрунтування прийнятих рішень;
- гнучкість експлуатації – runtime-механізми забезпечують швидку адаптацію до нових вимог.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті дослідження запропоновано інтегровану багаторівневу архітектурну модель інтелектуальної адаптивної навчальної платформи, у якій механізми персоналізації реалізовано як системну характеристику всієї архітектури. Адаптація здійснюється не лише на рівні добору навчального контенту, а й на рівні побудови освітніх сценаріїв, структурування траєкторії проходження курсу та динамічної модифікації інтерфейсу взаємодії. Це дозволяє враховувати не тільки рівень знань здобувача освіти, але й його темп навчання, стабільність результатів, типові помилки та поведінкові характеристики.

AI-модулі інтегровані у систему через спеціалізований оркестраційний механізм, який виконує роль узгоджувального контуру між результатами машинного аналізу та педагогічною логікою навчального процесу. Такий підхід мінімізує ризик прийняття ізольованих алгоритмічних рішень, що можуть суперечити дидактичним цілям або принципам послідовності навчання. Оркестраційний шар забезпечує адаптивне балансування складності завдань, інтенсивності подачі матеріалу та мотиваційних стимулів.

Використання runtime-конфігурації дозволяє здійснювати динамічну перебудову функціональності системи без припинення її роботи. Платформа підтримує активацію або деактивацію окремих модулів, зміну адаптивних стратегій та експериментальне впровадження нових механізмів персоналізації в режимі реального часу. Це підвищує гнучкість, масштабованість і придатність системи до впровадження в освітніх середовищах із різними вимогами.

З метою попередньої оцінки ефективності архітектури було проведено імітаційне моделювання адаптивного процесу навчання для трьох типів користувачів: з високим, середнім та початковим рівнем підготовки. У моделі порівнювалися два сценарії:

– традиційна LMS без багаторівневої адаптації;

– запропонована інтегрована AI-driven архітектура із замкненим адаптивним циклом.

Критеріями оцінювання виступали:

– середній час досягнення цільового рівня компетентності T;

– середня кількість повторних спроб виконання завдань R;

– точність рекомендацій навчальних матеріалів P_{rec};

– коефіцієнт стабільності прогресу S_{prog}.

Імітаційні результати показали:

– скорочення середнього часу досягнення цільового рівня на 12–18 % за рахунок проактивної корекції складності;

– зменшення кількості повторних спроб на 15–22 % завдяки точнішому підбору матеріалів;

– підвищення точності рекомендацій на 10–14 % у порівнянні з базовим rule-based підходом;

– зростання стабільності прогресу (зниження різких коливань результатів) приблизно на 8–11 %.

Основний внесок у покращення показників забезпечив оркестраційний шар, який координує AI-рішення з педагогічною логікою та не допускає різких змін складності. Runtime-конфігурація додатково дозволила оптимізувати стратегії адаптації для різних груп користувачів без зміни базової архітектури.

Отримані результати підтверджують, що інтеграція багаторівневої персоналізації та замкненого адаптивного циклу дозволяє не лише підвищити точність рекомендацій, а й оптимізувати загальну динаміку навчального процесу.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

На відміну від традиційних адаптивних систем, де персоналізація виступає окремим функціональним модулем, запропонований підхід розглядає адаптивність як базову архітектурну характеристику платформи. Введення шару адаптивної оркестрації дозволяє поєднати інструменти машинного навчання з дидактичними принципами, що підвищує узгодженість системи.

Практичне значення моделі полягає у можливості її використання при розробленні сучасних AI-driven освітніх платформ, систем дистанційного навчання та інтелектуальних тьюторських середовищ.

Перспективи подальших досліджень пов’язані з емпіричною верифікацією ефективності багаторівневої адаптації, впровадженням пояснюваного штучного інтелекту та розширенням механізмів аналітики освітніх даних.

ДЖЕРЕЛА

1. Gligorea, I., Cioca, M., Oancea, R., Gorski, A.-T., Gorski, H., & Tudorache, P. (2023). Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review. Education Sciences, 13(12), 2023, 1216. DOI: 10.3390/educsci13121216.
2. Kabudi, T., Pappas, I., Olsen, D. (2021) AI-enabled Adaptive Learning Systems: A Systematic Mapping of the Literature. Computers and Education: Artificial Intelligence. 2021, 2. 100017. 10.1016/j.caeai.2021.100017.
3. Abu Saa, A.; Al-Emran, M.; Shaalan, K. (2019). Factors afecting students’ performance in higher education: A systematic review of predictive data mining techniques. Technology, Knowledge and Learning, 24, 567–598. https://doi.org/10.1007/s10758-019-09408-7.



БОГДАН СКОЧИНСЬКИЙ
Аспірант Київського національного університету імені Тараса Шевченка, м. Київ, Україна
ORCID: 0009-0004-0603-8883
E-mail: bogdanskochynskyi@gmail.com
отримав ступінь бакалавра комп’ютерної інженерії у Національному авіаційному університеті (Київ, Україна) в 2012 році, ступінь магістра комп’ютерної інженерії за ОПП «Комп’ютерні системи і мережі» у Національному авіаційному університеті (Київ, Україна) в 2013, та ступінь магістра програмної інженерії за ОПП «Інженерія програмного забезпечення» у Національному авіаційному університеті (Київ, Україна) в 2023. Нині автор працює над здобуттям ступеня PhD зі спеціальності «Інформаційні системи та технології» у Київському національному університеті імені Тараса Шевченка (Київ, Україна). Серед наукових інтересів – адаптивні навчальні платформи, системи комп’ютерного моніторингу та контролю, системи контролю знань.

ЗАСТОСУВАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ РОЗКЛАДУ КОНСУЛЬТАЦІЙ ВИКЛАДАЧА

Олена Федусенко, Анатолій Федусенко

Анотація. *У роботі досліджено проблему автоматизації процесу формування розкладу консультацій викладачів у закладах вищої освіти на основі інтелектуальних методів. Обґрунтовано складність задачі як NP-повної задачі комбінаторної оптимізації, що зумовлене значною кількістю динамічних обмежень. Авторами запропоновано підхід до багатокритеріальної оптимізації розкладу консультацій із застосуванням генетичного алгоритму, що дозволяє одночасно враховувати нормативні вимоги та індивідуальні преференції учасників освітнього процесу. Описано трирівневу архітектуру інтелектуального застосунку та механізми еволюційної адаптації розкладу, що забезпечує раціональний розподіл ресурсів і зниження навантаження викладачів.*

Ключові слова: автоматизація розкладу, багатокритеріальна оптимізація, генетичний алгоритм, інтелектуальні системи, еволюційне моделювання, освітній менеджмент.

I. ВСТУП

Цифрова трансформація вищої школи потребує впровадження ефективних інструментів для управління часом усіх учасників освітнього процесу. Одним із найбільш трудомістких аспектів адміністрування є планування індивідуальних консультацій. Цей процес ускладнюється необхідністю вписування консультацій у вже існуючий розклад занять викладачів та студентів, врахуванням навчального навантаження та побажань викладачів. Традиційні методи ручного планування часто призводять до виникнення логістичних колізій та неефективного розподілу робочого часу викладача, що робить розробку спеціалізованих інтелектуальних застосунків критично важливою [1].

II. ДАНІ ТА МЕТОДИ

Для побудови ефективної моделі автоматизації розкладу консультацій було використано системний аналіз та методи еволюційного моделювання. Вхідними даними для системи слугують декілька масивів інформації: розклад академічних занять у форматі таблиць Excel, перелік робочих годин викладача, списки студентських груп та перелік навчальних дисциплін.

Методологія дослідження базується на формалізації задачі через систему обмежень:

Жорсткі обмеження визначають фізичну можливість проведення консультації. Вони включають недопустимість накладання консультації на лекційні чи практичні заняття як для викладача, так і для студента, а також обмеження щодо загальної кількості консультативних годин на тиждень згідно з нормами навантаження [2]. До сукупності жорстких обмежень моделі також включено умову детермінованості зв’язків у системі «викладач–студент», згідно з якою призначення консультації можливе лише за умови наявності встановленого академічного навантаження викладача за певною дисципліною у конкретній групі здобувачів освіти.

М’які обмеження відображають якісні показники розкладу. До них належать персональні преференції учасників (наприклад, бажані години проведення консультацій) та логіка «вікон» у розкладі, щоб уникнути надмірних перерв між заняттями.

Основним інструментом розв'язання задачі обрано генетичний алгоритм, який демонструє високу ефективність при роботі з NP-повними задачами комбінаторної оптимізації [4,5]. В основі алгоритму лежить ідея еволюційного пошуку, де кожен потенційний варіант розкладу розглядається як індивід (хромосома) у загальній популяції рішень [2].

Процес оптимізації реалізується через циклічне застосування генетичних операторів:

- Селекція: відбір найбільш придатних варіантів графіків на основі багатокритеріальної функції придатності, яка інтегрує ступінь задоволення всіх типів обмежень.
- Кросинговер: обмін структурними елементами між успішними варіантами розкладів для комбінування вдалих часових рішень.
- Мутація: випадкові точкові зміни в часових слотах окремих консультацій, що дозволяє алгоритму виходити з точок локального оптимуму та досліджувати нові ділянки простору пошуку.

Такий підхід дозволяє трансформувати суб'єктивні побажання учасників освітнього процесу в математично обґрунтований та логістично вивірений графік консультацій, що є критично важливим для ефективного управління часом як викладачів так і студентів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті проведеного дослідження було спроєктовано багаторівневу архітектуру інтелектуального застосунку, яка забезпечує повний цикл автоматизації: від збору первинних даних до динамічного коригування графіка в режимі реального часу. Функціональна структура системи представлена трьома логічними рівнями:

1. Рівень інтеграції та препроцесингу даних. На цьому етапі застосунок здійснює імпорт розкладу у форматі Excel та «очищення» часової сітки. Інтелектуальний застосунок автоматично ідентифікує вільні часові проміжки, де теоретично можливе призначення консультацій для конкретного викладача та відповідних студентських груп.
2. Рівень інтелектуальної генерації та багатокритеріального аналізу. Це ядро інтелектуального застосунку, де здійснюється запуск генетичного алгоритму. На цьому рівні проводиться зважена оцінка кожного варіанта розкладу за вектором критеріїв. Зокрема, алгоритм автоматично ранжує запити за їхньою важливістю: консультації з захисту кваліфікаційних робіт або підготовки до екзаменаційних сесій отримують найвищі пріоритетні коефіцієнти. Результатом роботи рівня є сформований набір оптимальних часових вікон, що мінімізують часові втрати викладача.
3. Рівень динамічної взаємодії. Цей рівень реалізовано через веб-інтерфейс, де студенти можуть обирати доступні слоти консультацій. Важливою особливістю є механізм «автоматичного ущільнення», а саме інтелектуальний застосунок в реальному часі аналізує тематику звернень: при реєстрації декількох осіб з однаковими запитами індивідуальна форма автоматично трансформується у групову консультацію. Це дозволяє уникнути дублювання інформації та суттєво оптимізує використання робочого часу викладача.

Аналіз запропонованого підходу показує, що автоматичне групування студентів за спільними дисциплінами дозволяє скоротити загальний час, витрачений на консультації, на 15-20%, одночасно підвищуючи охоплення аудиторії.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Впровадження інтелектуального застосунку, що базуються на еволюційних обчисленнях, дозволяє трансформувати традиційний статичний розклад консультацій у гнучке цифрове середовище, здатне до самоадаптації. На відміну від методів ручного планування, запропонована модель на основі генетичного алгоритму забезпечує системний підхід до вирішення конфліктів у розкладі, мінімізуючи вплив людського фактора та адміністративні помилки.

Проведений аналіз результатів свідчить, що багатокритеріальна оптимізація дозволяє досягти балансу між жорсткими нормативними вимогами навчального процесу та персональними інтересами викладачів і студентів.

Основною перевагою розробленого підходу є його здатність до швидкої реконфігурації при зміні вхідних умов (наприклад, перенесення основних занять або раптовій зміні доступності викладача). Механізми «інтелектуального ущільнення» запитів дозволяють зменшити часові витрати викладача.

ДЖЕРЕЛА

1. Федусенко О., Федусенко А. (2025) . Інтелектуальний застосунок формування розкладу консультацій викладача, Міжнародний науковий симпозіум «ІНТЕЛЕКТУАЛЬНІ РІШЕННЯ-С». Обчислювальний інтелект (результати, проблеми, перспективи). Теорія прийняття рішень: праці міжнар. наук. симпозіуму, 02 травня 2025 р.,с.86-89.
2. Снитюк В.Є., Сіпко О.М. (2022). Технологія еволюційного формування розкладів у закладах вищої освіти. Київ, Видавець: ФОП Піча Ю.В., 136 с..
3. Є. М. Федорченко, А. О. Олійник, О. О. Степаненко, Т. А. Зайко, К. В. Мєдвєдєв, Ю. В. Федорченко, Т. В. Федорончак, Т. О. Колпакова (2024). Генетичний метод розв’язання задачі складання розкладу навчальних занять, Реєстрація, зберігання і обробка даних, Т. 26, № 1, , с.9-23, DOI: 10.35681/1560-9189.2024.26.1.308332
4. Abdipoor S., Yaakob R., Goh S. L., Abdullah S. (2023) Meta-heuristic approaches for the University Course Timetabling Problem. Intelligent Systems with Applications Vol. 19. 200253 P.1-18. DOI: 10.1016/j.iswa.2023.200253
5. I. Gusti Agung Premananda, A. Tjahyanto and A. Muklason (2024) Timetabling Problems and the Effort Toward Generic Algorithms: A Comprehensive Survey, in IEEE Access, vol. 12, pp. 143854-143868, , doi: 10.1109/ACCESS.2024.3463721



ОЛЕНА ФЕДУСЕНКО
Доцент, кафедра інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна, Київ, Україна
ORCID: 0000-0002-5782-5922
E-mail: fedusenko@knu.ua
Отримала ступінь кандидата технічних наук у галузі інформаційних технологій у 2006 році. Є автором понад 70 наукових праць. До наукових інтересів належать системи адаптивного навчання, генетичні алгоритми та їх прикладне застосування, методи Data Mining.



АНАТОЛІЙ ФЕДУСЕНКО
військовослужбовець, Київ, Україна
ORCID: 0009-0008-8637-1262
E-mail: fantom_1973@ukr.net
Отримав ступінь кандидата технічних наук у галузі інформаційних технологій у 2016 році. Є автором багатьох наукових праць. До наукових інтересів належать генетичні алгоритми та їх прикладне застосування, методи Data Mining та візуалізації даних.

МЕТОД УНІФІКОВАНОЇ ІНТЕГРАЦІЇ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ У КРОСПЛАТФОРМНІ ПРОГРАМНІ СИСТЕМИ НА ОСНОВІ ONNX ТА КОНТЕЙНЕРИЗОВАНОГО INFERENCE

Даниіл Фуркало, Володимир Петрівський

Анотація. *У роботі запропоновано метод уніфікованої інтеграції моделей машинного навчання в кросплатформні програмні системи з використанням ONNX як єдиного представлення моделі та контейнеризованого серверного inference. Проведено експериментальне порівняння трьох сценаріїв розгортання (серверного, мобільного та веб-інференсу) за критеріями затримки, масштабованості та відтворюваності середовища. Визначено оптимальні стратегії розподілу inference між клієнтом і сервером.*

Ключові слова: ONNX, контейнеризація, кросплатформна архітектура, inference, MLOps.

I. ВСТУП

Стрімкий розвиток прикладних систем машинного навчання зумовив потребу у створенні універсальних підходів до розгортання моделей у гетерогенних середовищах виконання [1]. Сучасні програмні екосистеми передбачають одночасну підтримку мобільних клієнтів, веб-інтерфейсів і серверних обчислювальних потужностей, що формує складний інженерний ландшафт із різними обмеженнями ресурсів, вимогами до затримки та політиками безпеки. У цьому контексті особливої актуальності набуває проблема уніфікації представлення моделі та забезпечення її коректної роботи незалежно від платформи виконання. Дослідження спрямоване на формалізацію архітектурного шаблону, який дозволяє розгортати одну й ту саму ML-модель у середовищах Android, Web і Server без необхідності підтримки декількох ізольованих реалізацій.

Ключовим концептуальним положенням роботи є використання формату ONNX як центрального артефакту системи, що виступає спільною точкою інтеграції між різними середовищами виконання [2]. Підтримка ONNX-екосистеми, зокрема інструментів ONNX Runtime, які активно розвиваються за участі Microsoft, створює передумови для зниження інженерної складності портирування. У межах дослідження висувається гіпотеза, що ONNX-орієнтоване представлення здатне мінімізувати витрати на перенесення моделей без суттєвої втрати якості inference. Друга гіпотеза стосується ефективності гібридної стратегії, яка комбінує контейнеризований серверний inference із локальним виконанням на клієнтському пристрої з метою досягнення кращого балансу між latency та масштабованістю [3]. WebGPU - це сучасний веб-API для доступу до апаратного прискорення графіки та обчислень на GPU у браузерах. Зростання ролі браузерного inference та WebGPU також підтверджується сучасними дослідженнями у сфері in-browser обчислень [4], [5], [6].

II. ДАНІ ТА МЕТОДИ

Для дослідження була обрана модель для задачі класифікації зображень середнього розміру, навчена у середовищі PyTorch на стандартному наборі даних з 12 000 зображень, розподілених по 10 класах. Після завершення навчання модель була експортована у формат ONNX, що дозволило забезпечити платформонезалежне представлення і використання її у різних сценаріях виконання без повторного тренування [2].

Серверний сценарій передбачав розгортання моделі в Docker-контейнерах з використанням Kubernetes для масштабування та забезпечення стабільності інфраструктури.

Це дозволяло обробляти запити пакетами та ефективно використовувати ресурси CPU і RAM, зменшуючи загальну latency на запит.

Для мобільного сценарію використовувався Android-пристрій з ONNX Runtime Mobile. Локальний inference виконувався по одному зображенню за раз, що зменшувало мережеву затримку, проте обмежувало продуктивність через апаратні ресурси пристрою.

Веб-сценарій реалізовувався через браузер із WebGPU або WebAssembly-акселерованим виконанням. Такий підхід дозволяв обробляти запити локально, скорочуючи передачу даних на сервер, а апаратне прискорення WebGPU знижувало latency та покращувало стабільність обробки.

Було зібрано метрики latency (p50 та p95), загальний час обробки всього набору, а також споживання ресурсів та енергоспоживання для мобільного сценарію.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Як показано в Таблиці 1 відображає основні показники продуктивності трьох сценаріїв виконання ML-моделі на тестовому наборі з 12 000 зображень. Вона демонструє середню затримку обробки запиту (p50), затримку для 95-го перцентиля запитів (p95) та загальний час, необхідний для обробки всього набору.

Таблиця 1. *Порівняння сценаріїв розгортання ML-моделі*

Назва	**p50 (мс)**	**p95 (мс)**	**Час обробки 12 000 зображень**
Сервер	37	64	7.3 хв
Android	120	1204	24.4 хв
WebGPU	46	83	9.2 хв

Показник p50 (медіана) відображає типову затримку для половини запитів, тобто половина запитів обробляється швидше, а половина - повільніше. Показник p95 характеризує «хвіст» розподілу затримки і показує, що 95% запитів обробляються швидше зазначеного часу, а 5% можуть мати більші затримки. Ці метрики дозволяють оцінити не тільки середню продуктивність, але й стабільність і передбачуваність системи.

Як видно з таблиці, серверний сценарій має найнижчі значення p50 (37 мс) і p95 (64 мс), що свідчить про високу стабільність та передбачуваність обробки запитів. Завдяки пакетній обробці та паралельним потокам сервер зміг обробити весь набір за 7,3 хвилини, що є найкращим результатом серед усіх сценаріїв.

Android-сценарій має більшу середню затримку на один запит (p50 = 120 мс) та значно більшу варіативність (p95 = 1204 мс), що вказує на нерівномірну продуктивність при високих навантаженнях. Через обмежені ресурси пристрою повний прогін набору тривав 24,4 хвилини. Це показує, що локальне виконання ефективне для невеликих обсягів даних, але не масштабується на великі набори.

Технологія WebGPU, призначена для апаратного прискорення графічних і обчислювальних завдань у веб-браузерах, демонструє проміжні значення: p50 становить 46 мс, p95 - 83 мс, а повний прогін займає 9,2 хвилини. Це свідчить про те, що апаратне прискорення у браузері дозволяє скоротити час обробки і знизити варіативність, хоча досягти продуктивності серверного сценарію поки що неможливо через обмеження batch-обробки у WebGPU.

Таким чином, таблиця показує типовий компроміс між швидкістю окремого запиту, стабільністю системи та загальним часом обробки великого набору даних. Сервер оптимальний для пакетної обробки великих масивів даних, Android підходить для

локального виконання та швидкого отримання окремих результатів, а WebGPU забезпечує проміжний варіант із помірною latency та стабільністю.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати показали, що серверний сценарій обробляє запити швидко і стабільно, особливо для великих наборів даних. Android підходить для невеликих обсягів, але на великому наборі спостерігається велика різниця у часу обробки окремих запитів. WebGPU у браузері дає проміжний результат - обробка швидша, ніж на Android, але повільніша, ніж на сервері.

Таким чином, для пакетної обробки великих даних краще використовувати сервер, для швидкого локального отримання результату - Android, а WebGPU підходить для браузерних клієнтів із помірною швидкістю і стабільністю.

ДЖЕРЕЛА

1. MLR / Systematic reviews on MLOps practices (2023–2025). A Multivocal Review of MLOps Practices, Challenges and Solutions (2024–2025).
2. N. et al. (2023) A User Survey and Failure Analysis of ONNX Model Converters, arXiv (analysis of failures and pitfalls in converters).
3. R. Xue et al. (2025) HYBRIDSERVE: Efficient Serving of Large AI Models with Hybrid Model Serving, arXiv.
4. A. (2024) Empowering In-Browser Deep Learning Inference on Edge (nnJIT), arXiv (in-browser inference / JIT kernels).
5. Z. Chen (2025) Unleashing the Power of WebGPU on LLM Inference, ACM.
6. WebONNX / WONNX project (2025) - WebGPU-accelerated ONNX inference for web contexts (GitHub).



ДАНИІЛ ФУРКАЛО
Студент 3 курсу бакалаврату програмних систем і технологій у Київському національному університеті імені Тараса Шевченка, Київ, Україна
E-mail: daniilf077@knu.ua
Науковий інтерес полягає в області дослідження ефективних підходів до розгортання та використання моделей машинного навчання в різних програмних середовищах із забезпеченням їхньої продуктивності, стабільності та масштабованості.



ВОЛОДИМИР ПЕТРІВСЬКИЙ
PhD, асистент кафедри програмних систем і технологій у Київському національному університеті імені Тараса Шевченка, Київ, Україна
ORCID 0000-0001-9298-8244
E-mail: volodymyr.petrivskyi@knu.ua
Наукові інтереси: інженерія програмного забезпечення, оптимізація процесів різної природи, математичне моделювання.

ДОСЛІДЖЕННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ ПОПИТУ НА МОЛОЧНУ ПРОДУКЦІЮ

Катерина Чорнобай, Сергій Грибков

Анотація. *Досліджено методи прогнозування попиту молочної продукції. Проведено огляд та аналіз наукових джерел, присвячених підходам до прогнозування часових рядів, зокрема класичних статистичних моделей (ARIMA, GARCH, метод експоненційного згладжування Холта) та алгоритмів машинного навчання і глибокого навчання (LSTM, GRU, MLP, SVR, KNN, XGBoost). Обґрунтовано доцільність впровадження інтелектуальних систем прогнозування у системи підтримки прийняття управлінських рішень молокопереробних підприємств.*

Ключові слова: прогнозування попиту, машинне навчання, часові ряди, молочна продукція, нейронні мережі

I. ВСТУП

Виготовлення молочної продукції відноситься до п’ятірки провідних сільськогосподарських товарів та має стратегічне значення. Висока соціально-економічна значущість молочної галузі поєднується зі складністю управління виробничими та комерційними процесами, що зумовлено коротким терміном зберігання продукції, сезонністю надходження сировини, варіативністю попиту та багатономенклатурністю асортименту. За таких умов прогнозування обсягів готової молочної продукції набуває критичного значення для ефективного функціонування підприємства. Недостатня точність прогнозів призводить до перевиробництва та списання швидкопсувної продукції або, навпаки, до дефіциту та втрати ринкових можливостей, що безпосередньо впливає на фінансові результати та рівень конкурентоспроможності. На сьогодні актуальною науково-прикладною задачею є розроблення та впровадження сучасних інформаційних технологій прогнозування, заснованих на методах аналізу часових рядів, машинного навчання та інтегрованих систем підтримки прийняття рішень, що спрямовано на підвищення ефективності управління виробництвом, запасами та логістикою молокопереробних підприємств.

II. ДАНІ ТА МЕТОДИ

В роботі наведено результати аналізу, синтезу та абстрагування зарубіжних наукових джерел, що дало змогу окреслити ключові тенденції, підходи та напрями розвитку інформаційних технологій, перспективних для застосування при прогнозуванні попиту готової молочної продукції та усіх аспектів проходження пов’язаних бізнес-процесів. Проведений комплексний аналіз і узагальнення отриманих даних, що забезпечило систематизацію наявних наукових напрацювань, визначення актуальних проблем та обґрунтування перспектив подальших досліджень.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Доцільно виділити результати дослідження, присвячені висвітленню проблем прогнозування щомісячного виробництва коров'ячого сиру [1] де наводяться результати застосування моделей глибокого та машинного навчання, такі як GRU, LSTM, KNN, SVR та MLP. GRU (Gated Recurrent Unit) є різновидом рекурентної нейронної мережі, призначеної для моделювання послідовних даних із використанням механізмів керування внутрішнім

станом. Архітектура характеризується відносною обчислювальною ефективністю та здатністю відтворювати часові залежності при меншій кількості параметрів порівняно з іншими рекурентними моделями. LSTM (Long Short-Term Memory) є модифікованою рекурентною нейронною мережею зі спеціалізованою структурою пам'яті для збереження довгострокових залежностей. Модель мінімізує проблему зникнення градієнта та ефективно застосовується для аналізу складних часових послідовностей. KNN (K-Nearest Neighbors) є непараметричним алгоритмом машинного навчання, що здійснює класифікацію або регресію на основі близькості об'єктів у просторі ознак. Рішення формується шляхом аналізу k найближчих спостережень без побудови явної параметризованої моделі. SVR (Support Vector Regression) є методом регресійного аналізу, що базується на концепції опорних векторів і принципі структурної мінімізації ризику. Модель забезпечує ефективну апроксимацію як лінійних, так і нелінійних залежностей за рахунок використання ядрових функцій. MLP (Multilayer Perceptron) є багатошаровою нейронною мережею прямого поширення сигналу, здатною апроксимувати складні нелінійні функціональні залежності. Навчання здійснюється методом зворотного поширення помилки з використанням градієнтної оптимізації. Ефективність застосування моделі глибокого та машинного навчання підвержено на основі проведених досліджень на даних, зібраних за період з січня 2010 по вересень 2023 року взятих з Central Bank's EVDS Центрального банку Республіки Туреччина.

Робота [2] присвячена порівнянню та аналізу методів часових рядів для прогнозування, зокрема ARIMA та LSTM-мереж, у контексті задач прогнозування. ARIMA розглянуто як класичний статистичний метод, що моделює залежності у стаціонарних часових рядах через авторегресію та ковзне середнє. LSTM – як різновид рекурентних нейронних мереж, здатних захоплювати довгострокову пам'ять та нелінійні патерни. В роботі [2] обґрунтовано використання ARIMA для простих лінійних часових рядів, а LSTM-моделі більш ефективні у разі складної динаміки та складними зовнішніми впливами. Таким чином LSTM-моделі є більш ефективними для довгострокових прогнозів у випадках нелінійної залежності.

Порівняння моделей ARIMA/GARCH та лінійного підходу Холта здійснено для прогнозування виробництва молока в країнах Південної Азії (включаючи Китай) на основі щорічних даних з 1961 по 2018 рік в роботі [3]. Результати порівняння свідчать, що застосування комбінованого підходу ARIMA/GARCH забезпечує статистично та практично суттєво нижчий рівень середньої абсолютної відсоткової похибки порівняно з лінійною моделлю Холта. Отже, метод Холта демонструє вищі значення похибок прогнозування на даному наборі даних. Вищу адаптивність і точність мають моделі ARIMA/GARCH у порівнянні з простішою лінійною експоненційною моделлю при моделюванні довготривалих тенденцій виробництва молока в регіоні, що характеризується нелінійною динамікою.

У дослідженні [4] висвітлено актуальну науково-практичну проблему оптимізації управління ланцюгами постачання у молочній галузі шляхом імплементації методів машинного навчання для прогнозування попиту.

Наукова новизна дослідження полягає в теоретичному та прикладному обґрунтуванні переваг гібридного підходу, який забезпечує мінімізацію впливу сезонних коливань та скороченого терміну використання продукції, що підвищує точність прогнозування порівняно з класичними методами.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

В умовах сучасної цифрової трансформації молочної галузі перехід від традиційних статистичних методів до інтелектуальних систем прогнозування є стратегічною необхідністю. Адаптація досліджених методів до задач прогнозування попиту на молочну продукцію є науково обґрунтованою та практично доцільною. Найбільш ефективною видається стратегія використання адаптивних, нелінійних та гібридних моделей, здатних

забезпечити високу точність прогнозування в умовах динамічного та багатофакторного ринкового середовища.

Рекурентні нейронні мережі типу GRU та LSTM забезпечують високу ефективність у моделюванні часових залежностей різної тривалості. Їх здатність виявляти приховані нелінійні закономірності забезпечує підвищення точності прогнозів у середньо- та довгостроковій перспективі. Класичні статистичні моделі, зокрема ARIMA, GARCH, SARIMAX та метод експоненційного згладжування Холта, зберігають актуальність у випадках відносно стабільної структури попиту або за наявності переважно лінійних залежностей. За умов складної динаміки ринку, впливу макроекономічних чинників, змін споживчих переваг та сезонних коливань більш ефективними є нейромережеві або комбіновані підходи, які забезпечують нижчі показники прогнозної похибки.

Перспективним напрямом для прогнозування попиту на молочну продукцію є впровадження гібридних моделей, що інтегрують статистичні методи з алгоритмами машинного навчання (зокрема градієнтним бустингом). Такий підхід дозволяє одночасно враховувати трендові та сезонні компоненти часових рядів, а також складні нелінійні взаємозв'язки між попитом і зовнішніми факторами (ціновою політикою, доходами населення, логістичними обмеженнями тощо). Це особливо важливо для управління ланцюгами постачання швидкопсувної продукції, де точність прогнозу безпосередньо впливає на мінімізацію втрат і оптимізацію запасів.

ДЖЕРЕЛА

1. Gur, Y.E. (2024). Innovation in thedairy industry: forecasting cow cheeseproduction with machine learning anddeep learning models. InternationalJournal of Agriculture, Environment andFood Sciences, 8(2), 327-346.https://doi.org/10.31015/jaefs.2024.2.9
2. Shankar Vishnu S., Ajaykumar R., Ananthakrishnan S., Aravinthkumar A., Harishankar K., Sakthiselvi T., Navinkumar C. (2023). Modeling and Forecasting of Milk Production in the Western Zone of Tamil Nadu . Asian Journal of Dairy and Food Research. 42(3): 427-432. doi: 10.18805/ajdfr.DR-2103.
3. Mishra, P., Matuka, A., Abotaleb, M.S.A. et al. Modeling and forecasting of milk production in the SAARC countries and China. Model. Earth Syst. Environ. 8, 947–959 (2022). https://doi.org/10.1007/s40808-021-01138-z
4. Streefland, G., Herrema, F., & Martini, M. (2023). A Gradient Boosting model to predict the milk production. Smart Agricultural Technology.



КАТЕРИНА ЧОРНОБАЙ
здобувач ступеня доктора філософії, за спеціальністю 122 Комп'ютерні науки, кафедри Інформаційних технологій, штучного інтелекту і кібербезпеки Національного університету харчових технологій, Київ, Україна.
ORCID: 0000-0002-5627-4444
E-mail: chornobaiku@nuft.edu.ua
Наукові інтереси — розробка систем підтримки прийняття рішень.



СЕРГІЙ ГРИБКОВ
Д.т.н, професор, зав. кафедри Інформаційних технологій, штучного інтелекту і кібербезпеки Національного університету харчових технологій, Київ, Україна.
ORCID: 0000-0002-2552-2839
E-mail: sergio_nuft@nuft.edu.ua
Наукові інтереси — розробка систем підтримки прийняття рішень, мови програмування, розробка баз та сховищ даних, інтелектуальний аналіз даних, методи оптимізації системи.

ЖАНРОВА КЛАСИФІКАЦІЯ МУЗИЧНИХ КОМПОЗИЦІЙ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Антон Шаповалов, Ганна Красовська

Анотація. *У роботі розглянуто задачу автоматичної класифікації музичних композицій за жанром на основі методів машинного навчання. Запропоновано підхід до класифікації заснований на застосуванні моделі YAMNet та методу трансферного навчання. Результати експериментів підтвердили ефективність запропонованого підходу та можливість його використання для автоматизованого аналізу музичних даних.*

Ключові слова: машинне навчання, класифікація музичних композицій, аудіоаналіз, нейронні мережі, YAMNet, обробка аудіосигналів.

I. ВСТУП

Стрімкий розвиток цифрових музичних сервісів і стримінгових платформ призвів до значного збільшення обсягів аудіоконтенту, що зумовлює потребу в ефективних інструментах автоматизованого аналізу та структуризації музичних даних. Однією з базових характеристик музичної композиції є її жанрова приналежність, яка використовується для організації музичних бібліотек, навігації контентом та формування рекомендаційних систем.

Ручна класифікація музичних композицій є трудомісткою та суб'єктивною, тому сучасні системи використовують інтелектуальні методи обробки аудіоданих. Підходи до автоматичної класифікації музики базуються на алгоритмах машинного та глибинного навчання, що дозволяють аналізувати акустичні характеристики сигналу та визначати жанрову належність композиції [1]. Дослідження останніх років підтверджують активний розвиток методів жанрової класифікації на основі аналізу аудіосигналів та нейронних мереж [2].

Метою роботи є підвищення точності автоматичної жанрової класифікації музичних композицій з урахуванням обмежень обчислювальних ресурсів пристрою.

II. ДАНІ ТА МЕТОДИ

У дослідженні використано відкриті музичні датасети GTZAN та FMA, що містять аудіозаписи різних музичних жанрів. Вхідними даними системи є аудіофайли у форматах MP3, WAV або FLAC, які проходять попередню обробку та нормалізацію сигналу.

Процес автоматичної класифікації включає попередню обробку аудіосигналу, виділення аудіо-ознак та застосування моделі машинного навчання для визначення жанру композиції. Для аналізу використовуються спектральні характеристики сигналу, зокрема мел-кепстральні коефіцієнти (MFCC), що широко застосовуються у задачах музичної класифікації [3].

Для реалізації класифікації використано підхід трансферного навчання на основі архітектури YAMNet, поєднаної з багатошаровим перцептроном (Deep MLP). Використання попередньо навченої моделі підвищує ефективність виділення аудіо-ознак і зменшує обчислювальні витрати навчання системи [4].

Програмну реалізацію виконано у вигляді прогресивного веб-застосунку (PWA) із використанням бібліотеки TensorFlow.js, що дозволяє виконувати класифікацію безпосередньо на пристрої користувача без використання серверних обчислень.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті дослідження розроблено прототип програмного модуля, що реалізує повний цикл обробки аудіосигналу – від завантаження та попередньої обробки аудіофайлів до визначення жанрової належності композиції.

Проведені експериментальні дослідження показали, що запропонований підхід забезпечує ефективну класифікацію музичних композицій при помірному використанні обчислювальних ресурсів пристрою.

Під час тестування здійснено порівняння швидкодії системи з існуючими програмними рішеннями для жанрової класифікації музики. Отримані результати засвідчили, що використання легковагової моделі на основі трансферного навчання дозволяє скоротити час обробки аудіоданих і зменшити використання оперативної пам’яті, забезпечуючи водночас достатній рівень точності класифікації.

III. ВИСНОВКИ

Отримані результати підтверджують ефективність використання методів машинного навчання для задач автоматичної класифікації музичних композицій. Запропонований підхід дозволяє забезпечити баланс між точністю класифікації та використанням обчислювальних ресурсів пристрою.

Перспективним напрямом подальших досліджень є підвищення точності класифікації шляхом розширення навчальної вибірки та врахування додаткових музичних характеристик.

ДЖЕРЕЛА

1. Tzanetakis G., Cook P. (2002) Musical genre classification of audio signals. IEEE Transactions on Speech and Audio Processing, 10(5), 293–302. DOI: https://doi.org/10.1109/TSA.2002.800560
2. Shirol S., Kathiresan R. S. (2021) Machine learning based music genre classification with pre-processed feature analysis. International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 12 Issue 6, June-2023, pp. 183-192.
3. Ru G., Zhang X., Wang J., Cheng N., Xiao J. (2023) Improving music genre classification from multi-modal properties of music and genre correlations perspective. Available at: https://arxiv.org/abs/2303.07667 .
4. Islam M. S., et al. (2021) Machine learning-based music genre classification with pre-processed feature analysis. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), Vol. 7, No. 3, December 2021, pp. 491-502ISSN: 2338-3070, DO DOI: 10.26555/jiteki.v7i3.22327



АНТОН ШАПОВАЛОВ
студент 4 курсу бакалаврату освітньої програми «Комп'ютерні науки» у Київському національному університеті імені Тараса Шевченка.
E-mail: antonsapovalov0607@knu.ua
Студент Київського національного університету імені Тараса Шевченка.
Наукові інтереси – машинне навчання, аналіз аудіоданих та інтелектуальні методи класифікації.



ГАННА КРАСОВСЬКА
к.т.н., доцент, доцент кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-1986-6130
E-mail: hanna.krasovska@knu.ua
Наукові інтереси – інтелектуальні технології підтримки прийняття рішень, моделювання та аналіз складних систем.

ПРОГРАМНА СИСТЕМА ФОРМУВАННЯ НАВЧАЛЬНИХ НАБОРІВ ДАНИХ ДЛЯ СТРУКТУРНОЇ СЕГМЕНТАЦІЇ МУЗИЧНИХ СИГНАЛІВ

Дар'я Шкуратовська, Анастасія Ніколаєнко

Анотація. *У роботі розглядається проблема формування якісних навчальних вибірок для задач структурного аналізу музики. Запропоновано та реалізовано програмну систему, яка підтримує три підходи до автоматичної сегментації аудіосигналів: метод на основі функції новизни, алгоритмічну сегментацію із застосуванням бібліотечних засобів та нейромережеву модель, навчену на датасеті SALAMI. Система реалізує концепцію «людина в циклі», поєднуючи швидкість автоматизованої обробки з точністю експертної валідації. Результатом є структурований файл розмітки, придатний для навчання моделей у задачах класифікації та структурного аналізу музичних сигналів.*

Ключові слова: сегментація аудіосигналів; машинне навчання; розмітка даних; музичний аналіз; датасети.

I. ВСТУП

Зростання обсягів цифрового музичного контенту та розвиток методів машинного навчання зумовили підвищений інтерес дослідників до автоматизованого аналізу аудіосигналів. Однією з ключових задач у галузі пошуку музичної інформації (Music Information Retrieval, MIR) є сегментація музичних композицій – поділ аудіозапису на функціонально однорідні для подальшого аналізу [1].

Структурна розмітка є важливою для задач класифікації музичних жанрів, визначення повторюваних патернів, побудови рекомендаційних систем та навчання нейронних мереж. Однак більшість відкритих наборів аудіоданих не містять детальної сегментної розмітки, що ускладнює формування якісних навчальних вибірок. Проблема браку анотованих даних є одним із ключових обмежень у розвитку сучасних підходів до MIR-задач [2].

Наявні рішення здебільшого покладаються або на повністю ручну анотацію, яка є трудомісткою та погано масштабується, або на повністю автоматичну сегментацію, точність якої залишається недостатньою для формування еталонних вибірок [3]. Перспективним напрямом подолання цього протиріччя є напівавтоматичний підхід, що поєднує алгоритмічну обробку з експертною валідацією.

Метою роботи є вдосконалення процесу формування навчальних вибірок для задач комп'ютерного аналізу музики шляхом поєднання методів автоматичної сегментації аудіосигналів з концепцією інтерактивного експертного коригування визначених меж.

Для досягнення поставленої мети вирішуються такі завдання: огляд і порівняльний аналіз наявних підходів до сегментації музичного сигналу; реалізація різних алгоритмічних методів сегментації різного рівня складності; розроблення модуля ручного коригування розмітки; забезпечення експорту анотацій у форматах, придатних для навчання моделей.

II. МАТЕРІАЛИ ТА МЕТОДИ

Цифровий аудіосигнал доцільно розглядати як дискретний часовий ряд, що відображає зміну амплітуди звукової хвилі в часі. Його автоматизований аналіз ґрунтується на методах цифрової обробки сигналів (Digital Signal Processing, DSP) та процедурах виділення репрезентативних акустичних ознак. У сучасних дослідженнях задач сегментації музичного сигналу широко застосовуються часові, частотні та часо-частотні характеристики, зокрема: мел-частотні кепстральні коефіцієнти (MFCC), спектральна ентропія, спектральний центроїд, темпоральні характеристики сигналу, а також двовимірні подання у вигляді логарифмічних мел-спектрограм (log-mel) [1]. Останні є особливо ефективними при використанні глибоких

нейронних мереж, оскільки зберігають структурні закономірності сигналу у форматі, придатному для оброблення згортковими архітектурами [4].

Залежно від складності задачі та наявності розмічених даних, у MIR-дослідженнях застосовуються методи різних класів. Несупервізовані підходи – зокрема кластеризаційні алгоритми та методи на основі матриць самоподібності (Self-Similarity Matrix, SSM) – не потребують навчальних даних і надають можливість виявляти повторювані структурні блоки шляхом аналізу спектральної подібності фреймів [3, 5]. Ймовірнісні моделі, такі як приховані марковські моделі (Hidden Markov Model, HMM), моделюють послідовну природу музичного сигналу та дають змогу описувати переходи між структурними станами. Нейромережеві підходи – згорткові (CNN) та рекурентні (RNN/LSTM) архітектури – здатні автоматично навчатися ієрархічних представлень із розмічених даних і наразі демонструють найвищу точність у задачах сегментації [3, 6]. Трансформерні моделі з механізмом самоуваги (self-attention) є перспективним напрямом, що показує конкурентні результати в задачах аналізу довгострокових залежностей у музичному сигналі [4].

Для навчання та оцінювання моделей у дослідженнях структурної сегментації музики як еталонний набір даних (ground truth) зазвичай використовується корпус SALAMI (Structural Analysis of Large Amounts of Music Information). Цей датасет містить експертно анотовані часові межі структурних сегментів для понад 1300 музичних композицій широкого спектра жанрів [7]. Наявність такої репрезентативної вибірки забезпечує можливість навчання моделей у режимі контрольованого машинного навчання (supervised learning) та оцінювання точності алгоритмів сегментації за стандартизованими метриками.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У межах даного дослідження реалізовано програмну систему, яка підтримує три підходи до автоматичної сегментації музичного сигналу:

1) метод на основі функції новизни (Novelty-Based Approach),

2) алгоритмічну сегментацію із застосуванням спеціалізованої бібліотеки librosa,

3) застосування моделі машинного навчання, навченої на наборі даних SALAMI.

Перший підхід ґрунтується на виявленні різких змін спектральних характеристик сигналу. Після перетворення аудіоданих у спектрограму розраховується функція новизни, яка кількісно відображає ступінь відмінності між сусідніми часовими фреймами у вибраному ознаковому просторі. Локальні максимуми цієї функції інтерпретуються як потенційні точки структурних переходів, тобто межі сегментів. Перевагами методу є його обчислювальна ефективність, відсутність необхідності у попередньому навчанні та відносна простота реалізації.

Другий підхід реалізовано із застосуванням інструментів спеціалізованої бібліотеки обробки аудіоданих librosa. Використані алгоритми поєднують аналіз спектральних ознак, побудову матриць самоподібності (Self-Similarity Matrix, SSM) та методи кластеризації або виявлення структурних блоків. У межах дослідження цей варіант розглядається як базовий (baseline) для подальшої порівняльної оцінки якості сегментації.

Третій підхід передбачає використання моделі машинного навчання типу CRNN (Convolutional Recurrent Neural Network), навченої на структурно розміченому наборі даних SALAMI. Як вхідні ознаки використовуються спектральні подання сигналу – log-mel спектрограми або MFCC. Модель прогнозує ймовірність наявності межі сегмента для кожного часового фрейму, а отримані прогнози перетворюються у конкретні часові позиції шляхом аналізу локальних максимумів вихідної функції.

Розроблена програмна система реалізує повний цикл підготовки даних для задач сегментації музичного сигналу та забезпечує такі базові функціональні можливості:

- імпорт вхідних аудіоданих у поширених цифрових форматах (WAV, MP3) із попередньою перевіркою коректності зчитування;
- попередню обробку сигналу та обчислення необхідних акустичних ознак;
- ініціалізацію автоматизованого визначення структурних сегментів за вибраним алгоритмічним підходом;
- візуалізацію аудіосигналу з відображенням часових меж сегментів і можливістю їх експертного редагування;
- експорт сформованої розмітки у машинозчитувані формати (JSON, CSV) для подальшого використання під час навчання та тестування нейронних мереж.

Послідовність етапів запропонованого інтерактивного процесу наведено на рисунку 1. Для забезпечення високої якості навчальних вибірок система не обмежується автоматичною розміткою, а реалізує концепцію «людина в циклі» (human-in-the-loop). Після завершення етапу алгоритмічної сегментації в межах кожного з трьох підходів передбачено модуль ручного коригування визначених меж користувачем-експертом. Поєднання швидкості автоматизованої обробки з точністю експертної валідації дає змогу мінімізувати похибки та сформувати еталонну розмітку для подальшого навчання моделей у задачах класифікації та структурного аналізу музики.



Рисунок 1. *Блок-схема алгоритму розмітки аудіоданих*

Результатом роботи системи є структурований файл розмітки, що містить інформацію про кожен виділений структурний блок: часові мітки початку та завершення сегмента, його тривалість, а також додаткові метадані (за потреби). Сукупність отриманих файлів розмітки формує датасет, придатний для навчання та валідації моделей автоматичної структурної сегментації музики різних жанрів. Це визначає практичну цінність розробленої системи в контексті завдань комп'ютерного аналізу музичних сигналів.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Аналіз сучасних досліджень у галузі пошуку музичної інформації підтверджує, що хоча методи машинного та глибокого навчання демонструють високу точність у задачах аналізу аудіосигналів, їхня ефективність значною мірою залежить від наявності великих обсягів

якісно розмічених даних. Розроблений програмний комплекс вирішує проблему підготовки таких даних.

Використання виключно ручної розмітки є надто часозатратним, тоді як виключно автоматична розмітка не забезпечує достатньої точності для формування еталонних вибірок. Запропонована система поєднує швидкість трьох різних алгоритмічних підходів – від аналізу функції новизни до попередньо навчених ML-моделей – з точністю експертної валідації. Такий напівавтоматичний підхід дає змогу делегувати рутинний пошук первинних меж алгоритмам, залишаючи за експертом лише фінальне коригування результату.

У подальших дослідженнях планується проведення кількісного порівняльного аналізу точності реалізованих методів на матеріалі різних музичних жанрів. Окремим напрямом розширення системи є інтеграція сучасних трансформерних архітектур для підвищення точності автоматичного прогнозування меж сегментів.

ДЖЕРЕЛА

1. Lerch, A. (2022). An introduction to audio content analysis: Music Information Retrieval Tasks and Applications. John Wiley & Sons, 2nd edition, New Jersey, 464 p.
2. Ostermann, F., Vatolkin, I., Ebeling, M. (2023). AAM: a dataset of Artificial Audio Multitracks for diverse music information retrieval tasks. EURASIP Journal on Audio, Speech, and Music Processing, 2023:13, https://doi.org/10.1186/s13636-023-00278-7.
3. Salamon, J., Nieto, O., Bryan, N. J. (2021). Deep Embeddings and Section Fusion Improve Music Segmentation. In proceedings of the 22nd ISMIR Conference, Online, November 7-12, 2021, pp. 594-601.
4. Wu, S., Yu, D., Tan, X., Sun, M. (2023). CLaMP: Contrastive language-music pre-training for cross-modal symbolic music information retrieval. arXiv preprint arXiv:2304.11029, https://doi.org/10.48550/arXiv.2304.11029.
5. Wang, J. C., Smith, J. B., Lu, W. T., Song, X. (2021). Supervised metric learning for music structure features. arXiv preprint arXiv:2110.09000, https://doi.org/10.48550/arXiv.2110.09000.
6. Songailaitė, M. (2022). Encoding musical style using music information retrieval and deep learning methods (Doctoral dissertation, Vytautas Magnus university), 57 p. Available at: <https://www.vdu.lt/cris/bitstreams/978ceeab-b812-4a24-bb32-917da87b2e50/download> [Accessed 18 February 2026].
7. SALAMI Data Set version 2.0, Available at: <https://github.com/DDMAL/salami-data-public> [Accessed 18 February 2026].



ДАР'Я ШКУРАТОВСЬКА
Здобувач вищої освіти, кафедра програмних систем і технологій, Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID: 0009-0001-9276-7668
E-mail: shkuratovskadaria@knu.ua
Займається дослідженнями у сфері автоматичної сегментації аудіосигналів та формування навчальних датасетів для моделей машинного навчання. Наукові інтереси включають цифрову обробку сигналів, глибоке навчання та аналіз музичних структур.



АНАСТАСІЯ НІКОЛАЄНКО
Асистент кафедри програмних систем і технологій, Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID: 0000-0002-2402-2947
E-mail: n_nastja@knu.ua
Серед наукових інтересів – інформаційні технології, математичне моделювання, машинне та глибоке навчання.

СТОХАСТИЧНЕ МОДЕЛЮВАННЯ ФІНАНСОВИХ ЧАСОВИХ РЯДІВ: ВІД ГЕОМЕТРИЧНОГО БРОУНІВСЬКОГО РУХУ ДО НЕЙРОННОЇ ДИФУЗІЙНО-СТРИБКОВОЇ МОДЕЛІ

Юрій Юрченко, Олександр Заковортний

Анотація. *У роботі досліджено стохастичне моделювання фінансових часових рядів на основі стохастичних диференціальних рівнянь. На прикладі щоденних даних акцій SONY виконано порівняння геометричного броунівського руху, дифузійної моделі з нейромережевою апроксимацією коефіцієнтів та стрибково-дифузійної моделі з пуассонівською компонентою. Показано, що класична дифузійна модель не відтворює "товсті хвости" розподілу дохідностей, тоді як додавання стрибків і нейромережевої параметризації покращує узгодженість із реальними даними.*

Ключові слова: стохастичні процеси, геометричний броунівський рух, метрика надлишковий ексцес, нейронна мережа прямого поширення з повнозв'язними шарами, метрика Continuous Ranked Probability Score.

I. ВСТУП

Стохастичне моделювання є одним із ключових інструментів опису економічних і фінансових процесів, де спостереження містять як трендову(детерміновану), так і випадкову (невизначену) складові. Об'єктом дослідження виступають методи стохастичного моделювання для часових рядів фінансових цін, а предметом - їх порівняльний аналіз за статистичними критеріями якості. У якості даних використовуються часові ряди щоденних цін на акції корпорації SONY за 5 років (financialmodelingprep.com). Для побудови моделей використовується багатошарова нейронна мережа (MLP, fully-connected neural networks), що дозволяє апроксимувати нелінійні функції дрейфу та дифузії у стохастичному диференціальному рівнянні на основі емпіричних даних.

Фінансові часові ряди природно інтерпретуються як стохастичні процеси $\{X_t\}_{t\geq 0}$,. Математичною основою для опису таких процесів є стохастичні диференціальні рівняння (SDE). Центральним елементом є Вінерівський процес (або броунівський рух) W_t, який моделює неперервний випадковий ринковий шум. Загальна динаміка стохастичного процесу X_t описується стохастичним диференційним рівнянням(СДР) :

$$dX_t = a(X_t, t)\, dt + b(X_t, t)\, dW_t, \tag{1}$$

де $a(X_t, t)$ - функція дрейфу (детермінований тренд процесу),

$b(X_t, t)$- функція дифузії, (волатильність, що масштабує випадковий шум W_t).

Для вінерівського процесу характерні властивості $W_0 = 0$, незалежні прирости, $\Delta W \sim \mathcal{N}(0, \Delta t)$, тобто $\mathrm{Var}(\Delta W) = \Delta t$, а типовий масштаб приросту - $\sqrt{\Delta t}$. Ці базові властивості стохастичного числення є стандартним фундаментом для стохастичних фінансових моделей [2].

У прикладних задачах економіки/фінансів аналітичний розв'язок СДР майже ніколи не відомий. Тому на практиці широко застосовуються чисельні методи імітації траєкторій "крок за кроком" у дискретному часі (симуляція сценаріїв), що робить можливим оцінювання й порівняння моделей на реальних даних.

Однак емпіричний аналіз фінансових часових рядів, зокрема логарифмічних дохідностей акцій, свідчить про наявність дискретних "стрибків" — аномальних раптових коливань. Такі стохастичні процеси мають великі ексцеси (показник, що характеризує

"хвостатість" та піковість розподілу ймовірностей відносно нормального розподілу), які не відтворює модель броунівського руху, представлена формулою 1, і для їх моделювання варто розглядати Jump-Diffusion модель [1]. В ній використовується пуассонівський процес N_t з інтенсивністю λ. Підсумовуючи, пропонується сфокусуватися на стохастичній моделі, що враховує і детермінований процес (дрейф) і гладку дифузію броунівського руху і "стрибки" (jumps):

$$dX_t = a(X_t, t)dt + b(X_t, t)\, dW_t + X_t(Y-1)dN_t \quad (2)$$

де N_t Пуассонівський процес з інтенсивністю λ (частота стрибків),

Y — розмір стрибка.

Таким чином задача побудови стохастичної моделі вимагає пошуку коефіцієнтів дрейфу та дифузії. У класичних стохастичних моделях фінансових процесів (зокрема GBM – модель геометричного броунівського руху) коефіцієнти дрейфу та дифузії зазвичай вважаються сталими або мають наперед задану функціональну форму. Такий підхід забезпечує аналітичну зручність, однак істотно обмежує здатність моделі відтворювати реальні ринкові явища — нелінійність, режимні зміни волатильності, асиметрію реакцій на шоки та залежність параметрів від поточного стану ринку. Емпірично встановлено, що фінансові часові ряди характеризуються часовою змінністю волатильності (volatility clustering), структурними зламами та нелінійними залежностями, які не можуть бути адекватно описані моделлю з постійними коефіцієнтами.

Використання нейронних мереж для апроксимації дрейфу $a(x,t)$ та дифузії $\mathrm{b}(x,t)$ дозволяє перейти від параметричної моделі з фіксованою структурою до гнучкої функціональної апроксимації. З математичної точки зору нейронна мережа виступає універсальним апроксиматором неперервних функцій, що дає змогу наближати невідомі нелінійні залежності без явного задання їх аналітичної форми.

У межах першого етапу дослідження доцільно використовувати дифузійну модель, у якій коефіцієнти дрейфу $a(x,t)$та дифузії $b(x,t)$ апроксимуються простими багатошаровими перцептронами (MLP, fully-connected neural networks).

Такий вибір є методологічно обґрунтованим: MLP є універсальним апроксиматором неперервних функцій, що дозволяє моделі адаптивно відтворювати нелінійні залежності без явного задання їх аналітичної форми. У контексті стохастичних диференціальних рівнянь це означає, що замість припущення про сталий або лінійний дрейф і волатильність ми дозволяємо цим величинам бути нелінійними функціями стану процесу, зберігаючи при цьому дифузійну структуру шуму.

У сучасних роботах Neural SDE саме така архітектура використовується як базова конфігурація для фінансових застосувань [2],

II. ДАНІ ТА МЕТОДИ

Експерименти виконано на основі щоденних даних цін закриття акцій SONY за 5 років із ресурсу Financial Modeling Prep (у вибірці: 1254 ціни, 1253 лог-доходності). Емпіричний аналіз та калібрування моделей у цьому дослідженні базуються на використанні безперервно нарахованих (логарифмічних) дохідностей $r_t = ln\, S_t - ln\, S_{t-1}$. Вибір цієї метрики замість абсолютних рівнів цін обґрунтований низкою фундаментальних властивостей. По-перше лог-дохідності є строго адитивними в часі, що забезпечує інваріантність до початкового масштабу ціни. По-друге такі ключові факти фінансових ринків, як надлишковий ексцес та феномен «важких хвостів», за своєю природою є характеристиками розподілу ймовірностей саме відносних змін, а не самих цін. Отже, зіставлення емпіричних та симульованих

розподілів лог-дохідностей слугує найбільш статистично коректним критерієм адекватності моделей. Загальна стратегія експериментів - поступове ускладнення моделі:

МОДЕЛЬ "GBM"

Як базова дифузійна модель згідно формули 1 в спрощеному вигляді $dX_t=\mu dt+\sigma dW_t$, де параметри розраховуються, використовуючи формули:

$$\hat{\mu} = \frac{1}{dt} \cdot \bar{r};\ \hat{\sigma} = \sqrt{\frac{1}{dt} \cdot \widehat{Var}(r_t)} \tag{3}$$

Тобто в цій моделі параметри розраховуються без використання машинного навчання, а базовим статистичними методами. Такий підхід має обмеження - передбачає нормальний розподіл приростів цін.

МОДЕЛЬ "MINIMAL NEURAL SDE"

Як базовий підхід, для параметризації коефіцієнтів дрейфу та дифузії використано дві окремі прості багатошарові повнозв'язні нейронні мережі прямого поширення. Кожна мережа має два входи — поточне значення лог-ціни X_tта нормований час t, два приховані шари з нелінійністю гіперболічного тангенса та один вихідний нейрон. Мережа для дрейфу повертає дійсне значення $a(X_t, t)$, тоді як мережа для дифузії додатково застосовує функцію Softplus до виходу, що гарантує додатність волатильності $b(X_t, t) > 0$. Таким чином, зберігається гаусівський характер шуму (як в "GBM"), але коефіцієнти стають нелінійними та стан-залежними модель краще враховує динаміку фінансового процесу.

МОДЕЛЬ "NEURAL JUMP-DIFFUSION"

Модель із дифузійною (гаусівською) складовою, доповнена стрибковим компонентом, що моделюється пуассонівським процесом. Пошук очікуваної кількості стрибків на рік (λ), виконувався за допомогою методу максимальної правдоподібності (MLE). Знайдене значення λ приблизно 8 стрибків порядок величини узгоджується з тим, що реальний ринок акцій має обмежену кількість подій підвищеної турбулентності протягом року.

Чисельна симуляція траєкторій виконується методом Ейлера–Мураями- стандартною дискретизацією СДР. Цей метод природно узгоджується з властивістю $\Delta W \sim \mathcal{N}(0, \Delta t)$і є базовим інструментом симуляцій у стохастичному моделюванні.

Оцінка моделей здійснюється наступним чином: для симульованих лог-дохідностей обчислюються оцінки середнього μ та стандартного відхилення σ з метою перевірки відтворення дрейфу і волатильності.

Проте для фінансових рядів цього недостатньо, оскільки їх характерною рисою є "товсті хвости". Тому ключовим критерієм виступає ексцес: якщо він близький до нуля, модель не відтворює екстремальні коливання; додатний ексцес свідчить про здатність описувати рідкісні ринкові шоки.

Інструментом перевірки гіпотези про ідентичність розподілів двох стохастичних рядів використовується тест Колмогорова-Смірнова (KS-тест). Для оцінки "середнього сценарію" використовується метрика RMSE (Root Mean Squared Error), що вимірює квадратичну відстань між реальними лог-цінами та усередненим ансамблем симульованих траєкторій. Оскільки фінансове прогнозування має ймовірнісний характер, важливо оцінювати не лише "середній сценарій", а весь ансамбль можливих траєкторій. Для цього застосовується метрика CRPS (Continuous Ranked Probability Score), яка вимірює відстань між прогнозним розподілом і фактичним спостереженням.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У дослідженні виконано 10 000 симуляцій траєкторій для кожної моделі з метою забезпечення статистичної стабільності оцінок високих моментів розподілу, а для обчислення ансамблевої ймовірнісної метрики CRPS використано 2 000 траєкторій, що є достатнім компромісом між обчислювальною складністю та точністю оцінки розподілу прогнозу [4].

Таблиця 2.*Результати порівняння якості трьох стохастичних моделей*

Модель	**Середнє μ, ст.відх. σ (реальні дані проти симуляцій)**	**Ексцес (fat tails)**	**KS-тест (реальні дані проти симуляцій)**	**CRPS**	**RMSE**	**Обчислю-вальна складність**
GBM	μ розбіжності, σ добре узгоджується	≈ 0 не відтворює 'важкі хвости'	p = 0.037 значні відмінності від реальних даних	0.009756 базова якість	0.2068 велике відхилення	дуже швидка (≈40 с)
Minimal Neural SDE	μ, σ ближчі до реальних	≈ 0 не відтворює 'важкі хвости'	p ≈ 0.050 помірні відмінності від реальних	0.009700 трохи краще за GBM	0.0624 значне покращення	дуже повільна (≈1300 с)
Neural Jump-Diffusion (λ=8/рік)	μ, σ найбільш наближені до реальних	≈ 2.84 відтворює fat tails (близько до real=2.19)	p = 0.442 статистично узгоджена	0.009610 найкраща	0.0489 найменша помилка	(≈980 с) вища, тому що стартує з копіювання вже навчених мереж з попередньої моделі

IV. ВИСНОВКИ

У роботі порівняно три підходи до стохастичного моделювання фінансових часових рядів: класичний геометричний броунівський рух, його нейромережеву модифікацію та модель зі стрибковою компонентою. Встановлено, що дифузійні моделі (GBM і Minimal Neural SDE) коректно відтворюють середнє та волатильність лог-дохідностей, однак не здатні описати “товсті хвости” розподілу. Використання MLP, як базової архітектури нейронної мережі було зумовлене необхідністю підтвердження гіпотези про те, що нелінійна параметризація коефіцієнтів дрейфу та дифузії не є достатньою умовою для відтворення емпіричного ексцесу фінансових активів. Додавання пуассонівських стрибків суттєво покращує узгодженість моделі з емпіричними даними: відтворюється позитивний ексцес, покращуються результати KS-тесту та CRPS. Це свідчить про необхідність врахування рідкісних, але значних шоків для адекватного опису фінансових процесів. Отримані

результати підтверджують доцільність використання гібридних моделей із нейромережевою параметризацією та стрибковими механізмами для більш реалістичного моделювання фінансових часових рядів. Перспективи подальших досліджень пов’язані з розширенням структури шуму(наприклад, процес Леві), урахуванням складнішої динаміки волатильності, використання більш складних моделей машинного навчання.

ДЖЕРЕЛА

1. Shuya Kanagawa, Narn-Rueih Shieh. (2024) On an asset model of Merton type: long-term observations in financial time-series. *Journal of Stochastic Analysis,* Vol. 5, No. 4 (2024) Article 1. p.1,2 DOI: 10.31390/josa.5.4.01, URL: https://repository.lsu.edu/josa/vol5/iss4/1
2. Cuchiero Ch., Flonner E., Kurt K. Robust financial calibration: a Bayesian approach for neural SDEs. (2024), p.24. URL: https://doi.org/10.48550/arXiv.2409.06551.
3. Програмний код досліджень і результати симуляції, URL: https://github.com/u75u275/3model_IST_KNU_2026-.git
4. Masaki Adachi, et al. Fixing the Pitfalls of Probabilistic Time-Series Forecasting Evaluation by Kernel Quadrature. Proceedings of the 1st International Conference on Probabilistic Numerics 2025, Sophia Antipolis, France. p.4. URL: https://doi.org/10.48550/arXiv.2503.06079.



ЮРІЙ ЮРЧЕНКО
аспірант 2 курсу, кафедра "Комп'ютерна інженерія та програмування", Національний технічний університет "Харківський політехнічний інститут"
ORCID: 0009-0002-4489-1434
E-mail: Yurii.Yurchenko@cs.khpi.edu.ua
працює над дисертацією за темою "Використання методів глибокого навчання для стохастичного моделювання при створенні фінансового плану".



ОЛЕКСАНДР ЗАКОВОРОТНИЙ
доктор технічних наук, професор, лауреат Національної премії України імені Бориса Патона, завідувач кафедри комп’ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут"
ORCID: 0000-0003-4415-838X
E-mail: Oleksandr.Zakovorotnyi@khpi.edu.ua
штучні нейронні мережі, обчислювальний інтелект, методи й алгоритми прийняття рішень, математичне моделювання.

Section

Cognitive modeling and knowledge engineering

Секція

Когнітивне моделювання та інженерія знань

ABOUT ONE RECOMMENDATION MODEL FOR DATA PREDICTION BASED ON FUZZY LOGIC

Eugene Ivokhin, Glib Shelyakin

Abstract. *The article proposes a model for presenting data in recommendation systems, which is based on the implementation of fuzzy logic in the collaborative filtering method to improve the quality of personalized recommendations. Particular attention is paid to the problems of data sparsity, uncertainty of user ratings, and subjectivity of interpretation of criteria, which traditionally complicates the work of classical recommendation algorithms. The study substantiates the feasibility of using personalized triangular membership functions, which allow reflecting the personal preferences and evaluation characteristics of each user. A formalized procedure for constructing and dynamically updating the parameters of such functions for all evaluation criteria is proposed.*

Keywords: fuzzy logic, Mamdani method, collaborative filtering, data sparsity, uncertainty, fuzzy numbers.

I. INTRODUCTION

The generation of recommendations in modern recommender systems is based on various approaches, each of which involves the analysis of large volumes of information. Traditional methods are typically focused on precise numerical values, which does not always reflect real-world conditions, where user ratings and item properties are often vague, partially defined, or incomplete. To make well-founded decisions under such conditions, it is advisable to apply approaches based on fuzzy logic. The introduction of fuzzy logic into recommendation systems makes it possible to formally process uncertainty and inaccuracy in both the input data and the inference rules, to build logically consistent conclusions, and organize and structure the relationships between factors and recommendations, taking into account the limitations and specifics of the available information. In particular, the use of fuzzy models makes it possible to assess the degree of similarity between users based on fuzzy criteria of their preferences or behavior patterns rather than rigid ones.

II. DATA AND METHODS

The use of fuzzy numbers and fuzzy relations in conditions of situational or informational uncertainty makes it possible to construct fuzzy inference schemes, within which logical conclusions are formed based on a system of fuzzy rules and operations on fuzzy values in order to obtain target (output) values, and the combination of fuzzy logic tools with basic collaborative filtering methods contributes to the formation of more accurate and transparent personalized recommendations, especially in conditions of incomplete or fragmentary data with a high level of inaccuracy (uncertainty). This approach creates additional opportunities to improve the quality of recommendation systems and increase their effectiveness [1].

Taking into account the positive impact of fuzzy logic on the recommendation generation process, it is proposed to apply the Mamdani method [2] to compute the degree of similarity between users, which makes it possible to account for the fuzziness of ratings and to ensure well-grounded recommendation prediction.

III. RESULTS AND ANALYSIS

To validate the proposed approach, an artificial test dataset was created consisting of 7 users, 3 evalation criteria, 2,100 user-object ratings, and 6,300 criterion-based ratings. The use of generated data made it possible to fully control the structure of the sample, the level of sparsity, and

to repeat the experiment under identical conditions. First, a set of users and a set of objects that they could rate were formed. For each “user-object” pair, a rating was generated with a certain probability, which allowed the desired level of filling of the rating matrix to be specified. Rating values were generated in the range from 1 to 5, taking into account possible differences in user preferences and object characteristics. Separately, for each object, the values of the criteria by which it is evaluated were generated, and these criteria were used as input data for constructing personalized fuzzy membership functions. As a result, a model dataset was obtained that reproduces a typical information structure of recommender systems: a set of users, a set of objects, a partially filled rating matrix, and descriptive object criteria. This made it possible, under controlled conditions, to study the operation of the model, verify its ability to process sparse and partially uncertain data, and assess the impact of the proposed fuzzy mechanisms on recommendation quality. Three metrics were used for comparison: MSE, RMSE, and SSE. All of them reflect the error between predicted and actual ratings, where lower values indicate better model performance.

IV. DISCUSSION AND CONCLUSION

In this work, a modification of the naive collaborative filtering method was proposed by introducing elements of fuzzy logic, which allowed for the consideration of additional evaluation criteria for objects and the construction of a more flexible model of user preferences. A comparative experiment was conducted on an artificially generated dataset that reproduces the typical structure of information in recommendation systems, comparing the naive method with the proposed approach.

The results of the numerical experiments showed that even under conditions of artificially generated data, where the relationship between the criteria and user ratings does not fully reflect real behavioral patterns, the modified approach demonstrated a reduction in error values compared to the naive method. This indicates the potential effectiveness of incorporating evaluation criteria and using fuzzy membership functions to improve recommendation quality. At the same time, these results should be regarded as a conservative estimate of the model’s capabilities, since the absence of real correlations in synthetic data partially limits the advantages of the modified approach.

REFERENCES

1. Івохін Є.В., Шелякін Г.В. (2025) Застосування нечіткої логіки у реалізації методики колаборативної фільтрації. Artificial Intelligence, 3, 63–77.
2. Mamdani E. (1974). Application of Fuzzy Algorithms for Control of Simple Dynamic Plant. Proceedings of the IEEE, 121(12), 1585-1588.



EUGENE IVOKHIN
Dr.Sci., professor of intellectual program systems department of computer science and cybernetics faculty, National Taras Shevchenko university of Kyiv, Kyiv, Ukraine
ORCID: 0000-0002-5826-7408
E-mail: ivohin@knu.ua
Research interests include optimization models and methods, decision support systems, fuzzy sets.



GLIB SHELYAKIN
PhD-student of computer science and cybernetics faculty, National Taras Shevchenko university of Kyiv, Kyiv, Ukraine
ORCID: 0009-0002-7171-6535
E-mail: shelyakingleb17@gmail.com
Research interests include optimization models, recommendation systems, fuzzy sets and logic.

CONSIDERING PSYCHOLOGICAL CHARACTERISTICS OF STUDENTS FOR ADAPTIVE E-LEARNING

Mykola Kostikov, Vladlen Lisnevskyi

Abstract. *The paper analyzes the role of psychological characteristics in adaptive e-learning systems. A student model incorporating cognitive parameters, including individual forgetting rate, is proposed. The study reviews modern approaches to modeling memory decay and knowledge tracing and demonstrates how psychological parameters can complement data-driven models. The proposed approach may improve the personalization of learning trajectories and optimize repetition scheduling in foreign language learning systems.*

Keywords: e-learning, forgetting curve, forgetting rate, knowledge modeling, knowledge tracing, learning and forgetting, memory decay.

I. INTRODUCTION

Modern requirements for university education necessitate improving the efficiency of foreign language teaching, particularly by considering the individual and psychological characteristics of students. However, most e-learning tools do not sufficiently adapt the educational process to the level of training, native language, goals, and cognitive characteristics.

II. DATA AND METHODS

The study examines the application of information technology in foreign language learning. An analysis of existing approaches to creating a student model is conducted, in particular accounting for the level of knowledge, native language, learning goals, and psychological characteristics. Sources describing the modeling of the forgetting process during learning are also reviewed. Simulation modeling was used to evaluate the model efficiency.

III. RESULTS AND ANALYSIS

Analysis of modern e-learning tools for foreign languages has shown that most of them present the educational material without individualization. Each user follows the same learning trajectory and studies the same topics at a standard pace, regardless of their previous learning outcomes, individual characteristics, and interests.

As for educational systems including a student model, they usually record only the current level of knowledge, but psychological characteristics are rarely taken into account. This limits the possibility of building an adaptive learning trajectory.

At the previous stage of the study, it was proposed to use a comprehensive student model [1] to eliminate these shortcomings. This model combines the following groups of indicators:

- subject knowledge (knowledge levels for individual learning elements);
- knowledge in related areas (native language, level of proficiency in other languages);
- learning goals (specialty, interests, desired knowledge level);
- psychological characteristics (type of thinking, forgetting rate).

The current study focused on the last group of indicators, particularly on the forgetting process and its modeling.

When a student works with an e-learning tool, such parameters can be determined at the initial stage through testing. Later, during the learning process, these values can be refined depending on the results of the student's work.

It is well known that for better memorization, information must be repeated regularly. This is confirmed by many studies, including modern ones. The forgetting curve, known since 1885, remains one of the fundamental concepts in instructional science, although the technology and means of study have changed much over time.

The research [2], which focused on studying mathematics, proved the effectiveness of regular repetition of educational material in preventing forgetting of basic concepts.

Paper [3] also studies spaced repetition and proposes using an LSTM neural network for predicting the probability of remembering an information item. The authors mention language learning as one of the areas where spaced repetition works particularly well.

However, it is important to note that the process of learning and forgetting occurs differently for different people. Therefore, to increase the effectiveness of repetition, individual characteristics of students should be taken into account.

In [4], the functions of memory and forgetting in deep knowledge tracing models were investigated, and various mathematical models of memory decay were compared.

Study [5] introduces a forgetting factor that simulates the forgetting behavior in the learning process. This research applies the Transformer model for knowledge tracking.

The authors of [6] used the forgotten erasing function and the forgotten retention function to model knowledge loss. Here, the passage of time and previous learning activities are taken into account to determine the optimal moment for repeating the material.

The research [7] proposes a personalized forgetting mechanism. The authors state that existing knowledge tracing models based on the forgetting curve theory only consider the general forgetting caused by time intervals, ignoring the individualization of students and the causal relationship of the forgetting process.

Modeling the forgetting process during grammar learning was described in [8]. The simulation modeling of this system showed that predicting the level of knowledge to determine the points of repetition helps reduce the total time for mastering the material and increases the efficiency of learning grammar rules.

Thus, recent studies confirm the growing interest in modeling the dynamics of knowledge retention and forgetting in adaptive learning systems. Modern approaches (such as deep knowledge tracing and memory-decay modeling) focus primarily on analyzing behavioral data obtained during interaction with the learning system.

However, in many cases, the parameters of these models are derived only from observable learning actions and do not explicitly incorporate psychological characteristics of the learner.

The proposed student model complements these approaches by introducing psychological parameters, including the individual forgetting rate, as explicit elements of the learner profile. Such parameters can serve as initial conditions or additional variables for knowledge-tracing and memory-decay models, enabling more accurate prediction of knowledge retention and optimal scheduling of learning repetitions.

Consequently, integrating psychological characteristics into the student model may enhance the adaptability of e-learning systems and improve the efficiency of foreign language acquisition, particularly in areas such as grammar learning, where regular reinforcement of knowledge plays a crucial role.

IV. DISCUSSION AND CONCLUSION

The conducted analysis demonstrates that effective e-learning systems should take into account not only the current level of students' knowledge but also the cognitive and psychological characteristics that influence the learning process.

Incorporating psychological characteristics, particularly the individual forgetting rate, into the student model can enhance the adaptability of e-learning systems. Such integration allows the

learning environment to personalize the presentation and repetition of educational material according to the learner's cognitive features and learning goals.

Further research may focus on empirical validation of the proposed model in real e-learning environments, refining psychological parameters used in student modeling, and integrating these parameters with modern machine-learning-based knowledge-tracing methods.

The combination of psychological modeling and data-driven approaches may provide a promising direction for the development of adaptive educational systems.

REFERENCES

1. Костіков М. П., Гуржій А. М. (2015) Модель студента для експертно-навчальної системи граматики іноземної мови, Вісник Кременчуцького нац. ун-ту ім. Михайла Остроградського, вип. 6 (95), с. 125–129.
2. Lindquist D. S., Sparrow B. E., Lindquist J. M. (2024) Spaced recall reduces forgetting of fundamental mathematical concepts in a post high school precalculus course, Instructional Science, vol. 52, pp. 859–878. DOI: https://doi.org/10.1007/s11251-024-09680-w.
3. Pokrywka J., Biedalak M., Graliński F., Biedalak K. (2023) Modeling Spaced Repetition with LSTMs, Proceedings of the 15th International Conference on Computer Supported Education, vol. 2: CSEDU, pp. 88–95. DOI: 10.5220/0011724000003470.
4. Sha A., Gu Z., Nunes B. P. (2026) Is there a better way to forget? Modelling memory decay in deep knowledge tracing, Knowledge-Based Systems, vol. 332, 114884. DOI: https://doi.org/10.1016/j.knosys.2025.114884.
5. Liu T., Zhang M., Zhu C. et al. (2023) Transformer-based convolutional forgetting knowledge tracking, Scientific Reports, 13, 19112. DOI: https://doi.org/10.1038/s41598-023-45936-0.
6. Ma F., Zhu C., Lei P., Yuan P. (2025) Enhanced Learning Behaviors and Ability Knowledge Tracing, *Applied Sciences*, *15*(2), 883. DOI: https://doi.org/10.3390/app15020883.
7. Wang S., Hu Y., Yang X., Zhang Z., Wang K., Zhang X. (2024) Personalized Forgetting Mechanism with Concept-Driven Knowledge Tracing : arXiV preprint. URL : arXiv:2404.12127v2. DOI: https://doi.org/10.48550/arXiv.2404.12127.
8. Костіков М. П. (2017) Моделювання самонавчання зі змінним інтервалом часу між заняттями, Матер. 83 міжнар. наук. конф. молодих учених, аспірантів і студ. «Наукові здобутки молоді — вирішенню проблем харчування людства у XXI столітті», 5–6 квітня 2017 р., ч. 2, с. 294.



MYKOLA KOSTIKOV
PhD, Doc., associate professor at the Dept. of information systems and technologies Taras Shevchenko National University of Kyiv, Ukraine
ORCID: 0000-0002-1569-8179
E-mail: Kostikov@knu.ua
BSc (2009) and MSc (2010) in computer science, PhD (2016) in information technology (National University of Food Technologies). Teaches NLP, programming, and computer science. Scientific interests: computational linguistics; e-learning (foreign languages); API.



VLADLEN LISNEVSKYI
PhD student at the Dept. of psychology Taras Shevchenko National University of Kyiv, Ukraine
ORCID: 0009-0004-5488-1111
E-mail: vladlen2000@ukr.net
Achieved a bachelor's degree in sociology (2021) and master's degree in psychology (2023) from Taras Shevchenko National University of Kyiv, Ukraine. Scientific interests: addiction psychology; macroeconomics.

IDENTIFYING RESEARCHERS' SCIENTIFIC AREAS BASED ON PUBLICATION CLUSTERING

Alisher Shaimuran

Abstract. *This paper presents a reproducible method for identifying researchers' scientific areas from a publication corpus using a hybrid "text + graph" pipeline and cluster analysis. The core components are contextual document embeddings of scientific texts (SciBERT/SPECTER), dimensionality reduction (UMAP), density-based clustering (HDBSCAN), and topic interpretation via c-TF-IDF with representative publication exemplars. To ensure practical usability, we propose a mixed evaluation protocol: internal cluster-structure quality metrics combined with an expert audit of the produced topic labels. The output is a set of coherent thematic clusters and a visual analytics layer that supports author profiling, detection of topic shifts over time, and identification of interdisciplinary transitions.*

Keywords: scientific publications; embeddings; SPECTER; SciBERT; UMAP; HDBSCAN; c-TF-IDF; author profiling; topic clusters.

I. INTRODUCTION

Digital libraries and academic indexes have evolved into large-scale knowledge graphs describing papers, authors, organizations, venues, and their relationships. In this context, mapping research areas, detecting communities, and automatically profiling researchers are shifting from manual procedures to data-driven pipelines. Classical bibliometric techniques (co-citation, bibliographic coupling, co-word mapping) remain useful, but at modern scale they often suffer from terminology drift, noisy metadata, and limited ability to capture the "hidden" semantics of short abstracts.

The practical question is: how can we reliably and interpretably reconstruct an author's research areas from their publication trail—while accounting for temporal dynamics (topic transitions, emergence of new areas) and without depending on rigid, hand-crafted vocabularies?

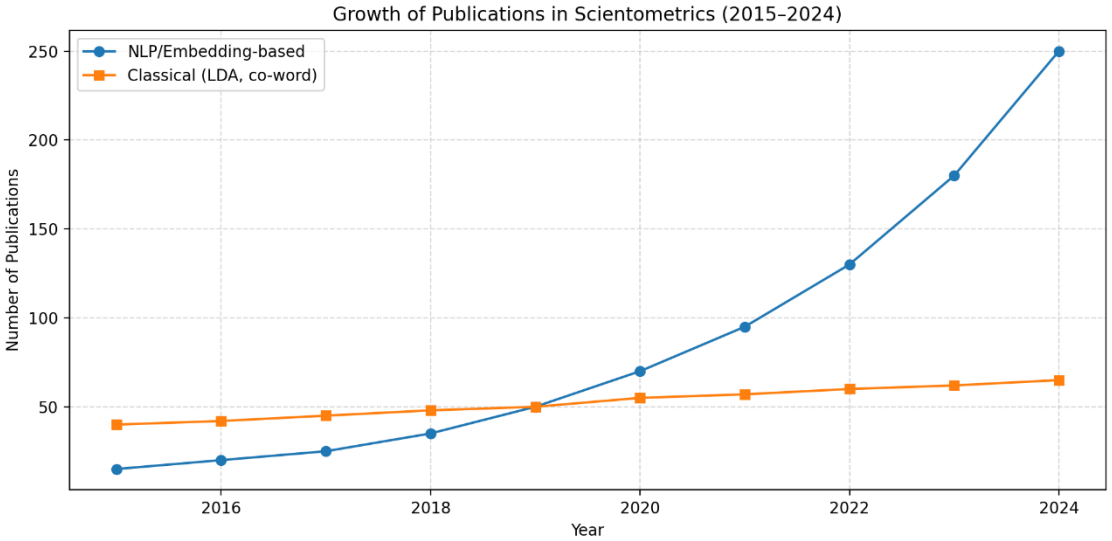


Figure 1. *Growth in the number of publications using embeddings compared with classical approaches (2015–2024, example)*

II. HYPOTHESES AND SCIENTIFIC NOVELTY

The report formulates three hypotheses that shape the system design. H1: a hybrid pipeline that combines document embeddings (including citation-informed representations) with density-based clustering yields more coherent and robust clusters than purely lexical features. H2: explicit treatment of time (clustering by temporal slices / dynamic modeling) improves longitudinal author profiles and makes topic drift observable. H3: a mixed evaluation protocol (metrics + expert audit of interpretations) provides higher validity than relying on metrics alone.

The novelty of the proposed approach lies in combining: (i) contextual document representations with graph signals (citations / co-authorship), (ii) transparent cluster interpretation via c-TF-IDF and exemplar sets, (iii) robustness checks as a criterion for selecting model configurations, and (iv) a reproducible package of artifacts (configs, fixed random seeds, and scripts for visualization).

III. METHOD

The method is implemented as a pipeline suitable for large and heterogeneous corpora (e.g., OpenAlex), where missing abstracts and disciplinary imbalance are common. The input consists of publication metadata (title, abstract, keywords, year, links/citations).

The pipeline stages are: 1) Preprocessing: text normalization, duplicate filtering, lightweight token cleanup; when available—enrichment with concepts/keywords. 2) Representation: computing document embeddings (SciBERT as a text-only baseline encoder and SPECTER as a variant that implicitly accounts for citation context). 3) Dimensionality reduction: UMAP to preserve local neighborhood structure prior to clustering. 4) Clustering: HDBSCAN, which is robust to noise, can identify clusters of arbitrary shape, and flags outliers. 5) Topic interpretation: c-TF-IDF computed over cluster documents (unigrams/bigrams), selection of the most representative publications, and assembling an “explanation panel” for each cluster.

At the author level, results are aggregated into topic distributions by year, dominant research areas, inter-cluster topic transitions, and short profile tags derived from c-TF-IDF weights. This supports narrative reports suitable for internal university reporting and expert review.

IV. EXPERIMENTS AND RESULTS

The practical evaluation is described on a 10,000-paper Computer Science subcorpus. Two encoders were compared: SciBERT and SPECTER; dimensionality reduction and clustering parameters were then fixed (UMAP: n_neighbors=30, min_dist=0.1; HDBSCAN: min_cluster_size=150).

Cluster quality was assessed using standard internal metrics and topic coherence. In the report, the numeric values below are presented in a demonstrational form (to illustrate the reporting format).

Table 1. *Comparison of clustering quality for different embeddings (example)*

Metric	SciBERT (baseline)	SPECTER (hybrid)	Change
Silhouette (higher is better)	0.32	0.41	+28%
Davies–Bouldin (lower is better)	1.85	1.42	-23%
Topic Coherence C_v (higher is better)	0.48	0.56	+16%

Improvements in Silhouette and Topic Coherence alongside a lower Davies–Bouldin score match H1: adding a citation-aware signal makes thematic groups denser and better separated. During interpretation, we also observed terminology drift after 2022 in the LLM/GenAI topic, consistent with H2 about the dynamic nature of the thematic landscape.

After dimensionality reduction (UMAP) and density-based clustering (HDBSCAN), thematic groups were interpreted via c-TF-IDF (unigrams/bigrams) and by selecting representative publication exemplars. Below is a typical slice of the resulting structure (example for n=10,000 papers).

Table 2. *Summary characteristics of topic clusters (example)*

No.	Cluster name	Size	Key terms (c-TF-IDF)
1	LLM & Generative AI	1,420 (14.2%)	transformer; alignment; fine-tuning; instruction; RLHF
2	Graph Neural Networks	980 (9.8%)	GNN; message passing; homophily; graph convolution; node classification
3	Natural Language Processing / IR	2,160 (21.6%)	NLP; information retrieval; question answering; language model; tokenization
—	Other clusters	4,690 (46.9%)	computer vision; recommender; security; optimization; databases
—	Noise (outliers)	750 (7.5%)	—

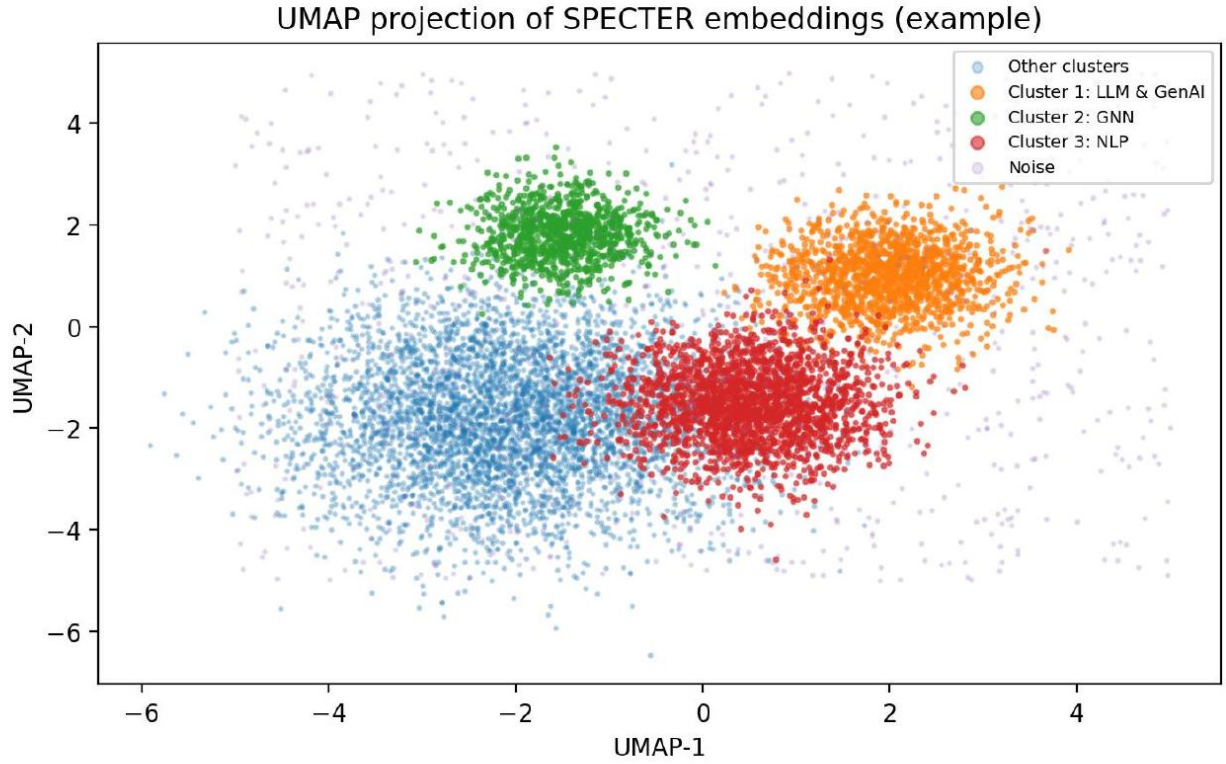


Figure 2. *2D projection of SPECTER embeddings (UMAP) and HDBSCAN cluster visualization (example)*

V. ROBUSTNESS ASSESSMENT AND EXPERT AUDIT

To test reproducibility of the cluster structure, a bootstrap analysis was performed (B=30). The variability of the reported metrics was approximately σ≈0.04, which is interpreted as acceptable robustness under resampling. Next, a human-in-the-loop audit of interpretations was conducted: two experts independently evaluated the correctness of the automatically generated labels (based on the top 10 most representative publications per cluster). Agreement with the labels reached 74% with a target threshold of 70%, supporting H3 and the need for mixed evaluation.

VI. VISUAL ANALYTICS AND AUTHOR PROFILES

Beyond aggregate metrics, practical value comes from visual representations that turn clustering output into user-friendly "stories". At the author level, we generate: (i) topic distributions by year, (ii) a graph of topic transitions (e.g., a Sankey diagram), and (iii) a ranked list of characteristic profile tags based on c-TF-IDF weights.

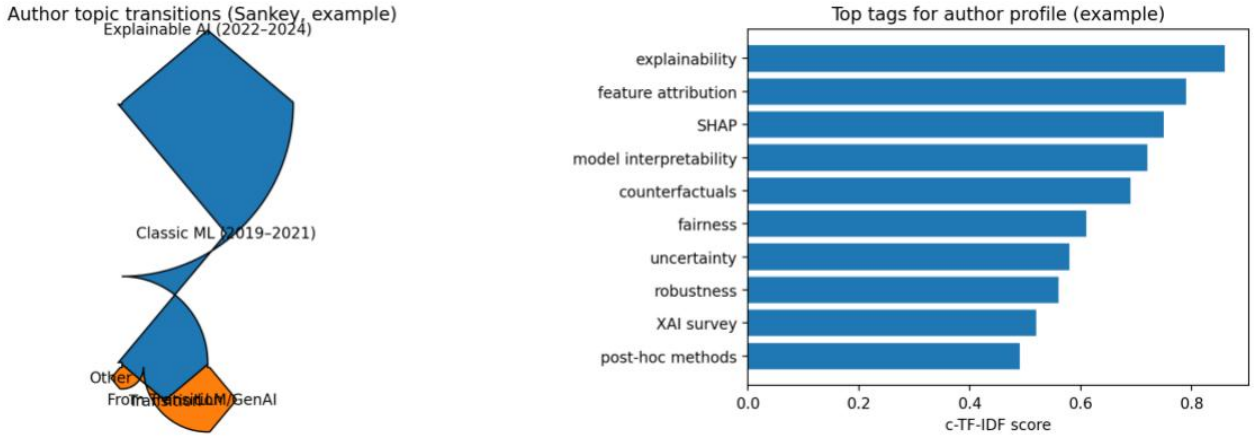


Figure 3. *Example author profile: topic transitions (Sankey) and top profile tags (c-TF-IDF)*

VII. LIMITATIONS AND FUTURE WORK

Key limitations are related to metadata completeness (quality of abstracts, keywords, and references), errors in deduplication and author disambiguation, disciplinary imbalance, and potential bias when using citation signals. The report proposes mitigation measures: year-normalized citation features, robustness checks (bootstrap/sensitivity), conservative cluster interpretation, and mandatory documentation of data-processing procedures and ethical assumptions.

Future work includes expanding the corpus, transferring the approach to other domains, deeper error analysis (mixed clusters and overlap between sub-topics), and developing dynamic models for stable tracking of how research interests evolve over time.

VIII. CONCLUSION

The proposed method combines modern document embeddings, dimensionality reduction, and density-based clustering with interpretable topic labeling and expert validation. In the experimental setup described in the underlying R&D report, citation-aware scientific encoders (e.g., SPECTER-like models) produced more coherent and stable thematic groups than general-purpose baselines, which supports the feasibility of automated research-area reconstruction from publication text and metadata.

Key contributions of the work can be summarized as follows:

- An end-to-end, reproducible pipeline for preprocessing publications, generating document representations, reducing dimensionality (UMAP), and extracting clusters (HDBSCAN) suitable for heterogeneous scholarly corpora.
- A comparative evaluation of multiple representation choices (classical TF–IDF topic features vs. transformer-based scientific embeddings), including internal cluster validity metrics and topic coherence checks.
- A robustness layer based on resampling/bootstrapping and an expert audit protocol to verify interpretability and to flag mixed or unstable clusters.
- A visual analytics output that converts cluster structure into practical author profiles, enabling trend tracking, topic transitions, and compact “profile tags”.

From a practical standpoint, the resulting profiles can support expert finding, team formation, collaboration recommendations, portfolio monitoring for research groups, and lightweight scientometric reporting. The approach is especially useful when an organization needs consistent, explainable summaries across many researchers and rapidly growing publication streams.

At the same time, several limitations remain important. The quality of inferred topics depends on metadata completeness (abstract availability, keyword quality, and reference coverage), and author name ambiguity can distort profiles when disambiguation is imperfect. Density-based clustering can also produce small “micro-topics” or merge nearby themes if the corpus is sparse or the embedding space is noisy; therefore, parameter sensitivity analysis and human-in-the-loop review remain advisable for high-stakes use cases.

Future work should prioritize: (i) stronger author disambiguation and affiliation normalization; (ii) dynamic/temporal topic modeling to better represent topic shifts across years; (iii) tighter integration of citation graphs (graph embeddings or GNNs) to capture influence and methodological lineage; and (iv) multilingual support to include non-English publications without losing topic coherence. These extensions would make the system more robust for cross-domain and cross-lingual deployments.

Overall, the study shows that combining scientific-text embeddings with density-based clustering and interpretable labeling is a viable foundation for identifying scientific research directions at the scholar level, while keeping the results transparent enough for expert validation and downstream decision-making.

REFERENCES

1. Beltagy I., Lo K., Cohan A. (2019). SciBERT: A Pretrained Language Model for Scientific Text. EMNLP-IJCNLP.
2. Cohan A. et al. (2020). SPECTER: Document-level Representation Learning using Citation-informed Transformers. ACL.
3. McInnes L., Healy J., Melville J. (2018). UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction.
4. McInnes L., Healy J., Astels S. (2017). hdbscan: Hierarchical density based clustering. JOSS.
5. Grootendorst M. (2022). BERTopic: Neural topic modeling with a class-based TF-IDF procedure.
6. Devlin J., Chang M.-W., Lee K., Toutanova K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. NAACL-HLT.
7. Reimers N., Gurevych I. (2019). Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. EMNLP-IJCNLP.
8. Gu Y. et al. (2021). Domain-Specific Language Model Pretraining for Biomedical Natural Language Processing (PubMedBERT). ACL.

9. Salton G., Buckley C. (1988). Term-weighting approaches in automatic text retrieval. Information Processing & Management.
10. Blei D. M., Ng A. Y., Jordan M. I. (2003). Latent Dirichlet Allocation. Journal of Machine Learning Research.
11. Ester M., Kriegel H.-P., Sander J., Xu X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise (DBSCAN). KDD.
12. Campello R. J. G. B., Moulavi D., Sander J. (2013). Density-Based Clustering Based on Hierarchical Density Estimates (HDBSCAN foundations). PAKDD.
13. MacQueen J. (1967). Some Methods for Classification and Analysis of Multivariate Observations (k-means). Proc. 5th Berkeley Symposium on Mathematical Statistics and Probability.
14. Rousseeuw P. J. (1987). Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. Journal of Computational and Applied Mathematics.
15. Davies D. L., Bouldin D. W. (1979). A cluster separation measure. IEEE Transactions on Pattern Analysis and Machine Intelligence.
16. van der Maaten L., Hinton G. (2008). Visualizing Data using t-SNE. Journal of Machine Learning Research.
17. Mikolov T., Chen K., Corrado G., Dean J. (2013). Efficient Estimation of Word Representations in Vector Space. arXiv preprint.
18. Pennington J., Socher R., Manning C. D. (2014). GloVe: Global Vectors for Word Representation. EMNLP.
19. Mimno D. et al. (2011). Optimizing Semantic Coherence in Topic Models. EMNLP.
20. Chang J. et al. (2009). Reading Tea Leaves: How Humans Interpret Topic Models. NeurIPS.
21. Halkidi M., Batistakis Y., Vazirgiannis M. (2001). On Clustering Validation Techniques. Journal of Intelligent Information Systems.
22. van Eck N. J., Waltman L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics.
23. Small H. (1973). Co-citation in the scientific literature: A new measure of the relationship between two documents. Journal of the American Society for Information Science.
24. Callon M., Courtial J.-P., Turner W. A., Bauin S. (1983). From translations to problematic networks: An introduction to co-word analysis. Social Science Information.
25. Börner K., Chen C., Boyack K. W. (2003). Visualizing knowledge domains. Annual Review of Information Science and Technology.
26. Fortunato S. (2010). Community detection in graphs. Physics Reports.
27. Perozzi B., Al-Rfou R., Skiena S. (2014). DeepWalk: Online Learning of Social Representations. KDD.
28. Grover A., Leskovec J. (2016). node2vec: Scalable Feature Learning for Networks. KDD.
29. Kipf T. N., Welling M. (2017). Semi-Supervised Classification with Graph Convolutional Networks. ICLR.
30. Lo K. et al. (2020). S2ORC: The Semantic Scholar Open Research Corpus. ACL.
31. Priem J., Piwowar H., Orr R. (2022). OpenAlex: A fully-open index of scholarly works, authors, venues, institutions, and concepts.



ALISHER SHAIMURAN
Master's student, School of AI & Data Science, Astana IT University, Astana, Kazakhstan
ORCID: 0009-0007-3417-8973
E-mail: 242914@astanait.edu.kz
Master's student in AI & Data Science at Astana IT University. His research focuses on scientometric analysis, bibliographic coupling networks, and time-weighted centrality methods for evaluating structural embeddedness in scholarly networks.

ОСОБЛИВОСТІ ТА ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНИХ ДАНИХ ПРИ ПЛАНУВАННІ ГУМАНІТАРНОГО РОЗМІНУВАННЯ В УКРАЇНІ

Дмитро Аеров

Анотація. *У дослідженні розглядаються ключові аспекти застосування геоінформаційних систем (ГІС) та даних дистанційного зондування для потреб планування гуманітарного розмінування територій України. Проаналізовано основні джерела просторових даних, їх переваги та обмеження. Висвітлено проблематику фрагментації даних, хибних спрацьовувань через засміченість територій залишками війни, а також питання стандартизації інформаційного обміну. Запропоновано підходи до оптимізації використання ГІС-технологій для підвищення ефективності нетехнічного обстеження територій.*

Ключові слова: геоінформаційні системи, гуманітарне розмінування, дистанційне зондування, просторовий аналіз, IMSMA.

I. ВСТУП

Внаслідок повномасштабного вторгнення Україна стала однією з найбільш замінованих країн світу. За оцінками національних та міжнародних експертів, значна частина території країни потребує обстеження на наявність вибухонебезпечних предметів (ВНП). У цих умовах класичні методи нетехнічного та технічного обстеження є занадто повільними. Тому критично важливим стає використання геоінформаційних систем (ГІС) та технологій дистанційного зондування Землі (ДЗЗ) для пришвидшення планування та пріоритезації процесів гуманітарного розмінування [1, 2].

Метою цієї роботи є аналіз особливостей інтеграції геоінформаційних даних у процеси планування протимінної діяльності в Україні, а також виявлення ключових проблем, що перешкоджають ефективному обміну та аналізу просторової інформації.

II. ДАНІ ТА МЕТОДИ

Основою для планування гуманітарного розмінування є міжнародна система управління інформацією протимінної діяльності (IMSMA), яка адаптована для використання в Україні [3]. Для наповнення системи та проведення просторового аналізу використовуються такі методи та дані [6]:

1. Мультиспектральні супутникові знімки високої (Maxar, PlanetScope) та середньої (Sentinel-2) розрізненої здатності.
2. Дані з безпілотних літальних апаратів (БПЛА), оснащених лідарами (LiDAR), магнітометрами та тепловізорами.
3. Дані відкритих джерел (OSINT) щодо місць ведення бойових дій.

Для оцінки ризиків та пріоритезації ділянок для розмінування застосовується метод багатокритеріального просторового аналізу (MCDA) [5]. Розрахунок індексу небезпеки ділянки обчислюється на основі формули 1:

$$R_i = \sum(w_j \times c_{ij}) \times V_i \quad (1)$$

де R_i — загальний індекс ризику для ділянки i; w_j — вага j-го фактора небезпеки (наприклад, наявність траншей, воронок); c_{ij} — нормалізоване значення фактора j; V_i —

коефіцієнт вразливості території (близькість до населених пунктів, критичної інфраструктури, сільськогосподарських угідь).

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Використання ГІС дозволяє автоматизувати виявлення ознак мінного забруднення. Наприклад, аналіз супутникових знімків дає змогу ідентифікувати лінії окопів, місця артилерійських обстрілів та знищену техніку, що є прямими індикаторами високої ймовірності наявності ВНП [2]. Як показано в Таблиці 1, кожне джерело геоінформаційних даних має свої специфічні особливості, переваги та недоліки, які необхідно враховувати при плануванні [1, 6].

Таблиця 1. *Порівняння джерел геоінформаційних даних для гуманітарного розмінування*

№	Джерело даних	Переваги	Недоліки
1	Супутникові знімки (оптичні)	Велике охоплення, історичний аналіз змін ландшафту	Залежність від погодних умов (хмарність), низька ефективність у лісистій місцевості
2	БПЛА з магнітометрами	Висока точність виявлення металевих аномалій у ґрунті	Обмежена площа покриття, необхідність фізичного доступу до ділянки
3	OSINT та дані від населення	Швидка актуалізація інформації, підтвердження інцидентів	Високий рівень інформаційного шуму, необхідність верифікації координат

Однак, впровадження цих технологій в Україні стикається з низкою серйозних проблем. По-перше, спостерігається фрагментація даних. Різні оператори протимінної діяльності (державні служби, міжнародні організації, приватні компанії) використовують різні формати збору геоданих, що ускладнює їх інтеграцію в єдину національну базу [3]. По-друге, значною проблемою є високий рівень засміченості територій металевим брухтом (залишками снарядів, побутовим сміттям), що призводить до величезної кількості хибних спрацьовувань при аналізі даних з магнітометрів [1, 6].

Для розуміння місця геоінформаційних даних у загальному процесі, розроблено концептуальну модель. Як показано на Рисунку 1, процес інтеграції даних є багатоетапним і вимагає постійної верифікації інформації з різних джерел.

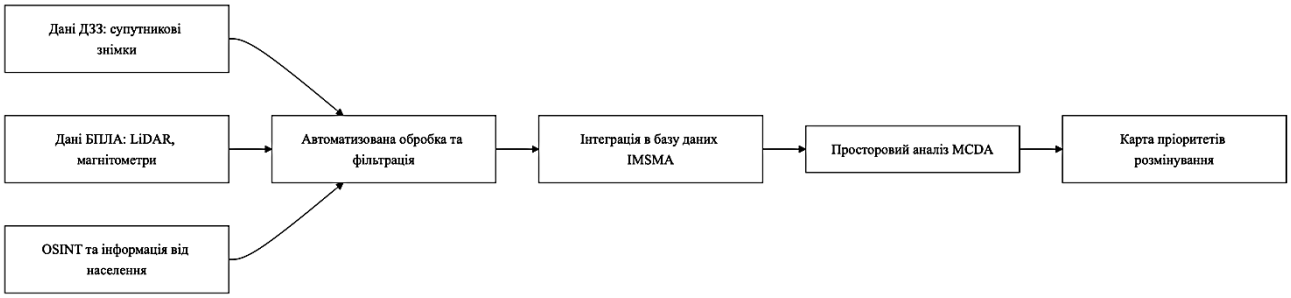


Рисунок 1. *Структурна схема інтеграції ГІС-даних у планування розмінування*

Додатковим викликом є динамічні зміни ландшафту. Швидке заростання покинутих сільськогосподарських угідь чагарниками робить використання оптичних супутникових знімків неможливим вже через рік після закінчення активних бойових дій на ділянці [6]. У таких випадках єдиним дієвим геоінформаційним інструментом залишається повітряне

лазерне сканування (LiDAR), яке здатне "проникати" крізь рослинність і фіксувати мікрорельєф (воронки, окопи) [4].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Геоінформаційні системи є безальтернативним інструментом для планування гуманітарного розмінування в Україні, оскільки вони дозволяють здійснювати пріоритезацію небезпечних територій на основі об'єктивних просторових даних. Однак, технологічний потенціал ГІС обмежений організаційними та методологічними проблемами.

Для підвищення ефективності використання геоінформаційних даних необхідно: затвердити на державному рівні єдині протоколи збору та обміну просторовими даними між усіма операторами протимінної діяльності [3]; впроваджувати технології машинного навчання (AI) для автоматизованої фільтрації хибних спрацьовувань (металевого брухту) на основі мультиспектрального аналізу ґрунтів [6]; розширити використання БПЛА з LiDAR-сенсорами для обстеження територій зі щільною рослинністю [4]. Вирішення цих проблем дозволить суттєво пришвидшити процес повернення територій до безпечного використання.

ДЖЕРЕЛА

1. Мироненко М. Л., Нестеренко С. Г., Рай А. В., Фролов О. В. (2024) 'Геоінформаційна підтримка розмінування територій Харківської області', Комунальне господарство міст [online]. URL: https://khg.kname.edu.ua/index.php/khg/article/download/6307/6227/14559
2. Чикота Віталій, Дмитро Янушкевич (2022) 'Картографування територій, забруднених вибухонебезпечними предметами', Електронний архів ХНУРЕ [online]. URL: https://openarchive.nure.ua/server/api/core/bitstreams/11432758-b221-4344-83ea-0d6073c4b9e5/content.
3. GICHD (2023) 'Better Information for Better Results: The Impact of IMSMA Core', Geneva International Centre for Humanitarian Demining [online]. URL: https://www.gichd.org/fileadmin/uploads/gichd/Media/GICHD-resources/rec-documents/GICHD_IMSMA_Impact_v08_WEB_final.pdf.
4. WWF-Ukraine (2023) 'Forest management on territories contaminated with unexploded ordnance', World Wildlife Fund [online]. URL: https://wwfeu.awsassets.panda.org/downloads/forest_management_on_territories_contaminated_with_unexploded_ordnance_1.pdf.
5. Зацерковний В. І., Ніколюк І. Р. (2025) 'Гуманітарне розмінування як складова протимінної діяльності', Technical sciences and technologies, № 1(39) [online]. URL: https://ir.stu.cn.ua/bitstreams/5d11d659-719c-4b20-920d-e10c142309b0/download.
6. Zatserkovnyi V., Tsiupa I., De Donatis M., Nikoliuk I., Kravchenia V., Tsvyk O., Mironchuk T. (2024) 'Methods to detect explosive hazards in agricultural areas', Вісник Київського національного університету імені Тараса Шевченка. Геологія [online]. URL: https://geology.bulletin.knu.ua/en/article/download/4383/3716/16708



ДМИТРО АЕРОВ
аспірант 1 курсу інформаційних систем та технологій у Київському національному університеті імені Тараса Шевченка.
ORCID: 0009-0005-2438-2554
E-mail: aerovd@fit.knu.ua
Отримав ступінь магістра за спеціальністю 126 «Інформаційні системи та технології» у Київському національному університеті імені Тараса Шевченка (Київ, Україна).

КОГНІТИВНА МОДЕЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАСТОСУВАННІ СУДОВОЇ ЕКСПЕРТИЗИ ТА ПИТАНЬ ВИКЛИКІВ ЩОДО КІБЕРБЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Єлизавета Бабенко

Анотація. *В даній тезі досліджено та розглянута теоретична і практична складова когнітивної моделі, як частини інформаційних технологій зі застосуванням в сфері судової експертизи та питань викликів щодо кібербезпеки персональних даних. Тенденція впровадження інформаційних технологій, де когнітивні технології моделювання, обчислень та оцінки при якому формується експертиза. Приведено можливі приклади методів технології штучного інтелекту в судовій експертизі. Здійснено порівняльний аналіз практичного використання в Україні та у світі.*

Ключові слова: когнітивні інформаційні технології, судова експертиза, кібербезпека, персональні дані, штучний інтелект.

I. ВСТУП

Інформаційні технології продовжують впроваджуватися в різні напрямки суспільства створюючи нові можливості для розвитку суспільства. Відповідно цього Україна активно впроваджує різні інформаційні технології в державні установи, а саме особливу увагу надає впровадженню штучного інтелекту. Однак, постає питання доцільності та питань безпеки таких впроваджень, адже дослідження демонструють відповідні виклики навіть на даних етапах зазначають не тільки дослідники в своїх наукових роботах, але й в різних медіа просторах, закликаючи звертати увагу на даний об’єкт зокрема в питаннях об’єктивності таких результатів досліджень. Судова експертиза та загалом експертні висновки є однією з тих видів державної діяльності, які ще не почали офіційно/публічно використовувати когнітивні моделі, а саме когнітивні обчислення штучного інтелекту, але звертаючи увагу на різні нормативні документи та стратегії розвитку можна зробити припущення, що після завершення пріоритетних напрямків можуть перейти і до інших.

II. ДАНІ ТА МЕТОДИ

Основні дані зазначають важливість тематики демонструючи проблематику. В досліджені враховуються дані та метрики з трьох напрямків, які є підгрунтям дослідження і формують загальний огляд теоретичної та практичної складової (Для більш точніших даних було проаналізовано українські та зарубіжні джерела):

– Інформаційно-технологічна документація та дослідження, а саме наукові праці, щодо опису технічної складової технології та його особливості з практичного впровадження;

– Нормативна база відповідного законодавства в сфері судової експертизи, в яких зазначена специфіка досліджуваного об’єкту;

– Інші дослідження (практичні кейси, статистика та публічні медіа дані), які мають дотичні елементи проаналізованого об’єкту;

– Застосовані методи дослідження: було використано збирання даних та подальший їх аналіз для формування дослідження.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Результати дослідження демонструють відповідно до низки реального потенціалу розвитку досліджень, які можуть сприяти новим можливостями та запобігти виникненню ризиків, які наразі можна спостерігати на практичних кейсах таких випадків. Поєднання інформаційних технологій з різними напрямками суспільної діяльності є невід'ємною частиною сучасного та майбутнього розвитку тому Україна спрямована на автоматизацію, залучаючи різні інформаційні технології, орієнтуючись на сучасні можливості автоматизації процесу.

Одним з мало досліджених напрямків впровадження інформаційних технологій є діяльність в сфері проведення експертизи (судові експертизи). Судова експертиза – «дослідження на основі спеціальних знань в різних галузях: науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів з метою надання висновку з питань, які є або будуть предметом судового розгляду» [2]. Особливу увагу варто звернути на вид експертиз: «Криміналістична», «Інженерно-технічна експертиза» та підвиди «Трасологічна експертиза», «Експертиза комп'ютерної техніки і програмних продуктів», «Експертиза електронних комунікацій» через безпосередню дотичність до технологій пов'язаних з питанням когнітивної оцінки кібербезпеки та даних (особливо щодо персональними даними) в експертній діяльності. Тобто при проведені цих експертиз задіються інформаційні та комп'ютерні технології при аналізу та формуванні експертних висновків задіюючі методи використання даної технології (ШІ), які базується на взаємодії з відповідними даними [3].

Когнітивна модель – зв'язок метрик/факторів пов'язаних з метою. В даному випадку задіюється когнітивне обчислення, як додаткова складова штучного інтелекту – «імітація процесу аналізу та видачу інформації». Алгоритмічно технологія здійснює процес оцінки переноситься в датасет, в якому буде зберігатися вся внесена інформація (тобто дані). Дана технологія може автоматизувати процес аналізу досліджувального об'єкту (доказів, тексту/даних) з подальшою обробкою, формуючи висновки поліпшуючі роботу, однак і дає змогу зберігати та навчати технологію для подальшої роботи [1, с. 173].

З цього випливає питання як захистити дані від несанкціонованого використання і реалізувати можливості кібербезпеки. Як продемонстровано на Рисунку 1 процес роботи автоматизації експертизи може здійснюватися таким чином: внесені дані обробляються ШІ (перед цим з пройденим машинним навчанням) з подальшим отриманням результату, який потім аналізується експертом і формується кінцевий висновок. Однак, як зазначає багато джерел потім такий висновок може бути переміщений в базу даних для подальшого вдосконалення технології когнітивного обчислення без відома фізичних осіб, які направили об'єкт дослідження на експертизу. Тобто застосування когнітивної моделі, для вровадження в проведення судової експертизи, може призвести до ризику безпеки даних зокрема персональних даних кожного дослідженого суб'єкта/об'єкта.

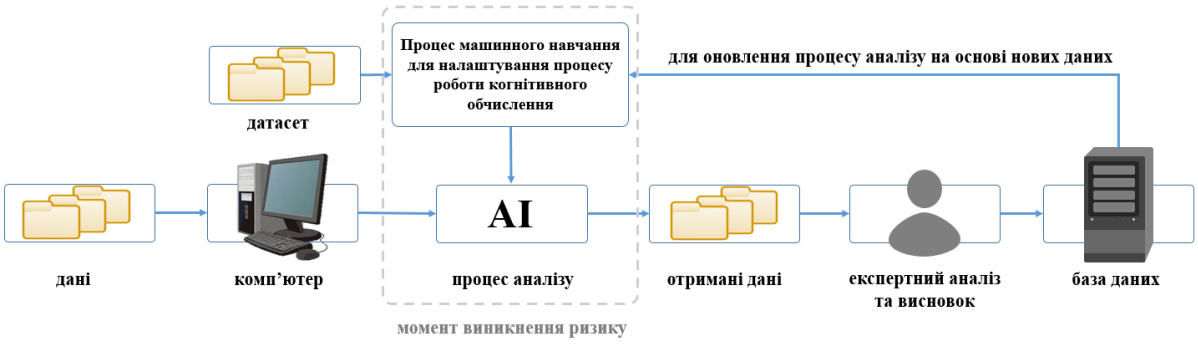


Рисунок 1. *Процес роботи та момент ризику*

При порівнянні практик України та зарубіжних країн можна бачити значну різницю через практичні можливості впроваджень та реальних практичних кейсів. До прикладу Україна в грудні 2025 року впровадила проєкт AI-помічника. На прикладі зарубіжних країн можна привести ПЗ Skeleton ID де ШІ задіює процес краніофаціальної накладки при цьому є ризик, що надані дані в подальшому можуть бути використані без дозволу. Закон ЄС щодо ШІ зазначає ризикованість застосування такої технології в судовій експертизі та обмежує деякі моменти. Також ще одним викликом є етичний аспект, де ШІ може стати перешкодою для запровадження адже технологія базується на процесі навчання, які уникають моменту моральних норм суспільства, які стосуються застосування даних експертиз (здебільшого це стосується персональних даних), які можуть бути неприйняті серед низки верств суспільства, які не бажають щоб їх дані в подальшому використовувалися в невизначених цілях.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отже, наразі спостерігається тенденція впровадження інформаційних технологій в більшість сфер діяльності для автоматизації, в сторону поліпшення та збільшення продуктивності виконання роботи особливо враховуючи сьогоденні реалі життя, за якими потрібно враховувати перешкоди. Однак з іншого боку виникає багато суперечливих питань щодо об’єктивності та безпеки, які можуть вникнути при впроваджені когнітивного обчислення, а саме деяких інформаційних технологій, особливо пов’язаних зі штучним інтелектом. Реалізація реального потенціалу та впровадження потребує обмеження доступу та залишення його використання в низки блоках роботи, які стосуються безпосередньої об’єктивності та питань безпеки даних. Судова експертиза як і будь-яка технологія повинна бути налаштована відповідно за процесом. Тобто варто враховувати не тільки етичні моменти реального висновку кваліфікованої експертизи, які людина може враховувати при проведенні (які може оминути техніка), але й питання безпеки, які можуть бути втрачені або несанкціоновано передані тертім особам при здійснені кібератак або втручань в системи.

Об’єктивно наразі дослідження має два напрямки розвитку, які можуть зменшити виникнення викликів та ризиків щодо даних та збільшити можливості кібербезпеки: Створити внутрішнє програмне забезпечення з обмеженим доступом та функціоналом, який може знизити ризик; Контролювати дані, які можуть бути застосовані для процесу вдосконалення технології/ПЗ, видаляючи персоналізацію.

ДЖЕРЕЛА

1. Попов М., Зайцев О., Стефанцев С. (2025). Інноваційний підхід до зменшення когнітивних помилок в експертному оцінюванні. Social Development and Security. Vol. 15. №1. DOI: https://doi.org/10.33445/sds.2025.15.1.16
2. Про судову експертизу: Закон України від 25.02.1994 р. №4038-XII Відомості Верховної Ради України. 1994. №28. Ст. 232
3. Нестор Н.В. (2024). Штучний інтелект у судові експертизі: загроза чи перспектива. Міжвідомчий науково-методичний збірник «Криміналістика і судова експертиза». DOI: https://doi.org/10.33994/kndise.2024.69.07



ЄЛИЗАВЕТА БАБЕНКО
здобувач 2 курсу магістерського рівня спеціальності міжнародного права, кафедри Міжнародного та галузевих правових дисциплін, Національної академії наук України Київського університету права, Київ, Україна
ORCID: 0009-0009-6444-7331
E-mail: liza.b2402@gmail.com
Наукові інтереси: комп’ютерні технології, сучасне право та дизайн.

КОНЦЕПТУАЛЬНА СХЕМА ПРИЙНЯТТЯ РІШЕНЬ В СИТУАЦІЇ ПЕРЕСЛІДУВАННЯ ЦІЛІ ГРУПОЮ ГРАВЦІВ З ОДНАКОВИМИ ТАКТИКО-ТЕХНІЧНИМИ ХАРАКТЕРИСТИКАМИ

Леся Барановська, Григорій Гнатієнко

Анотація. *Розглядається задача переслідування цілі групою переслідувачів на площині. Передбачається, що усі переслідувачі мають однакові тактико-технічні характеристики. Швидкість переслідувачів незначною мірою перевищує швидкість цілі. Запропоновано концептуальну схему переслідування формалізувати в термінах задач багатокритеріальної оптимізації. При цьому доцільно застосовувати задачі ранжування альтернатив та використовувати коефіцієнт ранжованості ряду. Описано та обґрунтовано підходи до екстраполяції руху цілі та апроксимації потенційних ситуацій прийняття рішень.*

Ключові слова: задача переслідування, динамічні ігри, ціль, переслідувачі, багатокритеріальна постановка, екстраполяція, апроксимація.

I. ВСТУП

Задача переслідування на площині є відомою задачею, яка добре вивчена, глибоко обґрунтована і має багато різноманітних застосувань [1, 2]. Дослідження здійснюються в рамках теорії динамічних ігор із застосуванням методів моделювання конфліктно-керованих процесів та диференціальних ігор. Розроблено та досліджено також задачі дискретної оптимізації, в термінах яких формалізуються задачі групового переслідування.

Водночас цікавим та перспективним є напрям формалізації задач переслідування в термінах задач багатокритеріальної оптимізації та управління процесом переслідування з урахуванням вибору компромісних стратегій гарантованого досягнення цілі з мінімізацією часу переслідування.

II. ПОСТАНОВКА ЗАДАЧІ

Нехай відомо координати, швидкість та курс цілі $x^0 = \left(x_1^0, x_2^0, x_3^0, x_4^0\right)$ та k гравців (переслідувачів)

$$x^i = \left(x_1^i, x_2^i, x_3^i, x_4^i\right), \;\; i = 1,...,k. \tag{1}$$

Рух цілі та переслідувачів є рівномірним, з маневрів допускається лише маневр курсом, тобто плавний поворот на площині. Отже, маємо двовимірну модель переслідування і у подальшому маємо на увазі розв’язання геометричних задач на площині.

Зауваження 1. Маневром по висоті у цій роботі нехтуємо, зокрема, через те, що шлях переслідування цілі переслідувачами по горизонталі є суттєво меншим від шляху по вертикалі.

Необхідно побудувати стратегію переслідування таким чином, щоб мінімізувати час мінімального зближення щонайменше одного переслідувача з ціллю, тобто досягти ситуації, коли:

$$\exists i, \;\; i \in \{1,...,k\} = I : \;\; \sqrt{\left(x_1^0 - x_1^i\right)^2 + \left(x_2^0 - x_2^i\right)^2} < \varepsilon, \tag{2}$$

де $\varepsilon-$ деяке достатньо мале число, яке забезпечує потрібний гарантований вплив на ціль і вибирається експертним шляхом.

Будемо вважати, що тактико-технічні дані переслідувачів та цілі в цілому є співмірними, але швидкість переслідувачів дещо перевищує швидкість цілі

$$\forall i,\ i \in I:\ x_3^0 = x_3^i + \delta,$$

де $\delta > 0-$ деяке відоме мале число.

Таким чином, мінімізація маневрування переслідувачів та їхній рух не паралельним до цілі курсом сприятиме додатковому зближенню переслідувачів з ціллю – з урахуванням теореми Піфагора в обох випадках.

Необхідно мінімізувати час зближення принаймні одного переслідувача з групи (1) в сенсі, описаному виразом (2). Тобто, необхідно визначити момент часу t, коли відстань між групою переслідувачів (1) та ціллю стає меншою від деякого заданого ε.

III. СХЕМА ПРИЙНЯТТЯ РІШЕННЯ В СИТУАЦІЯХ ПЕРЕСЛІДУВАННЯ

Схему прийняття рішення щодо маневрування переслідувачів та екстраполяції маневрування та місцезнаходження цілі доцільно описувати у вигляді кількох етапів. Опишемо деякі передумови прийняття рішень.

Використовуючи супутникову навігацію та автопілот, ціль змінює курс під час польоту, виконуючи численні повороти на маршруті – з метою для обходу зон дії протиповітряної оборони, виявлення «слабких місць» у захисті, виходу на ціль з несподіваного боку тощо. Тому мінімізація часу зближення переслідувачів з ціллю є надзвичайно важливим завданням.

Введемо поняття *такт переслідування* – проміжок часу, протягом якого доцільно здійснювати обчислення поточної ситуації прийняття рішення та визначати маневри кожного з гравців групи переслідувачів. Визначення конкретного значення такту переслідування може вводитися евристично або бути обчислене та обгрунтоване на основі деяких міркувань.

Означення 1. *Тактом переслідування* назвемо проміжок часу, протягом якого можна з великою ймовірністю передбачити маневрування та зміну місцезнаходження цілі.

Зрозуміло, що чим меншим є значення такту переслідування, тим більша ймовірність вірного прогнозування місцезнаходження цілі. Але наближення значення такту переслідування до нуля неможливе через запізнення надходження сигналів, витрати часу на обчислення та розв'язання оптимізаційної задачі тощо.

Означення 2. *Тактичним маневруванням* назвемо прийняття рішення щодо вибору локальної групи переслідувачів та початку розв'язання локальної підзадачі переслідування.

На першому етапі визначаємо ситуацію для початку *тактичного маневрування*. Для цього введемо евристику, яка у подальшому може не узгоджуватися з реальними маневрами цілі.

Евристика Е1. Тактичне маневрування здійснюється для проміжку часу, який вимірюється сотнями і тисячами тактів переслідування. Тобто, прогнозування у цьому випадку є на кілька порядків більшим, ніж такт переслідування.

Евристика Е2. Ціль здійснюватиме прямолінійний рівномірний рух до зближення з одним із переслідувачів групи (1).

Означення 3. Точку перетину екстрапольованого маршруту цілі з першим переслідувачем назвемо *цільовою точкою*, а цього переслідувача – *ведучим переслідувачем*.

З урахуванням евристики Е2 обчислюємо усі k точок зближення кожного з переслідувачів на прямолінійному маршруті цілі. Позначимо ці точки з координатами через

$$a^i = \left(a_1^i, a_2^i\right),\ i \in I. \tag{3}$$

Для ряду (3) визначимо коефіцієнт ранжованості ряду [3]. Після цього розв'язуємо задачу мінімізації цього показника, зменшуючи кількість точок ряду (3) до одержання деякого значення коефіцієнта ранжованості, достатнього для прийняття рішення про активізацію переслідувачів.

Означення 4. Підгрупу переслідувачів, яка доставляє мінімум коефіцієнту ранжованості ряду, назвемо групою активних переслідувачів і позначимо їхню кількість через $k_1 < k$.

Зауваження 2. Визначення групи активних переслідувачів можна здійснювати шляхом кластеризації елементів ряду (3) чи інших способів формалізації.

Зауваження 3. Розмір групи активних переслідувачів не є стабільною величиною і може змінюватися у процесі розв'язання задачі переслідування – з тенденцією до збільшення.

Опишемо схему переслідування цілі групою переслідувачів з урахуванням евристик, означень та зауважень, сформульованих вище, у вигляді послідовності кроків.

Крок 1. Визначення тривалості такту переслідування.

Цей показник є важливим не тільки з точки зору формалізації задачі переслідування, але й для обґрунтування параметрів екстраполяції місцезнаходження цілі. Наприклад, при здійсненні маневру на розворот існують обмеження на кут відхилення цілі протягом короткого проміжку часу. Коли такт переслідування вибрати тривалістю 1-2 секунди, то за цей час ціль зможе зробити відхилення від прямолінійного руху лише на 15-30 градусів – навіть, якщо вона почала маневрувати на самому початку чергового такту. Таким чином, обґрунтованою є наступна евристика.

Евристика Е3. Місцезнаходження цілі в кінці чергового такту є гарантованим на дузі сектора з кутом 30-60 градусів відхилення від прямолінійного руху цілі.

Слід також зважати на особливості поведінки цілі та переслідувачів у природних умовах з урахуванням особливостей сучасного стану зв'язку, обчислювальної техніки тощо. Тому при моделюванні цієї задачі слід зважати на ще одну евристику.

Евристика Е4. На прийняття рішення про переслідування цілі значною мірою впливає технічна затримка – на передачу сигналу, обчислення місцезнаходження тощо. Покладемо значення затримки рівним половині такту переслідування.

Крок 2. Екстраполяція місцезнаходження цілі в кінці чергового такту переслідування.

З метою дискретизації процесу переслідування введемо похідну від евристики Е3.

Евристика Е5. Три точки, які належать екстрапольованій дузі, достатньою мірою екстраполюють місцезнаходження цілі з метою прийняття рішення про дії переслідувачів – кінці дуги і її центр. Позначимо ці точки в кінці такту t через:

$$a_t^{01}, a_t^{02}, a_t^{03}\ . \tag{4}$$

Наступним підетапом схеми прийняття рішень на переслідування цілі є оперативне маневрування групи переслідувачів.

Крок 3. Обчислення відстаней від екстрапольованих точок місцезнаходження цілі (4) до підмножини екстрапольованих точок місцезнаходження групи активних переслідувачів з множини (3).

Крок 4. Прийняття рішення на маневрування переслідувача з групи активних переслідувачів, який є аргументом компромісного розв'язку багатокритеріальної задачі переслідування. Критеріями розв'язання цієї задачі є відстані від переслідувачів до цілі та зміна напрямку руху у попередніх тактах переслідування.

Для формалізації задачі багатокритеріальної оптимізації необхідно здійснити попереднє ранжування переслідувачів з урахуванням їхнього місцеположення та історії маневрування.

Крок 5. Перевірка стану задачі переслідування з урахуванням місцезнаходження усієї групи переслідувачів. Приєднання, у разі відповідної конфігурації переслідувачів, до активної групи додаткових переслідувачів. Перехід до кроку 2.

Крок 6. Вибір нового ведучого переслідувача у разі необхідності.

Зауваження 4. Ведучий на черговому такті переслідувач є найважливішим і одержує деякі преференції – мінімізацію маневрів тощо.

Зауваження 5. На основі аналізу поведінки цілі протягом останніх тактів може здійснюватися складна екстраполяція її поведінки. Для цього з рою переслідувачів можуть бути виділені дрони-розвідники.

Зауваження 6. Якщо рій великий, то частина переслідувачів може бути спрямована на перехоплення та прийняття рішень щодо маневрування з використанням інших евристик.

IV. ВИСНОВКИ

У цій роботі розглянуто задачу переслідування цілі кількома гравцями у дискретній постановці. Описано схему прийняття рішень з використанням задачі багатокритеріальної оптимізації. Наведено також деякі ідеї щодо подальшого розвитку цього напряму у розв’язанні задач групового переслідування.

ДЖЕРЕЛА

1. Baranovska, L.V.: Quasi-Linear Differential-Deference Game of Approach. In: Sadovnichiy, V., Zgurovsky, V. (eds.) Modern Mathematics and Mechanics. Understanding Complex Systems, pp. 505–524. Springer, Cham (2019)

2. Baranovska, Lesia V.: Pursuit differential-difference games with pure time-lag. Discrete and Continuous Dynamical Systems – Series B 24(3), 1024–1031 (2019).

3. Гнатієнко Г.М., Снитюк В.Є. Експертні технології прийняття рішень: Монографія. – К.: ТОВ «Маклаут», 2008. – 444с.



ЛЕСЯ БАРАНОВСЬКА
К.ф.-м.н., доцентка кафедри кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID: 0000-0003-0024-8180
E-mail: lesia@baranovsky.org

Нині авторка працює над науковими проєктами з конфліктно-керованих процесів. Серед наукових інтересів – динамічні ігри, теорія оптимального керування, диференціально-різницеві ігри, теорія ігор, теорія прийняття рішень, системи і методи штучного інтелекту.



ГРИГОРІЙ ГНАТІЄНКО
К.т.н., заступник декана з наукової роботи факультету інформаційних технологій, Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID: 0000-0002-0465-5018
E-mail: g.gna5@ukr.net

Нині автор працює над здобуттям ступеня доктора технічних наук. Серед наукових інтересів – системи підтримки прийняття рішень, методи обробки експертної інформації, моделювання складних систем.

КОГНІТИВНЕ МОДЕЛЮВАННЯ N-РІВНЕВИХ МІРКУВАНЬ LLM-АГЕНТІВ: АРХІТЕКТУРА ДИНАМІЧНОЇ ВЕРИФІКАЦІЇ ТА САМОКОРИГУВАННЯ

Єгор Башкевич, Любов Кубявка

Анотація. *Роботу присвячено вирішенню проблеми алгоритмічних галюцинацій у великих мовних моделях (LLM) під час виконання складних завдань із верифікації текстів. Запропоновано N-рівневу мультиагентну архітектуру когнітивного моделювання, яка перетворює ймовірнісну генерацію на контрольований детермінований процес. Суть роботи полягає у застосуванні нейросимволічних маркерів стану та методу конформного прогнозування на базі семантичної ентропії для кількісної оцінки невизначеності на кожному кроці міркувань. Алгоритм забезпечує динамічне виявлення хибної логіки, ініціюючи RAG-коригування або безпечну відмову. Це суттєво підвищує надійність автономних систем при семантичному розборі контенту та розпізнаванні маніпулятивних впливів.*

Ключові слова: когнітивне моделювання; мультиагентні системи; оцінка невизначеності; семантична ентропія.

I. ВСТУП

Стрімкий розвиток великих мовних моделей (LLM) відкрив нові можливості для автоматизованого семантичного розбору текстів. Проте використання генеративних моделей у задачах, що вимагають абсолютної фактологічної точності, стикається з перешкодою, а саме схильністю алгоритмів до генерації галюцинацій. При виконанні багатокрокових завдань LLM часто потрапляють у «спіраль галюцинацій», коли незначна похибка на ранніх етапах міркувань (Chain-of-Thought) інтегрується в контекст і призводить до експоненційного накопичення помилок [1-2].

Перехід від ізольованих моделей до мультиагентних систем (MAS) частково вирішує цю проблему, але традиційні методи, наприклад, мажоритарне голосування агентів залишаються вразливими до ефекту «сліпого консенсусу». Це формує потребу в розробці механізмів кількісної оцінки невизначеності (Uncertainty Quantification), які б виявляли відхилення безпосередньо під час генерації[3].

II. ДАНІ ТА МЕТОДИ

Основою запропонованого фреймворку є N-рівнева архітектура, що формалізує процес когнітивного аналізу як керований граф міркувань. Замість використання єдиної моделі, система запроваджує замкнений контур зворотного зв'язку (closed-loop) із залученням двох ізольованих агентів: Аналітика та Аудитора.

Алгоритм складається з чотирьох основних етапів, візуалізованих на Рисунку 1.

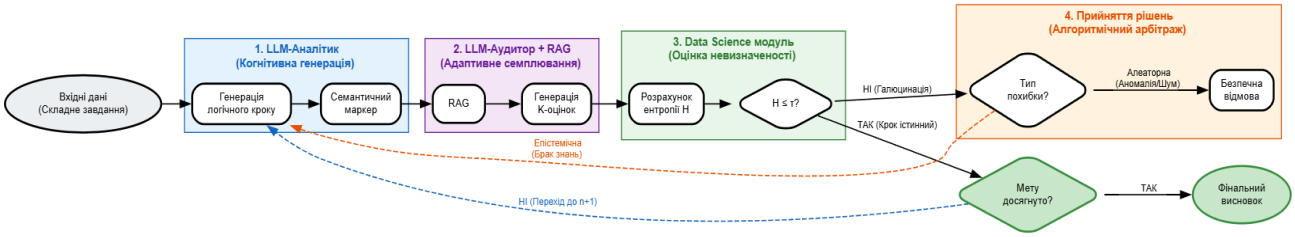


Рисунок 1. *Графічна модель N-рівневого алгоритму рекурсивної верифікації у Graphviz*

Нейросимволічна інкапсуляція.

На кроці n Агент-Аналітик формує проміжний висновок. Для уникнення «семантичної сліпоти», притаманної класичним векторним ембеддінгам, результат генерується у вигляді структурованого JSON-об'єкта («семантичного маячка»), що містить логічні трійки фактів та дозволяє алгоритмічно відстежувати втрату контексту.

Адаптивне семплювання.

Агент-Аудитор отримує маячок для перевірки. Замість ресурсоємної масової генерації, застосовується вибірковий каскад: спочатку генерується базова вибірка з K=2 оцінок. Якщо розбіжностей немає, перевірка завершується. Додаткове семплювання ініціюється виключно при виявленні суперечностей.

Оцінка невизначеності.

Ступінь згоди Аудитора із самим собою вимірюється через математичну модель семантичної ентропії. Для прийняття рішення використовується алгоритм Token-Entropy Conformal Prediction (TECP). Він адаптивно розраховує поріг надійності τ для поточного кроку. Якщо ентропія не перевищує поріг — крок фіксується як істинний[4-5].

Алгоритмічний тріаж та Рекурсія.

При перевищенні порогу τ (фіксація галюцинації), алгоритм звертається до зовнішнього пошуку (RAG) для визначення природи збою: 1) Епістемічна похибка (брак знань): RAG знаходить факти, система оновлює контекст і повертає Аналітика на переробку кроку n; 2) Алеаторна похибка (маніпулятивний/нелогічний вхідний текст): якщо RAG фіксує суперечність джерел, ініціюється протокол Абстенції (Безпечної відмови), блокуючи подальшу генерацію.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Теоретичний аналіз та моделювання запропонованої архітектури демонструють значні переваги над існуючими підходами. Традиційні методи мультиагентного аналізу (majority voting) виявляються вразливими до «консенсусу конфабуляцій», коли агенти поділяють спільні упередження і підтверджують галюцинації один одного. Це призводить до явища, відомого як «пастка стабільності», коли висока впевненість у кінцевому вердикті маскує критичні помилки у логіці міркувань. Натомість інтеграція семантичної ентропії дозволяє динамічно виявляти розбіжності та переривати цей цикл.

Крім того, запропонований механізм адаптивного семплювання оптимізує ресурсоємність. Завдяки тому, що система генерує розширену вибірку перевірок лише у випадках високої розбіжності між першими базовими оцінками, обчислювальні витрати скорочуються, зберігаючи при цьому математично довідну надійність.

Залучення зовнішнього RAG-заземлення на етапі тріажу розділяє епістемічну (нестача об'єктивних знань моделі) та алеаторну (інформаційний шум або пряма маніпуляція) невизначеність. Це забезпечує уникнення нескінченних рекурсивних циклів та дозволяє системі вчасно застосовувати протокол безпечної відмови.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована N-рівнева архітектура вирішує проблему нездатності імовірнісних моделей гарантувати послідовну логіку міркувань. Перехід до покрокового циклу з використанням нейросимволічних маячків та конформного прогнозування (TECP) дозволяє зупиняти генерацію хибної інформації на етапі її виникнення. Інтеграція протоколу

безпечної відмови (Abstention) формує надійний базис для впровадження автономних мультиагентних систем у завдання інформаційної аналітики.

ДЖЕРЕЛА

1. Kuhn, L., Gal, Y. and Farquhar, S. (2024) 'Detecting hallucinations in large language models using semantic entropy', Nature, 630, pp. 625–630.
2. Janiak, D., Binkowski, J., Sawczyn, A., Gabrys, B., Shwartz-Ziv, R. and Kajdanowicz, T. J. (2025) 'The Illusion of Progress: Re-evaluating Hallucination Detection in LLMs', Findings of the Association for Computational Linguistics: EMNLP 2025, pp. 34728–34745.
3. Sheng, H., Liu, X., He, H., Zhao, J. and Kang, J. (2025) 'Analyzing Uncertainty of LLM-as-a-Judge: Interval Evaluations with Conformal Prediction', Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing, Suzhou, China.
4. Nguyen, D., Payani, A. and Mirzasoleiman, B. (2025) 'Beyond Semantic Entropy: Boosting LLM Uncertainty Quantification with Pairwise Semantic Similarity', Findings of the Association for Computational Linguistics: ACL 2025, pp. 4530–4540.
5. Vashurin, R. et al. (2025) 'Benchmarking Uncertainty Quantification Methods for Large Language Models with LM-Polygraph', Transactions of the Association for Computational Linguistics, 13, pp. 220–248.



ЄГОР БАШКЕВИЧ
студент 1 курсу магістратури кафедри технологій управління Київського національного університету імені Тараса Шевченка, м. Київ, Україна
ORCID: 0009-0005-1377-312X
E-mail: yehorbashkevych@knu.ua
Науковий інтерес полягає в області інформаційної аналітики та Data Science. Серед наукових інтересів — дослідження великих мовних моделей (LLM), когнітивне моделювання штучного інтелекту та розробка автоматизованих систем для верифікації контенту і виявлення маніпулятивних впливів.



ЛЮБОВ КУБЯВКА
к.т.н., доцент кафедри технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0005-5397-1585
E-mail: liubov.kubiavka@knu.ua
Викладач з 2015 р. Має більше 100 наукових праць. Серед наукових інтересів — бізнес-аналітика ІТ проєктів, технології управління життєвим циклом ІТ проєктів, управління впливами проєктів, інформаційні технології реінжинірингу бізнес-процесів, механізми та інструменти управління програмами інформатизації, цифровізації.

КЛАСИФІКАЦІЯ КОГНІТИВНИХ ВИКРИВЛЕНЬ У ПРОЦЕСІ ПРОЄКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Владислав Безуглий, Ольга Кравченко

Анотація. *У роботі досліджено класифікацію когнітивних викривлень, які виникають на різних стадіях проєктування інформаційних систем. На основі теоретичного аналізу систематизовано типові когнітивні викривлення за фазами життєвого циклу: аналіз вимог, архітектурне проєктування, реалізація, тестування та впровадження. Визначено п'ять категорій чинників впливу — когнітивний, соціальний, організаційний, контекстуальний і технологічний, що формують середовище прийняття рішень у процесі створення інформаційних систем.*

Ключові слова: когнітивні викривлення, проєктування інформаційних систем, життєвий цикл, прийняття рішень, класифікація.

I. ВСТУП

У сучасних умовах високої динаміки технологічного розвитку проєктування інформаційних систем (ІС) все більше орієнтується не лише на технічні, але й на когнітивні фактори. Впровадження складних систем вимагає прийняття рішень в умовах невизначеності та обмеженого часу, де критично зростає роль людського фактора. Інформаційні системи у цьому контексті розглядаються як техніко-соціальні комплекси, на всіх етапах розробки яких активну участь беруть люди, а отже, процес проєктування ІС є вразливим до впливу когнітивних факторів. Когнітивні викривлення — систематичні відхилення у мисленні, що є результатом використання евристик, тобто спрощених ментальних стратегій — можуть істотно впливати на якість аналізу вимог, архітектурні рішення та загальну ефективність ІС.

Незважаючи на зростаючу увагу до цієї проблеми, наявні дослідження переважно зосереджуються на фрагментарному аналізі окремих типів викривлень у обмежених контекстах: інформаційний пошук [1], управління ефективністю [3], алгоритмічні викривлення [4], цифрові трансформації державного сектору [5]. Бракує комплексної моделі, яка б дозволяла ідентифікувати та класифікувати когнітивні викривлення на всіх етапах життєвого циклу проєктування ІС. Метою цього дослідження є систематизація когнітивних викривлень за фазами життєвого циклу проєктування ІС та визначення структури впливів, що сприяють їх формуванню.

II. ДАНІ ТА МЕТОДИ

Дослідження має теоретико-аналітичний характер. Застосовано міждисциплінарний підхід, який об’єднує системний аналіз, методи когнітивної психології та моделювання рішень. Використано методи абстрагування, аналізу і синтезу для побудови цілісної класифікації, а також концептуальне картування для формалізації впливів когнітивних викривлень. Теоретичну базу дослідження становлять наукові публікації [1–5].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На основі аналізу літературних джерел когнітивні викривлення були класифіковані за стадіями проєктування ІС. Результати систематизації представлено в Таблиці 1.

Ці викривлення можуть суттєво впливати на якість прийняття рішень, знижуючи ефективність системи та створюючи необґрунтовані ризики. Їхнє вчасне виявлення та подолання є ключовими елементами людиноцентричного підходу до проєктування ІС.

Таблиця 1. *Когнітивні викривлення в процесі проєктування ІС*

Стадія проєктування	Типові когнітивні викривлення
Аналіз вимог	Ефект якоря (anchoring), підтверджувальне упередження (confirmation bias), ефект фреймінгу (framing effect)
Архітектурне проєктування	Завищена впевненість (overconfidence bias), групове мислення (groupthink)
Реалізація	Сліпа пляма упередженості (bias blind spot), упередження виживання (survivorship bias)
Тестування та впровадження	Ефект ретроспективного викривлення (hindsight bias), статус-кво упередження (status quo bias)

Як показано в Таблиці 1, на стадії аналізу вимог домінують ефект якоря та підтверджувальне упередження [1], що можуть зумовити фіксацію на початкових варіантах без належного розгляду альтернатив. На стадії архітектурного проєктування критичними є завищена впевненість та групове мислення, що знижують якість колективних рішень [3]. На стадії тестування та впровадження домінують ефект ретроспективного викривлення та статус-кво упередження, яке блокує ініціативність і прийняття інновацій [5], що ускладнює об'єктивну оцінку прийнятих рішень. При цьому джерелом викривлень може бути не лише вихідне навчальне середовище, а й упередження, які проникають у логіку архітекторів системи [4].

Водночас аналіз показав, що середовище прийняття рішень під час проєктування ІС формується під впливом багаторівневої структури чинників, класифікованих за п'ятьма напрямами (Таблиця 2): когнітивні (внутрішні психологічні обмеження — евристики, викривлення пам'яті, емоційні упередження), соціальні (групова динаміка, конформізм, домінування окремих учасників), організаційні (стиль управління, корпоративна культура, рівень автономності команд), контекстуальні (часові обмеження, бюджетні рамки, тиск замовника) та технологічні (вибір інструментів і платформ, які можуть мати як компенсаторну, так і підсилювальну дію щодо когнітивних викривлень).

Таблиця 2. *Чинники впливу на прийняття рішень в процесі проєктування ІС*

Категорія	Чинники впливу
Когнітивні	Евристики, викривлення пам'яті, емоційні упередження
Соціальні	Групова динаміка, комунікація, групове мислення
Контекстуальні	Зовнішні обмеження, тиск замовника, терміни, невизначеність
Організаційні	Структура влади, система прийняття рішень
Технологічні	Платформи, системи підтримки рішень

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Результати дослідження підтверджують, що когнітивні викривлення мають системний характер і проявляються на всіх стадіях проєктування ІС. Ці висновки корелюють із результатами досліджень впливу когнітивних викривлень на прийняття рішень у контексті пояснювального штучного інтелекту [2], управління ефективністю організацій [3], цифрових трансформацій державного сектору [5] та алгоритмічних викривлень [4].

Порівняння результатів показує, що хоча більшість авторів зосереджуються або на окремих технологічних аспектах когнітивних викривлень [1, 4], або на їхніх проявах у конкретних організаційних контекстах [3, 5], поточне дослідження інтегрує міждисциплінарний підхід, доповнюючи його класифікацією за фазами життєвого циклу ІС та багаторівневою структурою впливів. Обмеженням дослідження є його теоретичний характер. Перспективи подальших досліджень включають верифікацію класифікації на реальних проєктних командах та розробку адаптивних інструментів для виявлення і компенсації когнітивних викривлень.

ДЖЕРЕЛА

1. Gomroki G., Behzadi H., Fattahi R., Salehi Fadardi J. (2023) Identifying effective cognitive biases in information retrieval. Journal of Information Science, 49(2), 348–358.
2.Bertrand A., Belloum R., Eagan J.R., Maxwell W. (2022) How cognitive biases affect XAI-assisted decision-making: A systematic review. Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society, pp. 78–91.
3. Hristov I., Camilli R., Mechelli A. (2022) Cognitive biases in implementing a performance management system. Management Research Review, 45(9), 1110–1136.
4. Kordzadeh N., Ghasemaghaei M. (2022) Algorithmic bias: Review, synthesis, and future research directions. European Journal of Information Systems, 31(3), 388–409.
5. Oschinsky F.M., Stelter A., Niehaves B. (2021) Cognitive biases in the digital age. Government Information Quarterly, 38(4), 101611.



ВЛАДИСЛАВ БЕЗУГЛИЙ
Аспірант, Факультет інформаційних технологій (кафедра інформаційних систем та технологій), Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0001-7338-3060
E-mail: bezuhlyiv@fit.knu.ua
Отримав ступінь бакалавра програмної інженерії у Національному технічному університеті України «Київському політехнічному інституті імені Ігоря Сікорського» (Київ, Україна) у 2014 році та ступінь магістра з інформаційних систем та технологій в Київському національному університеті імені Тараса Шевченка (Київ, Україна) у 2024 році, нині автор працює над здобуттям ступеня PhD з інформаційних систем та технологій в Київському національному університеті імені Тараса Шевченка (Київ, Україна). Серед наукових інтересів – проєктування інформаційних систем, інформаційні технології.



ОЛЬГА КРАВЧЕНКО
Доцент, доцент кафедри інформаційних систем та технологій, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-9669-2579
E-mail: olha.kravchenko@knu.ua
К.т.н., доцент, доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка (Київ, Україна). Серед наукових інтересів – проєктування систем моніторингу та прогнозування з урахуванням правил штучного інтелекту на основі поведінкової економіки, застосування IoT.

МЕТОДОЛОГІЯ ВИЯВЛЕННЯ ВРАЗЛИВИХ ГРУП НАСЕЛЕННЯ ДЛЯ РИЗИКОРІЄНТОВАНОГО МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ

Кирило Вадурін, Артем Васильєв, Іван Перекрест

Анотація. *Метою роботи є розробка аналітичного підґрунтя для ризикорієнтованої системи моніторингу атмосферного повітря шляхом виявлення кореляцій між концентрацією діоксиду азоту та психофізіологічними показниками людини. У дослідженні застосовано методи багатофакторної лінійної регресії, кореляційний аналіз Пірсона та методи кластеризації часових рядів на основі даних проєкту CitieS-Health. Встановлено статистично значущий негативний вплив діоксиду азоту на індекс ментального здоров'я, тоді як вплив на когнітивну швидкість виявився несуттєвим. Ідентифіковано географічні зони підвищеної вразливості, де зниження ментального індексу досягає 0,84 бала при зростанні забруднення. Практична цінність полягає у формуванні алгоритмів для персоналізованих екологічних попереджень.*

Ключові слова: системний аналіз, моніторинг якості повітря, діоксиду азоту, ментальне здоров'я, персоналізовані ризики, кореляційний аналіз, data mining.

I. ВСТУП

Тенденції розвитку інформаційних систем екологічного моніторингу у 2025–2026 роках характеризуються переходом від статичних спостережень до динамічних, людиноцентричних моделей. Традиційні мережі стаціонарних станцій контролю якості повітря надають усереднені дані, які часто не відображають реального експозиційного навантаження на конкретну особу, особливо в умовах щільної міської забудови та варіативної мобільності населення. Дослідження [1] демонструють, що використання персональних моніторів у поєднанні з даними про спосіб життя дозволяє прогнозувати загострення респіраторних захворювань зі значно вищою точністю. Водночас у інших дослідженнях [2] автори наголошують, що оцінки, базовані виключно на місці проживання, ігнорують мобільність особи, що призводить до суттєвих похибок у визначенні ризиків.

Однак в існуючих підходах спостерігається науковий пробіл: більшість систем фокусуються виключно на фізичних показниках здоров'я (респіраторна функція, серцевий ритм), залишаючи поза увагою психоемоційний стан людини як індикатор короткострокового впливу забруднення. Відсутність інтегрованих моделей, що враховують вплив атмосферних полютантів на когнітивні функції та рівень стресу, знижує ефективність превентивних заходів. Метою цієї роботи є проведення серії попередніх експериментів на історичних даних для підтвердження гіпотез щодо впливу NO_2 на психофізіологічний стан та формування стратегії для розгортання ризикорієнтованої системи моніторингу на основі indoor/outdoor пристроїв.

II. ДАНІ ТА МЕТОДИ

Об'єктом дослідження обрано масив даних CitieS-Health [3], зібраний у Барселоні (Іспанія), який містить 3348 записів, що охоплюють період з 2020 по 2021 рік. Набір даних включає часові мітки, геопросторову прив'язку (райони міста), демографічні характеристики учасників (вік, стать, освіта), результати когнітивних тестів (тест Струпа), суб'єктивні оцінки самопочуття та об'єктивні виміри концентрації діоксиду азоту та твердих часток ($PM_{2.5}$).

Методологія дослідження базується на принципах системного аналізу даних (CRISP-DM) і включає етапи попередньої обробки, конструювання ознак та статистичного моделювання. На етапі підготовки даних здійснено оптимізацію типів змінних для зменшення використання оперативної пам'яті (downcasting float64 до float32), що є

необхідним для проєктування архітектури реального часу. Категоріальні змінні, такі як район проживання та стать, трансформовано у відповідні формати для зручного групування.

Для кількісної оцінки впливу забруднення на психоемоційний стан запропоновано та реалізовано інтегральний показник «Індекс ментального здоров`я» (MHI). Розрахунок MHI здійснено шляхом агрегації нормалізованих значень самооцінки добробуту, енергії та інвертованого показника стресу. Математична модель MHI описується формулою усереднення складових, де вищі значення відповідають кращому стану:

$$MHI=B+En+(10-Es)3. \quad (1)$$

У формулі 1: B – суб'єктивна оцінка добробуту (із вхідних даних); En – суб'єктивна оцінка рівня енергії (із вхідних даних); Es – рівень стресу.

Аналіз впливу екологічних факторів на когнітивні здібності проводився з використанням показника P – швидкості та точності виконання тесту Струпа. Для перевірки гіпотез застосовано метод найменших квадратів у рамках багатофакторної регресійної моделі, де незалежними змінними виступали концентрація NO_2 та вік респондентів, а залежними – MHI та P. Додатково проведено аналіз чутливості підгруп із використанням методів розщеплення для оцінки впливу контекстуальних факторів, таких як пандемія COVID-19.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У ході експерименту було перевірено дві базові гіпотези: про вплив короткострокового забруднення повітря на когнітивну швидкість та на ментальне благополуччя. Результати регресійного аналізу продемонстрували відсутність прямого лінійного зв'язку між добовою концентрацією NO_2 та результатами когнітивного тесту Струпа. Коефіцієнт регресії для змінної NO_2 склав 0,016 при p-значенні 0,28, що свідчить про статистичну незначущість. Водночас, як виявлено з розподілу впливу факторів, домінуючим предиктором когнітивної ефективності є вік учасника ($p<10-100$), який пояснює левову частку дисперсії результатів.

Натомість аналіз впливу якості повітря на ментальне здоров'я виявив високозначущу негативну кореляцію. Як продемонстровано на Рисунку 1, коефіцієнт впливу NO_2 на MHI є від'ємним (-0,021) із рівнем значущості $p<10-18$. Це дозволяє стверджувати, що зростання концентрації діоксиду азоту є незалежним стресором, що призводить до статистично достовірного зниження суб'єктивного відчуття благополуччя, незалежно від віку респондентів ($p=0,08$ для вікового фактора).

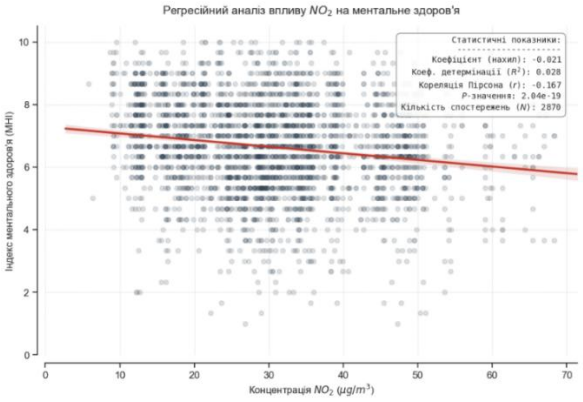


Рисунок 1. *Узагальнена візуалізація регресійної моделі*

Детальний аналіз підгруп виявив суттєву гетерогенність реакції населення залежно від району проживання та статі. Дані, наведені в Таблиці 1, свідчать про існування зон

підвищеної екологічної вразливості. Зокрема, у районі Gràcia зафіксовано найбільше падіння індексу ментального здоров'я при переході від низьких до високих рівнів забруднення: для чоловіків зниження склало 0,84 бала, для жінок – 0,76 бала за 10-бальною шкалою. Це контрастує з районом Ciutat Vella, де для чоловічої вибірки зафіксовано аномальне зростання індексу (+0,31), що потребує подальшого дослідження соціокультурних факторів.

Таблиця 1. *Зміна індексу ментального здоров'я залежно від рівня NO_2 та статі у районах*

Район	Стать	MHI (Низький NO_2)	MHI (Високий NO_2)	Падіння
Gràcia	Male	7,35	6,51	-0,84
Gràcia	Female	7,09	6,33	-0,76
Sant Martí	Male	7,30	6,64	-0,66
Sant Martí	Female	6,91	6,38	-0,53
Eixample	Male	6,78	6,31	-0,47

Дослідження взаємодії факторів показало, що контекстуальний стрес суттєво модулює чутливість до забруднення. Респонденти, які зазначили погіршення настрою через пандемію COVID-19, продемонстрували крутіший нахил лінії регресії MHI від NO_2 порівняно з тими, чий настрій не змінився. Це підтверджує гіпотезу про кумулятивний ефект стресорів: екологічне навантаження чинить сильніший деструктивний вплив на осіб із попередньо зниженим психологічним ресурсом.

Аналіз часових рядів виявив синхронність пікових значень забруднення та рівня стресу. У січні 2021 року спостерігався одночасний максимум середньої концентрації NO_2 (33 мкг/м³) та рівня стресу (4,7 балів), після чого обидва показники продемонстрували тенденцію до зниження. Така динаміка підтверджує валідність використання даних атмосферного моніторингу як предиктора періодів підвищеного соціального напруження.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Отримані результати дають підстави для перегляду архітектури систем персоналізованого моніторингу. Встановлено, що традиційний підхід до оцінки ризиків, який базується виключно на фізичних гранично допустимих концентраціях, є недостатнім. Доведення статистично значущого зв'язку між рівнями NO_2 та ментальним здоров'ям вказує на необхідність включення психофізіологічних показників у контур зворотного зв'язку системи моніторингу.

Відсутність кореляції з когнітивною швидкістю P свідчить про те, що короткострокові коливання якості повітря не чинять миттєвого впливу на базові нейрофізіологічні механізми реакції, або ж цей вплив ефективно компенсується організмом. Натомість емоційна сфера виявляється більш лабільною і чутливою до екзогенних хімічних подразників. Це узгоджується з висновками у статті [4] щодо необхідності врахування локальних екологічних умов при прогнозуванні загострень захворювань, розширюючи цей принцип на сферу ментального здоров'я.

Виявлена географічна неоднорідність чутливості населення підтверджує необхідність переходу від загальноміських оповіщень до гіперлокальних стратегій. Висока щільність забудови та, ймовірно, менша кількість зелених зон у певних районах можуть виступати каталізаторами негативного впливу забруднення. Це корелює з результатами викладеними у роботі [5], які вказують на складну залежність «експозиція-реакція».

Отже, на основі історичних даних підтверджено гіпотезу про значущий вплив забруднення повітря на психоемоційний стан та спростовано гіпотезу про миттєвий вплив на когнітивну швидкість. Сформовано методологічний базис для наступного етапу розробки системи, який передбачає інтеграцію носимих пристроїв. Перспективним напрямком

подальших досліджень є розробка алгоритмів машинного навчання для прогнозування індивідуальної реакції на забруднення з урахуванням даних indoor-моніторингу, як це запропоновано у роботі [6], що дозволить створити замкнений контур управління екологічними ризиками здоров'ю.

ДЖЕРЕЛА

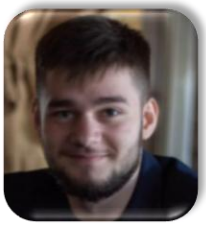
1. Atzeni M., Cappon G., Quint J. K. [et al.]. A machine learning framework for short-term prediction of chronic obstructive pulmonary disease exacerbations using personal air quality monitors and lifestyle data // Scientific Reports. 2025. Vol. 15, no. 1. P. 2385. URL: https://doi.org/10.1038/s41598-024-85089-2.
2. Bashan N. F., Zhang Y., Bell M. L., Wang Q. R. Mobility-driven estimate reveals elevated air pollution exposure and socioeconomic disparities beyond residence-based approaches in Boston // Journal of Exposure Science & Environmental Epidemiology. 2025. URL: https://doi.org/10.1038/s41370-025-00820-z.
3. The Devastator. Air Pollution and Mental Health: Identifying Short-Term Human Impacts of Air Pollution [Data set] // Kaggle. 2022. URL: https://www.kaggle.com/datasets/thedevastator/air-pollution-and-mental-health.
4. Bhowmik R. T., Most S. P. A Personalized Respiratory Disease Exacerbation Prediction Technique Based on a Novel Spatio-Temporal Machine Learning Architecture and Local Environmental Sensor Networks // Electronics. 2022. Vol. 11, no. 16. P. 2562.
5. Balakrishnan K., Steenland K., Clasen T. [et al.]. Exposure–response relationships for personal exposure to fine particulate matter (PM2.5), carbon monoxide, and black carbon and birthweight: an observational analysis of the multicountry Household Air Pollution Intervention Network (HAPIN) trial // The Lancet Planetary Health. 2023. Vol. 7, no. 5. P. e387–e396. URL: https://doi.org/10.1016/S2542-5196(23)00052-9.
6. Bernasconi S., Angelucci A., Rossi A., Aliverti A. A New Wearable System for Personal Air Pollution Exposure Estimation: Pilot Observational Study // JMIR Mhealth Uhealth. 2025. Vol. 13. Art. e60426. URL: https://doi.org/10.2196/60426.



КИРИЛО ВАДУРІН
асистент кафедри комп'ютерної інженерії та електроніки у Кременчуцького національного університету імені Михайла Остроградського, Кременчук, Україна.
ORCID: 0000-0001-7781-5783
E-mail: kir3337@gmail.com
Мій досвід поєднує проєктування складних апаратних комплексів із побудовою прогностичних моделей на основі нейронних мереж для цифровізації муніципальних та промислових об'єктів.



АРТЕМ ВАСИЛЬЄВ
аспірант 1-го курсу кафедри екології та біотехнології Кременчуцького національного університету імені Михайла Остроградського, Кременчук, Україна.
ORCID: 0009-0005-6307-1396
E-mail: VasylievArtem@proton.me
Працюю над створенням концепції ризикорієнтованої системи персоналізованого моніторингу атмосферного повітря на основі даних indoor/outdoor пристроїв.



ІВАН ПЕРЕКРЕСТ
здобувач 4-го курсу спеціальності 171 Електроніка у Кременчуцькому національному університеті імені Михайла Остроградського, Кременчук, Україна.
ORCID: 0009-0007-8285-9351
E-mail: ivanperekrest@proton.me
Працюю над впровадженням штучного інтелекту та великих мовних моделей для автоматизації підготовки даних у сучасних екологічних екосистемах та біометричних комплексах.

ПРО ОДНУ УЗАГАЛЬНЕНУ МОДЕЛЬ ЗАДАЧІ КОМІВОЯЖЕРА ЗА НАЯВНІСТЮ ОБМЕЖЕНЬ ВИПЕРЕДЖЕННЯ

Валерій Гавриленко, Катерина Івохіна

Анотація. *В даній статті розглянуто метод розв'язання узагальненої задачі комівояжера, яка формулюється як задача пошуку маршруту відвідування заданої кількості кластерів, що визначаються на множині міст транспортної мережі. Ставиться завдання побудови оптимального маршруту відвідування міст мережі без повторень та з мінімальними витратами при пересуванні. Розглянуто варіанти мегаполісів без обмежень та з обмеженнями щодо формування їх змісту. Пропонується метод побудови кластерів з урахуванням заданих обмежень на кількісні та ресурсні показники потужності, що дозволяє сформувати відносно однорідні за змістом мегаполіси та шукати оптимальні маршрути в узагальненій задачі комівояжера за спеціальною процедурою.. Отримано результати розрахунку розв'язків задачі комівояжера з різними параметрами обмежень, зроблено висновки щодо доцільності запропонованого способу групування міст мережі.*

Ключові слова: задача комівояжера, мегаполіси, кластеризація, обмеження групування, оптимізація.

I. ВСТУП

Узагальнена задач комівояжера (GTSP) є розширенням класичної задачі, в якій множина міст розділена на мегаполіси (кластери), що не перетинаються між собою, причому кожен кластер має відвідуватися за маршрутом руху лише один раз. Задача має широкий спектр застосувань, серед яких, наприклад, задачі маршрутизації, планування рятувальних операцій тощо.

Така постановка задачі вимагає визначення порядку відвідування мегаполісів, в результаті чого пошук оптимального маршруту по всіх містах мережі буде залежати від якості обраного порядку. У цьому випадку отримуємо задачу з обмеженням випередження.

II. ДАНІ ТА МЕТОДИ

Вважаємо, що задано n множин $M_1,...,M_n$, які будемо називати мегаполісами, і початкова точка x_0, що не належіть жодній з них. Без обмеження загальності, можна вважати множині однієї потужності, що визначаються співвідношеннями $M_k = \{m_{k1},...,m_{kp}\}, k = \overline{1,n}$.

Разом з витратами $c(m_{lu}, m_{kv})$, які для довільних індексів $l \neq k, l,k = \overline{1,n}$, $u,v = \overline{1,p}$, можуть бути визначені у формі часових інтервалів на переміщення або відстаней між містами або транспортних витрат, задано відповідні витрати на переміщення $\bar{c}(x_0, m_{kv})$ і $\bar{c}(m_{kv}, x_0)$ з точки x_0 в кожну з точок m_{kv} і назад. Якщо відомі витрати на відвідування кожного мегаполісу $c'(m_{kv})$, то задача полягає у знаходженні маршруту з найменшими витратами, що починається та закінчується в точці x_0 і який проходить через усі мегаполіси лише один раз [1].

З математичної точки зору потрібно знайти перестановку $(j(1),j(2),...,j(n))$, яка називається маршрутом, що визначає порядок відвідування мегаполісів, та скінченну послідовність $m_{j(1)u(1)}, m_{j(2)u(2)},...,m_{j(n)u(n)}$, яка має назву траси, такі, щоб

$$\bar{c}(x_0, m_{j(1)v(1)}) + \sum_{i=1}^{n-1}(c'(m_{j(i)u(i)}) + c(m_{j(i)u(i)}, m_{j(i+1)u(i+1)})) + \bar{c}(m_{j(n)u(n)}, x_0) \to \min \qquad (1)$$

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Розглянуто спосіб розв'язання узагальненої задачі комівояжера на транспортній мережі з використання двоетапного підходу. Розв'язок задачі комівояжера шукається при заданих та отриманих шляхом групування сукупностях мегаполісів. У випадку відсутності кластерів на першому етапі міста мережі групуються в кластери, після чого для кожного кластеру знаходиться оптимальний розв'язок задачі комівояжера. Розглянуто різні варіанти топології формування кластерів: з обмеженою кількістю доступних шляхів та повнозв'язної топології. Запропоновано розв'язання задачі за умови руху комівояжера в кожному мегаполісі без повторного відвідування міст транспортної мережі. Досліджено способи розв'язування задачі без обмеження на повторне відвідування окремих пунктів мегаполісів, для чого розроблено модифікацію алгоритму Пріма. Наведено результати розрахунків, проведених для невеликої логістичної мережі на основі генетичного алгоритму, з використанням різних метрик, що використовуються для групування міст у мегаполіси.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У статті наведено результати розробки методів розв'язання узагальненої задачі комівояжера при різних варіантах задання мегаполісів на мережі. Отримано розрахунки, яі свідчать про конструктивність використання методології попередньої кластеризації для великої кількості міст мережі, застосування якої дозволяє покращити маршрути в задачі комівояжера порівняно з випадком без використання кластерів. Розглянуто два способи задання кластерів. Запропоновано узагальнення методу Пріма для пошуку оптимального маршруту комівояжера в межах мегаполісу. Наведено результати практичного застосування програмних засобів та технологій для розв'язання сформульованих оптимізаційних задач з метою покращення транспортних та мережевих потоків.

ДЖЕРЕЛА

1. Sultana N., Chan J., Sarwar T. (2022) Learning to optimise general TSP instances. Int. Journ. Mach. Learn. & Cyber., 13, 2213-2228.
2. Ivohin E.V., Gavrilenko V.V., Yushtin K.E., Ivohina K.E. (2026) About rational methods for finding optimal routes in fuzzy traveling salesman problems. RadioElectronics Computer Science, Control, 1, 56-63.



ВАЛЕРІЙ ГАВРИЛЕНКО
Д.ф.-м.н., завідувач кафедри інформаційних систем і технологій Національного транспортного університету, Київ, Україна
ORCID: 0000-0001-9682-4204
E-mail: vvgavrilenko1953@gmail.com
Наукові інтереси — моделі та методи розв'язання задач оптимізації, моделі штучного інтелекту.



КАТЕРИНА ІВОХІНА
PhD студентка кафедри інформаційних систем та технологій Національного транспортного університету, Київ, Україна
ORCID: 0000-0001-9940-1178
E-mail: ivohina@gmail.com
Наукові інтереси — методи розв'язання чіткіх та нечіткіх задач оптимізації, моделі транспортної та мережевої маршрутизації

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ І ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ ТЕХНІЧНОГО ДІАГНОСТУВАННЯ І МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ

Сергій Глухов, Олександр Бабій, Сергій Семеха

Анотація. *В роботі запропоновано методи забезпечення потрібного рівня надійності військової техніки з використанням сучасних інформаційних технологій при створенні автоматизованих систем технічного діагностування і метрологічного забезпечення під час обслуговування і ремонту. Завдання вирішується при експлуатації зразків техніки поповненням баз даних в реальному масштабі часу і з використанням запропонованих рішень в базах знань. При цьому враховано як особливості побудови військової техніки, так і умови її експлуатації в мирний та військовий час. Впровадження запропонованих рішень дозволяє забезпечити необхідний рівень надійності підвищенням якості метрологічного і діагностичного забезпечення технічного обслуговування і ремонту.*

Ключові слова: інформаційні технології, військова техніка, автоматизована система технічного діагностування.

I. ВСТУП І ПОСТАНОВКА ЗАДАЧІ

Модернізація матеріально-технічної бази ремонтних підрозділів шляхом впровадження сучасних засобів обчислювальної техніки та мобільних апаратних технічного забезпечення створює умови для розробки систем технічного діагностування на основі новітніх інформаційних технологій. Автоматизована система технічного діагностування (АСТД) призначена для проведення об’єктивної оцінки технічного стану цифрових пристроїв вимірювальних приладів під час їх обслуговування та повірки, скороченні термінів відновлення працездатності та кількісному аналізі значень показників надійності [1]. Висока ефективність запропонованого підходу досягається завдяки реалізації таких методів:

- оцінювання надійності об’єктів зі зміною структурою, що забезпечує підвищення точності розрахунку значення комплексного показника надійності до 12% за рахунок виявлення прихованих дефектів [2];
- оцінювання середнього часу відновлення техніки після зберігання завдяки використанню алгоритмів пошуку кратних дефектів удвічі збільшує пропускну здатність ремонтних органів [3];
- фізичного діагностування цифрових пристроїв вимірювальної техніки підвищує ймовірність правильного визначення технічного стану на 6% [4].

Автоматизована система метрологічного забезпечення (АСМЗ) — це комплекс технічних, програмних та організаційних засобів призначений для автоматизації процесів калібрування, повірки, обліку та контролю засобів вимірювальної техніки (ЗВТ). Вона забезпечує єдність, точність вимірювань, підвищує ефективність виробництва та автоматизує обробку вимірювальної інформації [5].

II. ОСНОВНА ЧАСТИНА. ДАНІ І МЕТОДИ. РЕЗУЛЬТАТИ І АНАЛІЗ

Побудова автоматизованої системи технічного діагностування для об’єктів радіоелектронної техніки (РЕТ) з метою покращення техніко-економічних показників передбачала розташування діагностичних модулів на першому рівні системи технічного обслуговування і ремонту (СТОіР), що обумовлено наступними причинами: масо-габаритними показниками об’єктів РЕТ; кількістю та різноманітністю об’єктів РЕТ;

особливостями побудови об’єктів РЕТ конструктивно передбачена вбудована система контролю, глибина визначення несправності якої обмежувалась, як правило, рівнем блоку; необхідністю визначення технічно несправних цифрових пристроїв на даному рівні СТОіР.

На відміну від АСТД [4], при побудові АСМЗ передбачається використання діагностичних модулів на другому рівні СТОіР, а саме, у метрологічних центрах, де здійснюється повірка та ремонт ЗВТ.

Наявність "місцевих" баз даних обліку ЗВТ на рівні підрозділів (відділів), створення яких було спричинене, у переважній більшості, для подолання складнощів, які поставали у деяких категорій службових осіб при пошуку відомостей про будь-який прилад і необхідність використання діагностичної інформації для прогнозування стану РЕТ викликає необхідність не тільки розбудови АСТД і АСМЗ, но і об'єднання баз знань і баз даних автоматизованих систем.

Під час експлуатації вимірювальної техніки поповнюється база даних системи технічного діагностування, а потім база знань із використанням отриманих результатів реалізує рішення перелічених завдань.

Об'єднання автоматизованих систем дозволяють: мати відомості щодо технічного стану ЗВТ; мати статистичні дані щодо виникнення несправностей ЗВТ; упереджувати виникнення несправностей ЗВТ при використанні фізичного діагностування; проводити розрахунок строків та обсягів проведення наступної повірки; отримати оновлений (адаптований) перелік робіт при проведенні наступної повірки.

Зазначене дозволить переходити до обслуговування ЗВТ за станом, що є дуже актуальним. Головні переваги технічного обслуговування за станом:

– економічна доцільність: змінюються лише ті деталі, які фактично зношені, що знижує витрати на запчастини;

– зростання (зменшення) міжремонтних інтервалів: здатність з високою точністю визначити залишковий ресурс дає змогу безпечно експлуатувати техніку довше, ніж при плановому технічному обслуговуванні;

– запобігання критичним несправностям: контроль стану (вібрація, температура, тощо) дозволяє знайти дефекти на ранній стадії, унеможливлюючи раптові аварії;

– підвищення безпеки: постійний нагляд технічного стану знижує ймовірність виникнення небезпечних ситуацій під час роботи техніки;

– скорочення простоїв: ремонт планується лише тоді, коли він дійсно потрібен, що зменшує час перебування техніки в ремонті;

– поліпшення ефективності: техніка, що працює в оптимальному стані, споживає менше ресурсів та має вищу продуктивність.

Використання інформаційних технологій полягає у: отриманні та обробці діагностичної інформації про технічний стан; передачі її від об’єктів до центрів обробки, зберіганні її на першому та другому рівнях СТОіР; прогнозуванні залишкового ресурсу; зберіганні інформації про технічний стан у базі даних; визначенні міжповірочних інтервалів базою знань АСМЗ. Ефективність автоматизованих систем зростає також завдяки документуванню результатів і можливості їх статистичної обробки із подальшим прогнозуванням значень показників метрологічної надійності окремих ЗВТ. Отримані наукові результати досліджень доведено до формалізованих алгоритмів використання та технічних рішень на основі реалізації сучасних інформаційних технологій, застосуванням методів теорії ймовірності, теорії експлуатації складних технічних систем, теорії дискретного пошуку і метрології.

III. ВИСНОВКИ

Отримані результати мають наукову і практичну спрямованість при проєктуванні перспективних зразків військової техніки, їх випробуваннях під час дослідної експлуатації із

використанням отриманих результатів в системах технічного діагностування в період нормальної експлуатації для забезпечення необхідних значень показників надійності удосконаленням діагностичного забезпечення.

Побудова автоматизованих систем та використання інформаційних технологій на основі фізичного діагностування дозволить зменшити кількість поступових відмов, які виникають у міжповірочний інтервал, збільшити середній наробіток на відмову, збільшити коефіцієнт готовності цифрових засобів вимірювань як комплексний показник надійності.

ДЖЕРЕЛА

1. Глухов С.І. Використання інформаційних технологій для прогнозування технічного стану об’єктів радіоелектронної техніки / С.І. Глухов, Л.М. Сакович, О.С. Бабій // Наука і техніка Повітряних Сил Збройних Сил України. – 2022. – № 1 (46). – С. 72-78.
2. Удосконалений метод оцінювання надійності об'єктів зі змінною структурою/ [О.С. Бабій, Л.М. Сакович, О.О. Слюсарчук, Ю.М. Єлісов, Я.Е. Курята] // Радіоелектроніка, інформатика, управління. – 2024. – №2. – С. 6-14 https://doi.org/10.15588/1607-3274-2024-2-1 .
3. Бабій О.С. Метод оцінки середнього часу відновлення радіоелектронних засобів після короткочасного зберігання / О.С. Бабій, Л.М. Сакович // Вісті вищих учбових закладів. Радіоелектроніка. – 2024. – Том 67 №2. – С.91-99. https://doi.org/10.20535/S002134702312004X.
4. С.І. Глухов, С.М. Семеха, М.В. Мороз, О.О. Кушнір. Використання інформаційних технологій для оцінювання технічного стану засобів вимірювальної техніки на основі фізичного діагностування / Системи озброєння і військова техніка. – 2025. – № 2(82) С. 50-55
5. Побудова автоматизованої системи метрологічного забезпечення цифрових вимірювальних приладів з використанням інформаційних технологій / [О.С. Бабій, С.І. Глухов, Л.М. Сакович, В.В. Козєл, С.М. Семеха] // Scientific Collection «InterConf+», №45 (201), 8th International Scientific and Practical Conference «International Scientific Discussion: Problems, Tasks and Prospects», Brighton, Great Britain, 19-20 May 2024



СЕРГІЙ ГЛУХОВ
доктор технічних наук, професор, завідувач кафедри Київського національного університету імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0002-4918-3739
E-mail: gluhov1971@ukr.net



ОЛЕКСАНДР БАБІЙ
старший викладач Київського національного університету імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0001-5752-5025
E-mail: al-babij@ukr.net



СЕРГІЙ СЕМЕХА
начальник факультету професійної військової та післядипломної освіти Військового інституту Київського національного університету імені Тараса Шевченка, Київ, Україна.
ORCID: 0000-0003-3539-2051
E-mail: serhio174@ukr.net

ПРОГРАМНИЙ МОДУЛЬ ВИЯВЛЕННЯ ОЗНАК МАНІПУЛЮВАННЯ В НАУКОМЕТРИЧНІЙ БАЗІ SCOPUS

Григорій Гнатієнко, Артур Домбровський

Анотація. *У роботі запропоновано метод аналізу форми розподілу цитувань наукових публікацій за допомогою гіперболічної апроксимації (закон Ціпфа) для виявлення штучного підвищення наукометричних показників у базі Scopus. Розроблено програмний модуль, який класифікує профілі на основі інтегрального показника підозри, що враховує локальні відхилення (NRMSE) та нахил кривої (параметр α). Це дозволяє виявляти «картелі цитувань» та перехресне самоцитування, що характеризуються аномально плоскими розподілами.*

Ключові слова: Scopus, маніпулювання цитуваннями, закон Ціпфа, гіперболічна апроксимація, h-індекс.

I. ВСТУП

Необхідність застосування різних підходів до виявлення ознак маніпулювання науковцями популярністю в наукометричній базі є очевидною та актуальною [1, 2]. У таких випадках проблема полягає у тому, щоб на основі розроблених математичних моделей забезпечити достовірний аналіз профілів науковців та виявлення ознак маніпулювання науковцями популярністю в наукометричній базі [3, 4].

У сучасному науковому світі наукометричні показники відіграють ключову роль в оцінюванні продуктивності дослідників та розподілі фінансування. Водночас зростання значення кількісних показників призвело до появи нечесних практик – надмірне самоцитування, створення «картелів цитування», публікації у хижацьких журналах, подрібнення та деталізація наукових результатів тощо [5]. Маніпулювання наукометричними даними призводить до необґрунтованого та неоптимального розподілу коштів, які виділяються на фінансування науки [6].

Очевидно, що існуючі методи оцінювання, зокрема, h-індекс, не є стійкими до маніпуляцій. Крім того, наявні програмні засоби не надають автоматизованого аудиту профілів науковців. Також виявлено, що просте відстеження відхилень від теоретичного розподілу (похибка апроксимації) може бути недостатнім для виявлення складних схем маніпуляцій [7]. Розподіл цитувань наукових публікацій підпорядковується загальним закономірностям, які можуть бути описані математичними моделями.

II. ОСНОВНА ЧАСТИНА

Упорядкуємо публікації у профілі автора за спаданням їхньої цитованості. Для апроксимації розподілу цитувань обрано трипараметричну гіперболічну функцію, що описує залежність кількості цитувань c(i) від рангу публікації i:

$$c(i) = \frac{A}{(B+i)^{\alpha}}, \quad (1)$$

Параметри моделі (1) мають такий зміст:

- *параметр* A *(Scale Parameter):* визначає абсолютний масштаб цитованості;
- *параметр* B *(Shift Parameter):* характеризує «плато» високоцитованих робіт на початку графіка;
- *параметр* α *(Shape Parameter):* визначає швидкість спадання «хвоста» розподілу.

Значення $\alpha > 1$ вказують на швидкий спад інтересу до старих або менш значущих робіт, що є характерним для природного розподілу уваги до наукових здобутків. Значення $\alpha < 1$ (та особливо $\alpha < 0.8$) свідчать про аномально «плоский» розподіл, де навіть роботи з низьким рангом мають значну кількість цитувань. Це може бути індикатором штучної підтримки показників.

У багатьох дослідженнях як основний індикатор аномальності використовується нормалізована середньоквадратична похибка (NRMSE), яка характеризує відхилення емпіричних даних від теоретичної кривої:

$$NRMSE = \frac{\sqrt{\frac{1}{N}\sum_{i=1}^{N} ([c_{obs}(i) - c_{model}(i)]^2)}}{c_{max} - c_{min}}, \quad (2)$$

де N– загальна кількість публікацій автора;

$c_{obs}(i)$ – фактична кількість цитувань публікації з рангом i;

$c_{model}(i)$ – прогнозована кількість цитувань за формулою (1);

c_{max} , c_{min} – максимальна та мінімальна кількість цитувань у профілі.

Однак використання лише метрики NRMSE є недостатнім. Деякі маніпулятивні профілі можуть зберігати гладку форму гіперболи (низький NRMSE), але мати неприродно пологий нахил, що описується параметром α у формулі (1).

Тому для класифікації профілів у цій роботі запропоновано інтегральний показник підозри (S_{score}), який є зваженою сумою двох факторів:

– *фактор форми (NRMSE):* виявляє локальні аномалії («сходинки», різкі обриви тощо), характерні для накрутки h-індексу під конкретне значення;

– *фактор нахилу (Alpha Score):* виявляє глобальні аномалії. Неприродно низьке значення α (пологий графік) свідчить про штучну підтримку слабких статей.

Математична модель інтегрального показника має вигляд:

$$S_{score} = w_a \cdot score_a + w_{nrmse} \cdot score_{nrmse}, \quad (3)$$

де w_a, w_{nrmse} – вагові коефіцієнти значущості (у роботі прийнято 0.45 та 0.55 відповідно);

$score_a = max(0, \frac{\alpha_{ref} - \alpha}{\alpha_{ref}})$ – штраф за відхилення параметра α від референсного значення α_{ref} (для природних розподілів $\alpha_{ref} \approx 1.15$);

$score_{nrmse} = min(1, \frac{NRMSE}{NRMSE_{ref}})$ – штраф за похибку апроксимації (де $NRMSE_{ref} \approx 0.07$).

Такий підхід дозволяє значно підвищити чутливість системи до різних видів маніпуляцій порівняно з використанням лише NRMSE.

Для реалізації методу виявлення ознак маніпулювання на основі гіперболічної апроксимації (закон Ціпфа) розроблено архітектуру програмної системи, яка забезпечує інтеграцію з офіційним Scopus API, обробку даних, апроксимацію розподілу цитувань та візуалізацію результатів. Архітектура включає шість основних компонентів:

– *модуль інтеграції (Scopus API Client):* забезпечує отримання даних про автора через офіційний API Elsevier;

– *модуль обробки даних (Data Processor):* виконує парсинг отриманих JSON-відповідей та формування структурованих даних для аналізу;

– *модуль апроксимації (Approximation Engine):* реалізує алгоритм підбору параметрів гіперболи (A, B, α) методом найменших квадратів та обчислення NRMSE;

– *модуль візуалізації (Visualizer):* створює графіки розподілу цитувань;

– *модуль збереження (Database Manager):* забезпечує збереження результатів у базі даних SQLite;

– *графічний інтерфейс (GUI):* надає зручний інтерфейс для взаємодії з системою.

Для підбору оптимальних параметрів гіперболічної моделі, які описуються формулою (1), використовується метод найменших квадратів, який мінімізує суму квадратів відхилень:

$$L(A,B,\alpha) = \sum_{i=1}^{N} w_i(c_{obs}(i) - \frac{A}{(B+i)^{\alpha}})^2 \rightarrow min, \quad (4)$$

Для підвищення точності апроксимації на «хвостах» розподілу у класичний метод найменших квадратів введено логарифмічне зважування. Вага кожної точки (w_i) у цільовій функції мінімізації визначається так:

$$w_i = \frac{1}{1+ln(c_i+1)}. \quad (5)$$

Це змушує алгоритм апроксимації враховувати структуру всього масиву публікацій автора, а не лише кількох високоцитованих статей.

Експериментальну перевірку розробленого методу та програмного модуля проведено на вибірці з 40 реальних профілів авторів бази Scopus. Результати автоматизованої класифікації продемонстрували збалансовану точність (Accuracy) та метрику F1-Score на рівні 75%. Під час детального аналізу хибних спрацювань алгоритму (кейс-стаді) було виявлено фундаментальну проблему перенавчання (overfitting) трипараметричної моделі.

Математично доведено, що під час аналізу профілів із наявністю «картелів цитувань», параметр зсуву B діє як «абсорбер аномалій», маскуючи штучні горизонтальні плато розподілу. Крім того, виявлено вразливість класичної метрики NRMSE до «ефекту блокбастера» (екстремального перепаду цитованості).

Для усунення цих обмежень обґрунтовано необхідність переходу до двопараметричної моделі з використанням методу максимальної вірогідності (MLE) [8], застосування логарифмічних метрик (RMSLE) та інтеграції графового аналізу для побудови комплексного індексу довіри Trust Factor.

III. ВИСНОВКИ

Розроблена система автоматизованого виявлення ознак маніпулювання може бути використана університетами та науковими установами для перевірки профілів кандидатів на академічні посади, грантовими агенціями для оцінювання заявників на фінансування досліджень, а також науковцями для самоперевірки власних профілів у Scopus. Система забезпечує аналіз та опосередковано підвищення академічної доброчесності та сприяє справедливому розподілу наукових ресурсів.

ДЖЕРЕЛА

1. Гнатієнко Г.М., Олецький О.В. Порівняння методик ранжування науковців на основі індексів Гірша та PageRank: суперечливі ситуації // Сучасні інформаційні технології. – 2021. – №1(1). С.39-44.

2. Гнатієнко Г. Непрямі методи визначення ознак маніпулювання популярністю авторів у наукометричних базах даних / Матеріали 2-ї Міжнародної науково-практичної конференції «Інформаційні системи та технології: результати і перспективи» (IST 2025), 5 березня 2025 р. (Київ, Україна). К.: ФІТ КНУТШ, 2025 р. С.388-393.
3. Діденко Ю. В., Радченко А. І. (2017) Публікаційна активність як спосіб наукової комунікації та гонитви за рейтингами. Вісник Національної академії наук України, 9, 82–98.
4. Гнатієнко Г., Снитюк В., Тмєнова Н. Метод класифікації наукових результатів науковців на основі аналізу їхніх профілів у SCOPUS // Прикладні інформаційні системи та технології в цифровому суспільстві: зб. тез доповідей і наук. повідомл. учасників IX Міжнародної науково-практичної конференції (Київ, 01 жовтня 2025 р.) / за заг. ред. В. Плескач, О. Фендьо. К.: Київський нац. ун-т ім. Тараса Шевченка, 2025. С. 77-89.
5. Fong E. A., Wilhite A. W. (2017) Authorship and citation manipulation in academic research. PLoS ONE, 12(12), e0187394.
6. Else H., Van Noorden R. (2021) The fight against fake-paper factories that churn out sham science. Nature News, 591, 516–519.
7. Radicchi F., Fortunato S., Castellano C. (2008) Universality of citation distributions: Toward an objective measure of scientific impact. Proceedings of the National Academy of Sciences, 105(45), 17268–17272.
8. Clauset A., Shalizi C. R., Newman M. E. J. (2009) Power-law distributions in empirical data. SIAM Review, 51(4), 661–703.



ГРИГОРІЙ ГНАТІЄНКО
К.т.н., заступник декана з наукової роботи факультету інформаційних технологій, Київський національний університет імені Тараса Шевченка, м.Київ, Україна
ORCID: 0000-0002-0465-5018
E-mail: g.gna5@ukr.net
отримав диплом спеціаліста прикладної математики у Київському національному університеті імені Тараса Шевченка (Київ, Україна) в 1984 році та ступінь кандидата технічних наук у Київському національному університеті імені Тараса Шевченка (Київ, Україна) в 1994. Нині автор працює над здобуттям ступеня доктора технічних наук. Серед наукових інтересів – системи підтримки прийняття рішень, методи обробки експертної інформації, моделювання складних систем.



АРТУР ДОМБРОВСЬКИЙ
студент 4 курсу бакалаврату, кафедра інформаційних систем та технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
E-mail: anytguy@gmail.com
Здобуває ступінь бакалавра за спеціальністю «Комп'ютерні науки». Має практичний досвід у розробці інформаційно-аналітичних систем. Наукові інтереси включають наукометрію, машинне навчання (ML), автоматизований аналіз великих даних та розробку алгоритмів для виявлення системних аномалій.

СТРУКТУРА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Олексій Гнатієнко, Владислав Сингаївський

Анотація. *У цьому дослідженні представлено важливість та актуальність вирішення проблеми забезпечення функціональної стійкості інформаційної системи. Наведено схему взаємодії факторів, які забезпечують функціонування внутрішнього середовища організаційної системи. Авторами запропоновано структурну схему інформаційних потоків забезпечення стійкого функціонування організаційної системи. Розглянуто також схему взаємодії підсистем, які складають автоматизовану систему обчислення, забезпечення та обґрунтування функціональної стійкості організаційної системи.*

Ключові слова: організаційна система, функціональна стійкість, забезпечення надлишковості, корпоративна культура, інфраструктура організаційної системи.

I. ВСТУП

В сучасних умовах, які характеризуються різноманітними викликами та динамічністю впливів зовнішнього середовища на організації, надзвичайно важливим є своєчасне визначення нештатних ситуацій у діяльності організаційних систем (ОС) та підтримка їх тривалого функціонування на високому рівні. Актуальність вирішення цієї проблеми обумовлена необхідністю усунути наявні протиріччя між існуючими методами та моделями виявлення нештатної ситуації, застосуванням існуючої в ОС надлишковості, оцінюванням якості застосування варіантів заміни виконавців функцій ОС та необхідністю підтримки функціональної стійкості (ФС) ОС. Слід зазначити, що сучасні виклики вимагають підвищення ефективності діяльності організаційних систем [1]. Причому, існуючий інструментарій вирішує ці протиріччя не в повному обсязі і вимагає створення нових інструментів, які дозволять ефективно забезпечити вирішення зазначених задач.

II. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Авторами розроблено необхідні умови забезпечення ФС ОС, при задоволенні яких значною мірою буде покращена якість функціонування системи. Серед таких умов слід у першу чергу навести:

– оперативне виявлення нештатної ситуації та активація процедури заміни елементів ОС;

– завчасне виявлення джерел надлишковості для парирування нештатних ситуацій;

– достовірна оцінка якості функціонування ОС при різних варіантах заміни виконавців функцій;

– зважене та обґрунтоване прийняття рішення щодо заміни виконавців функцій в умовах обмеженого часу;

– удосконалення корпоративної культури та системи управління організації в цілому;

– розробка та впровадження в ОС системи мотивації, спрямованої на забезпечення функціональної стійкості ОС.

Для забезпечення виконання наведених необхідних умов важливим атрибутом є належна підготовка та підтримка у відповідному стані внутрішнього середовища ОС. На рисунку 1 наведено схему внутрішнього середовища ОС.

При виконанні умов ефективного та стійкого забезпечення функціонування ОС слід створити особливу конфігурацію відповідної системи підтримки такої діяльності. Структурну схему автоматизованої системи забезпечення ФС ОС наведено на рисунку 2.



Рисунок 1. *Схема внутрішнього середовища організаційної системи*

У роботі [2] описано концепцію побудови автоматизованої системи забезпечення ФС ОС. А в роботі [3] розглянуто сучасні тенденції в галузі функціональної стійкості складних систем. На основі цих робіт авторами розроблено структурну схему такої автоматизованої системи. Основні елементи такої автоматизованої системи, взаємозв'язки між ними та відповідні інформаційні потоки представлено на рисунку 2.

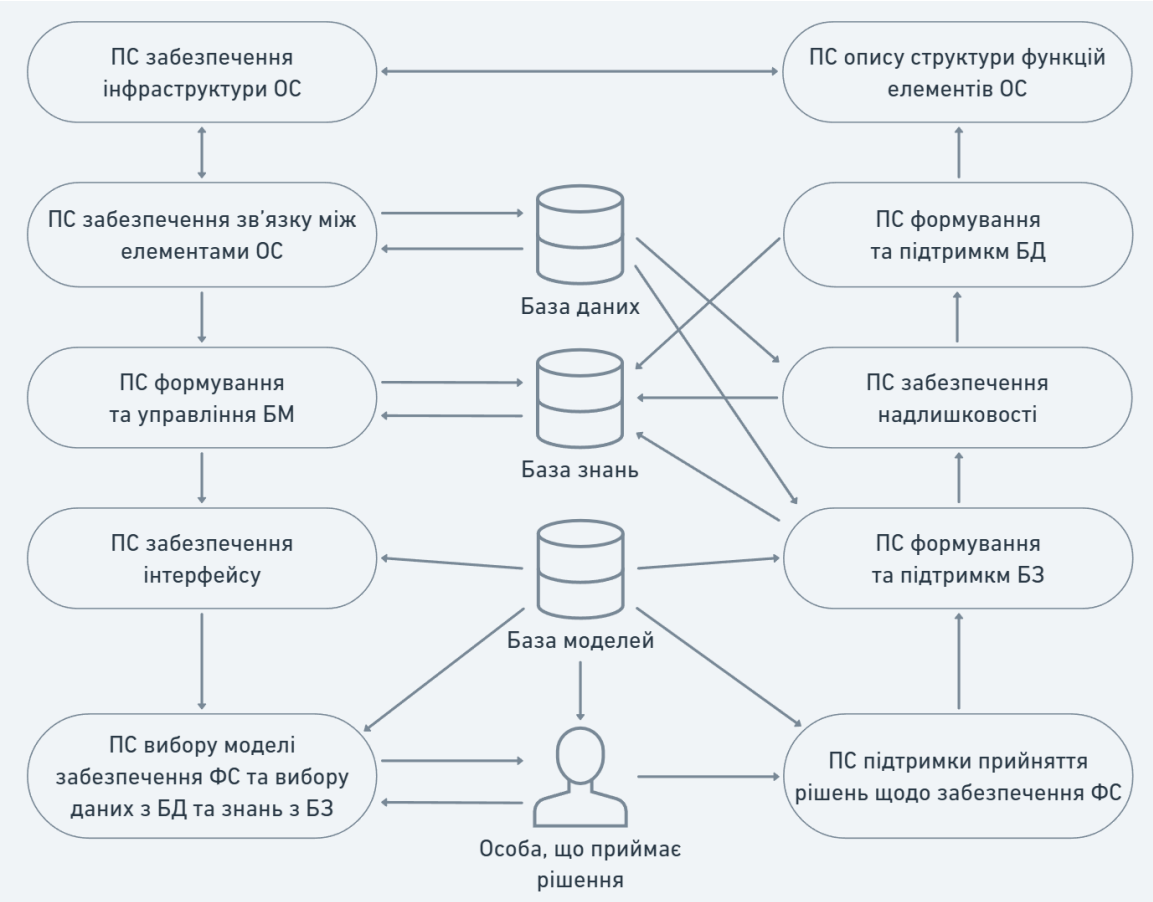


Рисунок 2. *Структурна схема інформаційних потоків системи забезпечення ФС ОС*

У стандарті ISO 9000:2015 [4, 5] фундаментальним є поняття «*контекст організації*» або «*середовище організації*». Згідно зі стандартом ISO 9000:2015, *контекст організації* – це

сукупність внутрішніх та зовнішніх чинників, які можуть впливати на підхід організації до розроблення та досягнення її цілей. При цьому основними складовими контексту є зовнішні та внутрішні чинники. *Зовнішні чинники* – це правове, технологічне, конкурентне, економічне тощо середовище. *Внутрішні чинники* – це цінності ОС, корпоративна культура, знання, ресурси тощо. І у цьому контексті, організація – це сукупність (група) людей та засобів виробництва з розподілом відповідальності, повноважень та взаємовідносин.

Для успішного функціонування інформаційних потоків, представлених на рисунку 2, необхідно реалізувати інтелектуальну систему підтримки прийняття рішень. Перелік та особливості взаємодії підсистем (ПС) такої системи, розробленої авторами цієї роботи, наведено на рисунку 3.

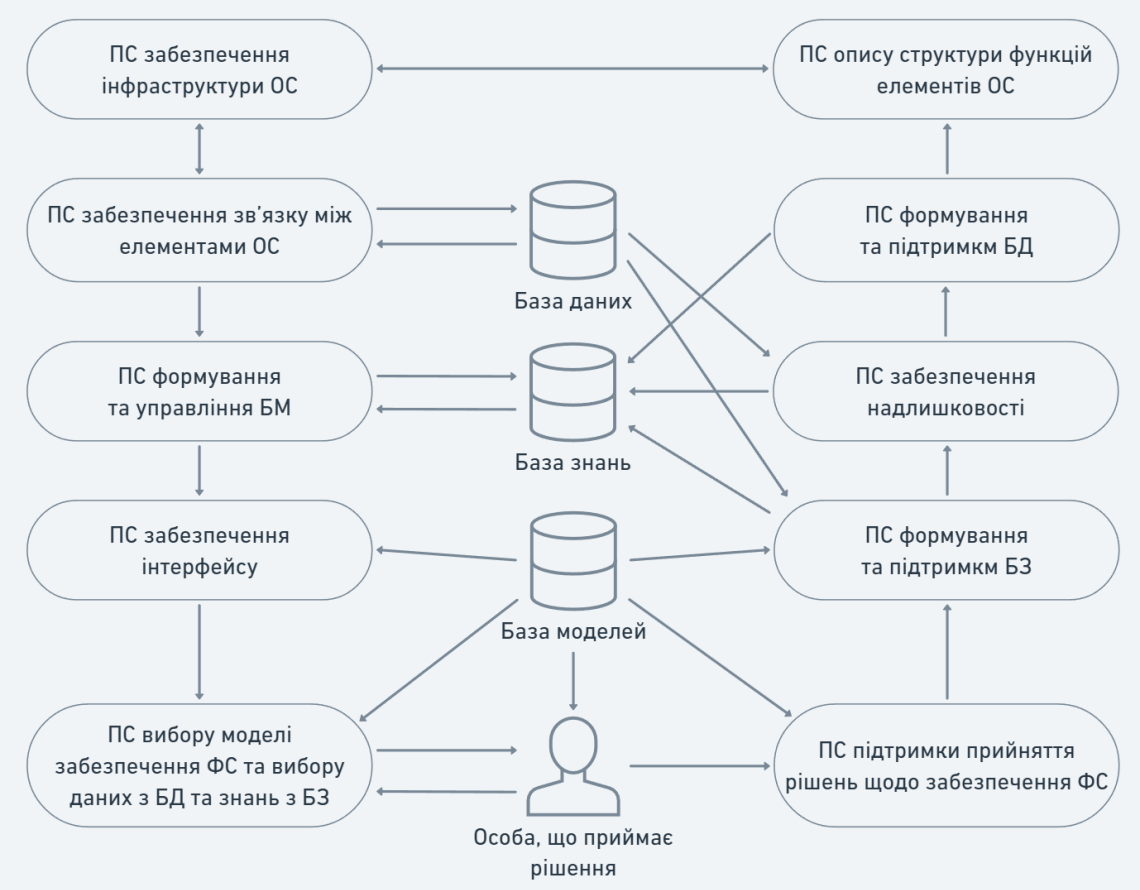


Рисунок 3. *Структурна схема автоматизованої системи забезпечення ФС ОС*

III. ОБГОВОРЕННЯ ТА ВИСНОВКИ

В умовах сучасного глобального світу, для якого є характерними надзвичайно швидкі та докорінні зміни, ОС мають постійно оптимізувати управління діяльністю, модернізувати стратегію та структуру, узгоджувати відповіді на постійні виклики у зовнішньому та внутрішньому середовищі. У цій роботі наведено схеми функціонування ОС для забезпечення її ФС, які забезпечують високий рівень та результативність реакцій ОС на зовнішні та внутрішні чинники.

Для реалізації концепції забезпечення ФС ОС, описаної в роботі [2], авторами було розроблено відповідні ПС, які стали основою автоматизованої системи. Зокрема, ПС для забезпечення зв'язку між елементами організаційної системи описано в роботі [6]. А опис ПС опису структури ролей та виконавців ОС з метою забезпечення її ФС наведено в роботі [7].

ДЖЕРЕЛА

1. Монастирський Г. Л. Теорія організації: підручник. 2-е видання, доповнене й перероблене. Тернопіль: ЗУНУ, 2020. 329 с.

2. Hnatiienko, O. & Kuchanskyi, O. (2023). The concept of analysis the functional sustainability of the organizational system. Management of Development of Complex Systems, 55, 98–103, dx.doi.org\10.32347/2412- 9933.2023.55.98-103.

3. Hnatiienko, O. & Druzhynin, V. (2024). Modern trends in the field of functional stability of complex systems. Management of Development of Complex Systems, 60, 13–17, dx.doi.org\10.32347/2412-9933.2024.60.13-17.

4. Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT): ДСТУ ISO 9000:2015. — [Чинний від 2016-07-01]. Київ: ДП «УкрНДНЦ», 2016. — 41 с.

5. Системи управління якістю. Основні положення та словник термінів (EN ISO 9000:2015, IDT; ISO 9000:2015, IDT) : ДСТУ EN ISO 9000:2022. — [На заміну ДСТУ ISO 9000:2015 ; чинний від 2023-01-01]. — Київ : ДП «УкрНДНЦ», 2022. — 61 с.

6. Hnatiienko O. Web Application for Ensuring the Communication Between Elements of the Organizational System // Information Technology and Implementation (Satellite): Conference Proceedings, December 01, 2022, Kyiv, Ukraine / Taras Shevchenko National University of Kyiv and [etc]; Vitaliy Snytyuk (Editor). – Kyiv: Publisher Individual entrepreneur Picha Y.V., 2022. Pp. 59-61.

7. Oleksii Hnatiienko, Volodymyr Druzhynin. A Web Application for Describing the Structure of Roles and Performers of an Organizational System to Ensure its Functional Sustainability / Proceedings of the 1st international scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2024), March 6, 2024 (Kyiv, Ukraine). Kyiv: FIT TSNUK, 2024. Pp.136-139.



ОЛЕКСІЙ ГНАТІЄНКО
Аспірант кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0001-8546-5074
E-mail: oleksii.hnatiienko@knu.ua

Отримав ступінь спеціаліста з математики Київського національного університету імені Тараса Шевченка (Київ, Україна) у 2008 році та ступінь магістра з менеджменту та маркетингу в Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського» (Київ, Україна) у 2010 р. Зараз навчається в аспірантурі за спеціальністю «Інформаційні системи та технології» Київського національного університету імені Тараса Шевченка (Київ, Україна). Його наукові інтереси включають експертні технології, системи підтримки прийняття рішень, функціональну стійкість, комп'ютеризовані системи моніторингу та управління.



ВЛАДИСЛАВ СИНГАЇВСЬКИЙ
Аспірант кафедри радіотехніки та радіоелектронних систем факультету радіофізикиб електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0002-6858-2695
E-mail: vladssss19@gmail.com

Отримав ступінь бакалавра телекомунікацій та радіотехніки у Київському університеті імені Тараса Шевченка (Київ, Україна) в 2019 році та ступінь магістра телекомунікацій та радіотехніки у Київському національному університеті імені Тараса Шевченка в 2021 році. Нині автор працює над здобуттям ступеня PhD з електрокомунікацій в університеті імені Тараса Шевченка. Науковий інтерес полягає в області розробки та застосування бездротових сенсорних мереж. серед наукових інтересів — системи ком'пютерного зору, розпізнавання та обробки невізуальної інформації.

КРИТЕРІЇ ОЦІНКИ ВІЗУАЛЬНОГО ІНТЕРФЕЙСУ СИСТЕМИ ВІДДАЛЕНОГО КЕРУВАННЯ ДИНАМІЧНИМИ ОБ'ЄКТАМИ

Олексій Губський, Ігор Попов, Олександр Бушма

Анотація. *Підвищення складності систем віддаленого керування потребують визначення критеріїв оцінки візуальних людино-машинних інтерфейсів. Визначено шість базових критеріїв та їх декомпозицію, що дозволяє отримати об'єктивну оцінку ефективності віддаленого керування динамічними об'єктами. Формалізація цієї структури закладає підґрунтя для розробки універсальних інтегральних метрик та формує науково-методичну базу для подальшого моделювання людино-машинних інтерфейсів.*

Ключові слова: віддалене керування, інтерфейс користувача, класифікація, динамічний об'єкт.

I. ВСТУП

Розвиток віддаленого керування динамічними об'єктами (ДО) характеризується стрімким впровадженням інтелектуальних систем підтримки прийняття рішень та мультимодальних засобів візуалізації. Незважаючи на значний технологічний прогрес, більшість рішень у сфері проєктування людино-машинних інтерфейсів (ЛМІ) все ще базуються на інтуїтивних дизайнерських підходах або вузькоспеціалізованих стандартах, які не повною мірою враховують комплексну динаміку когнітивного навантаження оператора. Це зумовлює потребу у переході від фрагментарних оцінок до уніфікованих підходів, що дозволяє створити формалізовану базу порівняльного аналізу.

Підвищення складності систем керування ДО супроводжується зростанням обсягів візуальної інформації, тоді як психофізіологічні можливості оператора залишаються обмеженими. Це загострює суперечність між інформаційною насиченістю інтерфейсу та здатністю підтримувати ситуаційну обізнаність. Водночас у наявних підходах відсутній узгоджений комплекс критеріїв, який дозволяв би системно оцінювати вплив візуального ЛМІ на ефективність віддаленого керування. Тому актуальним є формування структурованої системи критеріїв і їх формалізація, що забезпечує об'єктивність аналізу та знижує суб'єктивність експертних суджень. Метою роботи є визначення ключових критеріїв оцінки візуального людино-машинного інтерфейсу, які впливають на ефективність віддаленого керування динамічними об'єктами.

II. ДАНІ ТА МЕТОДИ

У дослідженні застосовано науковий інструментарій, що базується на аналізі технічних параметрів та експертних оцінок. Вхідними даними слугували технічні характеристики візуальних ЛМІ [1] та статистичні показники операторської діяльності, що відображають вплив візуальної уваги та когнітивного навантаження [2]. Також використано результати досліджень сприйняття візуальної інформації для проєктування дизайну ЛМІ [3].

Методологічну основу роботи склали методи системного аналізу для структуризації підходів до керування життєвим циклом ЛМІ. Формування системи критеріїв оцінювання та узгодження графічних елементів із моделями ситуаційної обізнаності було використано теорію динамічних систем та принципи інженерної психології щодо продуктивності людини.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Визначення ключових критеріїв оцінювання здійснено через структурування узагальнених характеристик, які безпосередньо не піддаються експериментальному

вимірюванню. Їх декомпозиція на підкритерії з подальшим формуванням кількісних показників забезпечує перехід до системи вимірюваних параметрів.

Ключовим чинником пропонованого підходу є ергономіка (E), що характеризує відповідність інтерфейсу психофізіологічним можливостям оператора та визначає організацію елементів керування і читабельність інформації. Із нею безпосередньо пов'язане когнітивне навантаження (C), яке відображає інтенсивність розумових процесів і обсяг даних, що підлягають одночасній обробці. Операційний потенціал системи формалізується через автономність (A) та функціональну повноту (F): перша визначає рівень автоматизації керування, друга — достатність інструментальних засобів для реалізації повного циклу операцій. Характер взаємодії оператора з системою задається типом інтерфейсу (I), тоді як потреба в навчанні (L) відображає складність його опанування та часові витрати на досягнення професійної компетентності. Результуюча концептуальна ієрархічна структура для оцінки візуального інтерфейсу віддаленого керування ДО з шести критеріїв верхнього рівня та їх декомпозиція наведена на рис.1.



Рисунок 1. *Концептуальна ієрархічна структура оцінки візуального інтерфейсу*

Критерій «Ергономіка (E)» характеризує якість та зручність візуальної комунікації. Його формалізовано через п'ять підкритеріїв: візуальна ієрархія (E_{vh}), що забезпечує структуроване представлення інформації; інтуїтивність (E_{int}), яка визначає швидкість засвоєння логіки інтерфейсу; кількість кліків (E_{cl}) та час до виконання дії (E_{tm}); а також наявність та якість зворотного зв'язку (E_{fb}), що забезпечує підтвердження результатів дій. Ці підкритерії охоплюють повний цикл взаємодії та відповідають класичним підходам до ергономіки [2]. Психологічна напруга оператора формується з чинників втоми та перевантаження, з яких було сформовано другий рівень критерію «Когнітивне навантаження (C)». Він включає: суб'єктивне навантаження (C_{ld}) для врахування індивідуального сприйняття складності та напруженості діяльності; кількість одночасних задач (C_{mt}) як показник щільності інформаційних потоків, що потребують паралельної когнітивної обробки; а також рівень автоматизації рутинних операцій (C_{ar}), який розглядається як ключовий механізм зниження перевантаження та підтримання ситуаційної обізнаності. Така декомпозиція охоплює об'єктивні параметри системної складності і суб'єктивні реакції, що відповідає сучасним концепціям теорії когнітивного навантаження. Це забезпечує можливість формування кількісної оцінки когнітивної складності взаємодії у ЛМІ [4].

Аналіз взаємодії в контурі «людина–машина» показав, що автономність системи керування формується як результат розподілу функцій між оператором та технічним

контуром управління. Критерій «Ступінь автономності (A)» визначається через зіставлення технологічних можливостей об'єкта та ролі людини в циклі прийняття рішень. Його декомпозиція здійснена за трьома ключовими підкритеріями: рівень автоматизації (A_{al}), що характеризує здатність системи самостійно виконувати функції контролю та керування; кількість ручних дій (A_{mn}), який відображає інтенсивність прямого втручання оператора в процес керування; та наявність автопілоту (A_{ap}), що визначає можливість переходу об'єкта в режим автоматичного утримання параметрів руху. Запропонований набір підкритеріїв є достатнім для формального опису автономності, оскільки охоплює як програмну незалежність системи, так і фактичне навантаження на оператора в контурі керування [5].

Оцінка операційних можливостей ЛМІ дозволила виокремити критерій «Функціональна повнота (F)» з наступною декомпозицією: інтеграцією функцій (F_{in}), що відображає здатність забезпечувати керування різнорідними підсистемами; зовнішніми засобами (F_{ex}), які характеризують можливість взаємодії з додатковими пристроями, сенсорами та інформаційними базами; та автоматичними діями (F_{au}), сфокусованими на підтримці комплексних сценаріїв управління. Така декомпозиція реалізує системно-інженерний підхід до формалізації і є достатньою для опису функціональної повноти, бо вона охоплює як внутрішні можливості системи керування, так й інтеграцію у ширший інформаційно-технологічний контур виконання місії [6].

Порівняльний аналіз архітектурних рішень показав, що технічна реалізація ЛМІ визначає функціональні межі його застосування та масштабованість. У межах цього було сформовано критерій «Тип інтерфейсу (I)», який відображає архітектурно-технологічні характеристики взаємодії людини з системою. Він узагальнює тип GUI (I_{ty}), що описує парадигму подання інформації; кількість каналів введення (I_{in}), яка характеризує технічні засоби комунікації з оператором та мультимодальність цієї взаємодії; а також мобільність (I_{mb}), що відображає експлуатаційну гнучкість інтерфейсу. Результат їх інтеграції формує другий рівень моделі оцінювання ЛМІ, та є достатнім для формалізації типу інтерфейсу [7].

Аналіз ресурсних витрат на підготовку оператора засвідчив, що складність опанування ЛМІ є критичним фактором його практичної придатності до впровадження. Було сформовано критерій «Потреба в навчанні (L)», який відображає особливості процесу опанування інтерфейсу. Його декомпозиція реалізована як три підкритерії: час навчання (L_{tm}) як кількісну міру тривалості досягнення компетентності; необхідність інструктора (L_{tr}), що відповідає показнику автономності навчального процесу та рівню підтримки; а також складність інтерфейсу (L_{cx}), пов'язаною зі засвоєнням. Критерій потреби в навчанні відображає не лише людський фактор, але й організаційно-економічні аспекти впровадження інтерфейсу [8].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Визначено ключові критерії оцінки візуального ЛМІ, які безпосередньо впливають на ефективність віддаленого керування ДО. Систематизація базових показників — ергономіки, когнітивної відповідності, інформаційної складності, надійності та предикативності — дозволила впорядкувати різнорідні параметри ефективності в єдину ієрархічну структуру.

Формування множини критеріїв верхнього рівня забезпечує концептуальну основу для аналізу стану системи «людина-машина» у складних операційних ситуаціях. Декомпозиція критеріїв деталізує вплив окремих елементів графічного середовища на ефективність роботи оператора в системі віддаленого керування ДО. Подальша формалізація цієї структури закладає підґрунтя для розробки універсальних інтегральних метрик, що адаптують інтерфейс до когнітивних можливостей людини. Запропонований ієрархічний критеріальний підхід формує науково-методичну базу для моделювання та цілеспрямованої оптимізації візуальних середовищ станцій керування ДО.

ДЖЕРЕЛА

1. Hubskyi, O. M. (2024). Analysis of user interfaces for ground control stations of unmanned aerial vehicles. Cybernetics and Computer Engineering, 2024(3), 5–21. https://doi.org/10.15407/kvt217.03.005
2. Liu, H., et al. (2026). Operational performance, cognitive load, visual attention, and usability of fixed-, manual-, and autonomous-camera control in single- and multiple-camera telemanipulation systems. Applied Ergonomics, 130, Article 104647. https://doi.org/10.1016/j.apergo.2025.104647
3. Рябовол, Д. А. (2021). Аналіз досліджень щодо сприйняття візуальної інформації для проєктування адитивного кібер-дизайну людино-машинного інтерфейсу для Smart Manufacturing. У Радіоелектроніка та молодь у XXI столітті: матеріали 25-го Міжнар. молодіж. форуму (Т. 2, с. 21–22). ХНУРЕ.
4. Picardi, A., & Caruso, G. (2024). User-centered evaluation framework to support the interaction design for augmented reality applications. Multimodal Technologies and Interaction, 8(5), 41. https://doi.org/10.3390/mti8050041
5. Telli, K., Kraa, O., Himeur, Y., Ouamane, A., Boumehraz, M., Atalla, S., & Mansoor, W. (2023). A comprehensive review of recent research trends on unmanned aerial vehicles (UAVs). Systems, 11(8), 400. https://doi.org/10.3390/systems11080400.
6. Endsley, M. R., & Jones, D. G. (2025). Designing for situation awareness: An approach to user-centered design (3rd ed.). CRC Press.
7. Brdnik, S., Heričko, T., & Šumak, B. (2022). Intelligent user interfaces and their evaluation: A systematic mapping study. Sensors, 22(15), 5830. https://doi.org/10.3390/s22155830
8. Смалько, О. (2025). Еволюція цифрових інтерфейсів. Вісник Кам'янець-Подільського національного ун-ту ім. Івана Огієнка. Фіз.-мат. науки, 18, 115–120.



ОЛЕКСІЙ ГУБСЬКИЙ
м.н.с. відділу «Інтелектуального керування», Інститут інформаційних технологій і систем НАН України, Київ, Україна
ORCID: 0009-0004-3106-2770
E-mail: gubish@gmail.com
Отримав ступінь бакалавра у Київському національному університеті будівництва і архітектури (Київ, Україна) в 2005 році, а в 2006 ступінь магістра. Нині працює над здобуттям ступеня PhD з комп'ютерних наук в Інституті ІТС НАН України, (Київ, Україна). Серед наукових інтересів — інтелектуальне керування, дизайн інтерфейсів.



ІГОР ПОПОВ
н.с. відділу «Інтелектуального керування», Інститут інформаційних технологій і систем НАН України, Київ, Україна
ORCID: 0009-0009-7961-9431
E-mail: popigor7@gmail.com
Отримав ступінь бакалавра у Київському національному університеті будівництва і архітектури (Київ, Україна) в 2005 році та ступінь магістра з Управління проєктами у 2007. Нині автор працює над здобуттям ступеня PhD з комп'ютерних наук в Інституті ІТС НАН України, (Київ, Україна). інтелектуальне керування динамічними об`єктами, підготовка операторів, імітаційне моделювання.



ОЛЕКСАНДР БУШМА
професор кафедри комп'ютерних наук, Київський столичний університет ім. Бориса Грінченка, Київ, Україна
ORCID ID 0000-0003-1604-6129
E-mail: o.bushma@kubg.edu.ua
Закінчив Київський політехнічний інститут у 1976 році. доктор технічних наук, професор. Серед наукових інтересів — інформаційно-комунікаційні технології, людино-машинні системи, інформаційно-вимірювальні системи, системи моніторингу, вбудовані системи, сенсорика.

ФОРМАЛІЗАЦІЯ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАДАЧІ ЕКСПЕРТИЗИ НА ОСНОВІ КОНЦЕПТІВ OPENALEX

Ірина Доманецька, Ярослав Хроленко

***Анотація**. У роботі розглянуто проблему формалізації предметної області задачі експертизи у науково-технічних процедурах оцінювання. Запропоновано семантико-статистичну модель, яка описує об'єкт експертизи у вигляді багаторівневої структури наукових концептів. Модель формується шляхом ітеративного розширення початкової множини термінів на основі статистики їх співвживання у наукових публікаціях. Джерелом даних для формування концептів виступає відкрита наукова база OpenAlex, що містить структурований граф наукових публікацій і тематичних концептів. Використання OpenAlex дозволяє локалізувати релевантну область знань у глобальному науковому просторі та формалізувати тематичну структуру задачі експертизи.*

Ключові слова: семантична модель, предметна область експертизи, наукові концепти, тематична структура, статистика співвживання..

I. ВСТУП

Експертні процедури широко застосовуються у науково-технічній сфері для оцінювання результатів досліджень, конкурсних проєктів, інноваційних розробок та наукових публікацій. Центральним елементом будь-якої експертної процедури є формалізація предмету експертизи, тобто визначення тематичних меж та змістових характеристик об'єкта оцінювання. У традиційній практиці опис предметної області здійснюється за допомогою ключових слів або класифікаційних рубрик. Проте такі підходи мають обмежену здатність відображати реальну структуру наукового знання, яка характеризується складними міждисциплінарними зв'язками та різноманітністю термінологічних формулювань[1].

Розвиток цифрових наукових інфраструктур і відкритих бібліографічних баз даних створює нові можливості для аналізу структури наукових знань. У таких системах наукові публікації асоціюються з концептами, що формують мережу тематичних зв'язків. Аналіз статистики співвживання концептів у великому масиві публікацій дозволяє виявляти приховані тематичні структури та визначати ступінь семантичної близькості між науковими поняттями. Це відкриває можливість побудови формалізованих моделей предметних областей, які відображають реальну структуру наукового дискурсу.

II. ДАНІ ТА МЕТОДИ

Джерелом даних для побудови семантико-статистичної моделі виступає відкрита база наукових знань OpenAlex, яка представляє глобальний граф публікацій, авторів, установ та тематичних концептів [2]. У цій системі кожна публікація асоціюється з множиною концептів, організованих у багаторівневу ієрархію Fields of Study, що формується на основі аналізу текстів і статистики співвживання термінів у науковому дискурсі.

У запропонованому підході предмет експертизи розглядається як підмножина глобального простору наукових концептів [3]. Основою побудови моделі є початкова множина концептів, що безпосередньо описують об'єкт експертизи. Нехай

$$C_0 = \{c_1, c_2, \dots, c_m\} \quad (1)$$

— множина базових концептів, що характеризують тематику задачі експертизи.

На основі цієї множини формується вибірка наукових публікацій

$$P_0 = \{p_i \mid p_i \cap C_0 \neq \emptyset\}, \quad (2)$$

де p_i— множина концептів, що асоціюються з публікацією i.

Для кожного концепту cвизначається множина публікацій, у яких він зустрічається,

$$D(c) = \{p_i \in P_0 \mid c \in p_i\}, \quad (3)$$

та обчислюється частота його появи

$$f(c) = \mid D(c) \mid. \quad (4)$$

Множина концептів першого рівня формується як

$$C_1 = \{c \notin C_0 \mid f(c) \geq L\}, \quad (5)$$

де L— порогове значення частоти співвживання.

Далі для множини концептів C_kформується нова вибірка публікацій

$$P_k = \{p_i \mid p_i \cap C_k \neq \emptyset\}, \quad (6)$$

після чого визначається множина концептів наступного рівня

$$C_{k+1} = \{c \notin (C_0 \cup \ldots \cup C_k) \mid f_k(c) \geq L\}. \quad (7)$$

Ітеративне розширення триває до досягнення максимальної глибини моделі Kабо до вичерпання нових концептів. У результаті формується багаторівнева структура

$$M = \{C_0, C_1, C_2, \ldots, C_K\}, \quad (7)$$

яка відображає тематичну організацію предметної області експертизи.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Отримана структура концептів формує семантичний опис задачі експертизи у вигляді багаторівневої моделі. Початковий рівень моделі відповідає концептуальному ядру предметної області. Наступні рівні формуються на основі статистичних зв'язків між концептами, що виникають у наукових публікаціях. У результаті модель поступово розширюється, охоплюючи суміжні тематичні напрями.

Особливістю запропонованого підходу є те, що зв'язки між концептами визначаються не на основі експертної інтерпретації, а шляхом аналізу статистики їх співвживання у науковому дискурсі. Це дозволяє отримати об'єктивну структуру предметної області, що відображає реальні взаємозв'язки між науковими поняттями.

На віддалених рівнях моделі можуть з'являтися концепти, які належать до інших галузей знань, але використовують спільний теоретичний апарат або методологію. Таке розширення є природним наслідком міждисциплінарного характеру сучасних наукових досліджень. У результаті модель відображає не лише ядро предметної області, але й ширший контекст наукових знань, пов'язаних із задачою експертизи.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Запропонована семантико-статистична модель дозволяє формалізувати предмет експертизи у вигляді багаторівневої структури наукових концептів. Побудова моделі ґрунтується на аналізі статистики співвживання термінів у великому масиві наукових публікацій, що забезпечує об'єктивність формування тематичних зв'язків між поняттями.

Багаторівнева організація моделі дозволяє впорядковувати концепти за ступенем їх семантичної близькості до початкового ядра предметної області. Це створює можливість локалізації релевантної області знань у глобальному науковому просторі та забезпечує формалізований опис структури задачі експертизи.

Отримана модель може використовуватися як основа для подальшого аналізу тематичних структур наукових досліджень, а також для розроблення інформаційних систем підтримки експертних процедур у науково-технічній сфері.

Запропонована модель може бути корисна для вирішення задачі оцінювання компетентності експертів. Ідея полягає у зіставленні концептів наукового профілю експертів з концептами моделі предметної області. Використання частотних характеристик і вагових коефіцієнтів дозволяє кількісно оцінити ступінь тематичної відповідності експерта запиту експертизи.

Перевагами запропонованого підходу є об'єктивність, міждисциплінарна чутливість та масштабованість. Модель може бути інтегрована у цифрові системи добору експертів і використовуватися для автоматизованого формування експертних груп у конкурсних, грантових і рецензійних процедурах.

ДЖЕРЕЛА

1. Modern world trends in the development of science, education, and technology: A collection of abstracts of the International Scientific-Practical Conference (Bila Tserkva, March 20, 2024): In 2 parts (Pt. 2). (2024) Bila Tserkva: CFEND. Available at: https://www.economics.in.ua/2024/03/20-2.html (Accessed: 7 March 2026).

2. Priem, J., Piwowar, H., Orr, R. and Carbery, S. (2022) OpenAlex: A fully-open index of scholarly works, authors, venues, institutions, and concepts. arXiv preprint arXiv:2205.01833. Available at: https://arxiv.org/abs/2205.01833 (Accessed: 7 March 2026).

3. Tsyganok, V., Khrolenko, Y., Domanetska, I., Tsyhanok, O. and Trubitsyna, O. (2024) 'An automated approach to forming a jury of student research competitions based on scientometric and altmetric indicators', in Proceedings of the XXIV International Scientific and Practical Conference "Information Technologies and Security" (ITS 2024), Kyiv, Ukraine, pp. 176–189. Available at: https://ceur-ws.org/Vol-4068/paper14.pdf (Accessed: 7 March 2026).



ІРИНА ДОМАНЕЦЬКА
Доцент, кафедра інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна, Київ, Україна
ORCID: 0000-0002-8629-9933
E-mail: domanetska@knu.ua

Отримала ступінь кандидата технічних наук у галузі інформаційних технологій у 1992 році. Є автором понад 120 наукових праць. До наукових інтересів належать системи адаптивного навчання, нейронні мережі та їх прикладне застосування.



ЯРОСЛАВ ХРОЛЕНКО
Аспірант з комп'ютерних наук в Інституті проблем реєстрації інформації НАН України.
ORCID: 0009-0004-0641-827X
E-mail: yaroslav.khrolenko@knu.ua

отримав ступінь бакалавра комп'ютерних наук в Національному технічному університеті Украíни «Київський політехнічний інститут імені Ігоря Сікорського» (Київ, Україна) в 2020 році та ступінь магістра комп'ютерних наук у у Київському національному університеті імені Тараса Шевченка (Київ, Україна) в 2022. Нині автор працює над здобуттям ступеня PhD з комп'ютерних наук в Інституті проблем реєстрації інформації НАН України (Київ, Україна). Серед наукових інтересів — методи експертного оцінювання, великі мовні моделі, інтелектуальні підходи до прогнозування та аналізу часових рядів.

СИСТЕМА МОНІТОРИНГУ ЕМОЦІЙНОГО СТАНУ ТА САМОСВІДОМОСТІ ДИТИНИ ЗА ДОПОМОГОЮ ПСИХОЛОГІЧНИХ ІНСТРУМЕНТІВ

Катерина Жукова, Мирослава Гладка

Анотація. *У представленому дослідженні розглядається актуальна проблема своєчасного виявлення та м'якої корекції емоційних розладів у дітей. Запропоновано інноваційну систему моніторингу емоційного стану та рівня самосвідомості дитини, що базується на інтеграції інформаційних технологій та валідизованих психологічних інструментів. Робота розкриває архітектуру такої системи, методи збору й аналізу психоемоційних показників, а також демонструє її потенціал для забезпечення психологічного благополуччя дитини завдяки своєчасному сповіщенню батьків про можливі психологічні ризики.*

Ключові слова: система моніторингу; емоційний стан.

I. ВСТУП

У сучасному динамічному світі проблема збереження психологічного здоров’я та емоційного благополуччя дітей набуває особливої гостроти. Стрімкий розвиток суспільства, зміна соціальних умов та високий рівень повсякденного стресу безпосередньо впливають на формування емоційного інтелекту та самосвідомості дитини. Вчасне виявлення тривожних станів, депресивних тенденцій чи зниження рівня самооцінки є критично важливим для запобігання розвитку серйозних психологічних розладів у майбутньому. Традиційні методи психологічної діагностики зазвичай потребують безпосередньої участі фахівця, займають значний час і проводяться лише періодично, що ускладнює безперервне відстеження динаміки стану дитини. Батьки та педагоги не завжди здатні самостійно розпізнати приховані ознаки емоційного дискомфорту. Саме тому виникає об’єктивна потреба у створенні автоматизованих систем моніторингу, які б дозволяли інтегрувати перевірені психологічні інструменти у повсякденне безпечне середовище дитини. Метою даної роботи є розробка та концептуальне обґрунтування системи моніторингу емоційного стану та самосвідомості дитини. Запропонована система базується на використанні валідизованих психологічних методик, адаптованих для зручного інтерактивного формату, що забезпечує регулярний ненав'язливий збір даних, їх оперативний аналіз та своєчасне інформування батьків і психологів про можливі ризики [1].

II. ДАНІ ТА МЕТОДИ

Для досягнення поставленої мети було розроблено архітектуру системи моніторингу, в якій збір даних здійснюється через інтерактивний веб-додаток, адаптований для дітей. Традиційні психологічні інструменти були трансформовані у формат цифрових тестів-ігор, що дозволяє проводити діагностику в природному та комфортному для дитини середовищі. Основними методами збору даних у системі є:

1. Колірний тест Люшера — використовується для оцінки поточного емоційного стану, рівня стресу та психофізіологічної втоми. У цифровому форматі дитина інтуїтивно обирає кольорові картки на екрані пристрою [2].

2. Методика «Драбинка» (В. Щур) — застосовується для дослідження рівня самооцінки та самосвідомості. Інтерфейс пропонує дитині розмістити свого віртуального персонажа на

одній зі сходинок, що символізують різні полюси самосприйняття (наприклад, щастя – смуток).

3. Проєктивний тест тривожності (Теммл-Доркі-Амен) — адаптований у вигляді серії зображень типових ситуацій із прихованим обличчям головного героя. Дитина обирає емоцію (веселе чи сумне обличчя), що дозволяє системі кількісно оцінити рівень її соціальної та особистісної тривожності [3].

Отримані результати у вигляді числових показників та виборів передаються до бази даних системи. Алгоритми обробки даних аналізують результати кожного тесту, порівнюють їх із попередніми сесіями дитини для відстеження динаміки та формують загальний профіль психологічного благополуччя.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У ході дослідження було спроєктовано прототип веб-системи моніторингу емоційного стану дітей. Архітектура розробленого рішення передбачає логічний розподіл на два основні модулі: інтерактивний ігровий інтерфейс для дитини та інформаційну панель (дашборд) для батьків. Як показано на Рисунку 1, взаємодія користувачів із системою відбувається через клієнтську частину веб-сайту, звідки результати проходження цифрових тестів-ігор у зашифрованому вигляді надсилаються на сервер для подальшої обробки.

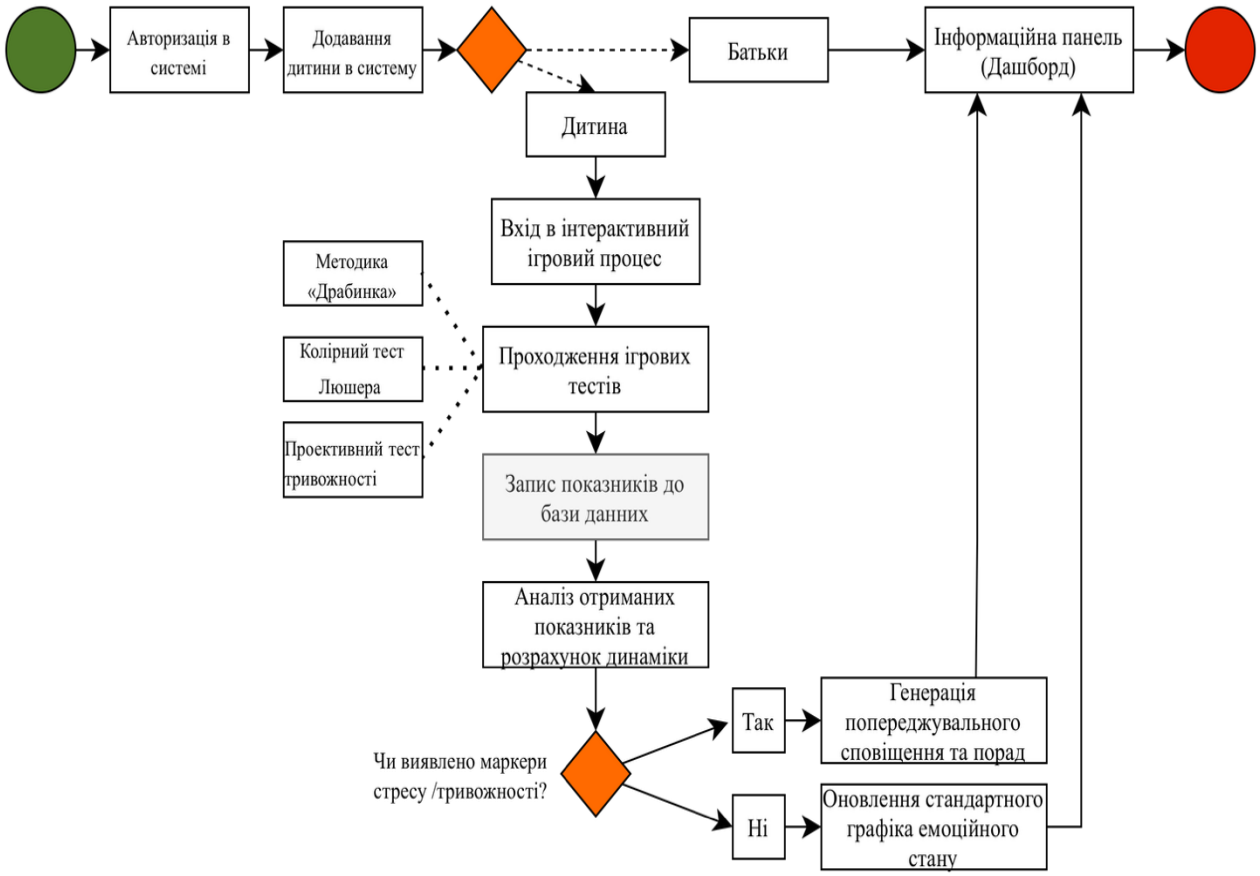


Рисунок 1. *Структурна схема веб-системи моніторингу емоційного стану дитини*

Алгоритм системи автоматично підраховує бали за кожною з адаптованих методик (колірний вибір, рівень самооцінки, показники тривожності) та візуалізує динаміку змін у вигляді зрозумілих графіків у батьківському кабінеті. Важливою функцією веб-системи є

генерація автоматичних рекомендацій: якщо алгоритм фіксує маркери емоційного напруження, підвищеної тривожності або стабільного погіршення настрою, система формує попереджувальне сповіщення з базовими порадами. Отримуючи ці об'єктивні, зібрані у динаміці результати моніторингу, батьки можуть своєчасно звернутися за фаховою допомогою до дитячого психолога, що підтверджує високу практичну цінність запропонованого програмного рішення.

IV. ВИСНОВКИ

У результаті проведеного дослідження обґрунтовано доцільність та розроблено концепцію веб-системи моніторингу емоційного стану та самосвідомості дитини. Переведення класичних психологічних інструментів (колірний тест, методики оцінки тривожності та самосвідомості) у цифровий ігровий формат дозволило мінімізувати стрес від процесу тестування та значно підвищити залученість дітей. Розроблена система не покликана замінити професійну психологічну допомогу, проте вона виступає ефективним інструментом превентивної діагностики. Вона надає батькам зручний механізм для регулярного відстеження емоційного фону дитини у динаміці. Завдяки автоматизованому аналізу та своєчасній генерації сповіщень (із можливістю вивантаження результатів для фахівця), система сприяє ранньому виявленню прихованих психологічних проблем.

ДЖЕРЕЛА

1. Liu Y., Ren Y., Liu C., Chen X., Li D., Peng J., Tan L., Ma Q. Global burden of mental disorders in children and adolescents before and during the COVID-19 pandemic: evidence from the Global Burden of Disease Study 2021 / Psychol Med. – 2025.: https://pmc.ncbi.nlm.nih.gov/articles/PMC12080646/
2. Колірний тест Люшера / сайт ФСП НТУУ «КПІ ім. І. Сікорського». https://fsp.kpi.ua/ua/kolirnij-test-lyushera/
3. «Тест тривожності Р. Темлінга та М. Доркі» / https://www.annadomina.com/test-trivozhnist-r-teml-m-dorki-v-amen/



КАТЕРИНА ЖУКОВА
студентка 1 курсу магістратури комп'ютерні науки у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: k.zhukova-zk51mp@edu.kpi.ua
Науковий інтерес полягає в області розробки та застосування інформаційних систем. Серед наукових інтересів — системи моніторингу, людино-машинна взаємодія та застосування ІТ-технологій для підтримки психологічного благополуччя.



МИРОСЛАВА ГЛАДКА
к.т.н., доцент кафедри інформаційних систем та технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0001-5233-2021
E-mail: myroslava.gladka@knu.ua
Коло наукових інтересів: управління проєктами, моделювання та інжиніринг бізнес-процесів.

ПРО ОДНУ ГІБРИДНУ АВТОМАТНО-АГЕНТНУ МОДЕЛЬ ПРОЦЕСІВ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ

Євген Івохін, Лариса Аджубей, Дмитро Афонін

Анотація. *У статті розглянуто проблему моделювання процесів поширення інформації в соціальних мережах з урахуванням як індивідуальної поведінки користувачів, так і структурних особливостей мережі. Запропоновано гібридний підхід, що поєднує автоматні та агентні моделі, завдяки чому досягається більш реалістичне відтворення інформаційної динаміки. Поведінка користувачів формалізується за допомогою скінченних автоматів, а вплив у мережі описується через моделі змішаного характеру, які враховують міжособистісну комунікацію та зовнішній інформаційний тиск у вигляді засобів масової інформації. На основі запропонованої моделі проведено порівняльне моделювання з класичною грою «республіканці–демократи».*

Ключові слова: соціальні мережі, поширення інформації, агентне моделювання, скінченні автомати, гібридна модель, інформаційний вплив.

I. ВСТУП

Ефективне моделювання процесів поширення інформації в соціальних мережах вимагає врахування як індивідуальної поведінки користувачів, так і структурних особливостей мережевого середовища. Однак більшість існуючих моделей [1-2] або надто спрощують поведінкові аспекти агентів, або не відображають складної динаміки взаємодії в масштабі мережі. У цьому контексті виникає потреба в розробці нових гібридних підходів, які б об'єднували переваги різних методів моделювання. Одним із перспективних напрямів досліджень є використання агентних моделей, що базуються на підходах математичної теорії автоматів. У цьому контексті агентами вважають користувачів соціальних мереж, які активно поширюють інформацію. Для опису їх поведінки в межах функціональної структури соціальних мереж доцільно застосовувати моделі скінченних автоматів та їх розширених модифікацій. Поєднання автоматних моделей з іншими моделями відкриває нові можливості для прогнозування інформаційних процесів і розробки стратегій боротьби зі шкідливим контентом.

II. ДАНІ ТА МЕТОДИ

В рамках даного дослідження основну увагу зосереджено на використанні гібридного підходу до моделювання поширення інформації в соціальних мережах, що поєднує автоматні моделі та концепцію змішаного впливу. Поведінку користувачів описано за допомогою скінченних автоматів, які дозволяють формалізувати стани агентів та переходи між ними під впливом різних інформаційних сигналів. Такий підхід забезпечує структуроване й гнучке представлення індивідуальної реакції на інформаційні стимули. У межах гібридної моделі автоматне ядро інтегрується в агентну архітектуру, що дозволяє враховувати як локальні поведінкові закономірності, так і глобальні властивості соціальної мережі. Основою для побудови сценаріїв слугують моделі змішаного впливу, що поєднують елементи масового, цільового та міжособистісного інформаційного впливу, що робить модель більш реалістичною в умовах сучасного цифрового середовища.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Запропоновано способи формалізації процесу розповсюдження інформації у соціальних мережах на основі імовірнісного автомату $M=<Q,V,Ф>$, функціонування якого розглядається

на графі V. Для перевірки розглянутої моделі проведено порівняння її з класичною грою «республіканці–демократи». Для порівняння результатів використано алгоритм, за яким кожен користувач, що не визначився, наслідує ту ж саму ідею, що і більшість його сусідів. Для коректності порівняння моделювання відбувається у графі поділеному на групи, алгоритм створення якого описано у [3].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У даній роботі запропоновано та реалізовано гібридну автоматно-агентну модель для дослідження процесів поширення інформації в соціальних мережах. На відміну від класичних підходів, які часто надто спрощують динаміку взаємодії між користувачами, розроблена модель поєднує переваги скінченних автоматів і методів агентного моделювання. Це дозволило формалізувати індивідуальні поведінкові реакції користувачів, врахувати групову структуру соціальних мереж, а також описати вплив зовнішніх джерел інформації. Модель враховує природну кластеризацію соціальних мереж і дозволяє моделювати передачу інформації між окремими групами, що надає можливості застосувати її в якості універсального інструменту для аналізу інформаційних процесів у соціальних мережах, а також для оптимізації інформаційно-психологічних кампаній у бізнесі, політиці та суспільному житті.

ДЖЕРЕЛА

1. Ivohin E.V., Adhubey L.T., Gavrilenko O.V., Naumenko Yu.O. (2020) Research of dynamics of information distribution processes based on diffusion hybrid models. Радіоелектроніка, інформатика, управління, 2, 129-136.
2. Centola D. (2010) The spread of behavior in an online social network experiment. Science, 329, 1194-1197.
3. Івохін Є.В., Афонін Д.Е., Аджубей Л.Т. (2025) Про один гібридний підхід до агентного моделювання процесів інформаційного розповсюдження. Вісник Кам'ян.-Поділ. нац. університету імені Івана Огієнка, "Математичне та комп'ютерне моделювання. Серія: Технічні науки", 28, 49-62.



ЄВГЕН ІВОХІН
Д.ф.-м.н., професор кафедри інтелектуальних програмних систем факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-5826-7408
E-mail: ivohin@knu.ua
Наукові інтереси — моделі інформаційного розповсюдження, нечіткі моделі.



ЛАРИСА АДЖУБЕЙ
К.ф.-м.н., доцент кафедри обчислювальної математики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-8487-0884
E-mail: adzhubey@knu.ua
Наукові інтереси — моделі інформаційного розповсюдження, обчислювальні методи.



ДМИТРО АФОНІН
PhD-студент Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0009-2296-7304
E-mail: afonin.di@gmail.com
Наукові інтереси — моделі інформаційного розповсюдження, агентні моделі.

ПРО ОДИН ПРИКЛАД ОПТИМІЗАЦІЇ МАРШРУТІВ ДОСТАВКИ ВАНТАЖІВ НА ОСНОВІ МЕТОДУ ІМІТАЦІЇ ВІДПАЛУ

Євген Івохін, Дмитро Івохін

Анотація. *У статті розглянуто моделювання процесів доставки на основі розв'язання задачі комівояжера з урахуванням кількості наявних транспортних засобів, кількості заявок для розподілу, габаритів вантажу та вікон бажаного часу доставки. Для оптимального перерозподілу заявок запропоновано використання методу відпалу. Розроблено підхід, що базується на розподілі заявок за маршрутами: заявка розміщується у маршруті, який відповідає обмеженням за вагою та кількості заявок у маршруті. Для обчислення ймовірності прийняття нового стану системи у методі імітації відпалу використовується спеціальний показник. Проведено чисельні розрахунки на основі запропонованого підходу, визначено наявні проблеми використання, що пов'язані з нерівномірністю початого розподілу заявок.*

Ключові слова: моделювання, оптимізація, задача комівояжера, метод відпалу, інформаційні процеси.

I. ВСТУП

На сьогоднішній день вирішення проблеми пошуку найкоротшого шляху між довільними пунктами транспортної мережі залишається дуже актуальною: обсяги та потреби транспортно-логістичних послуг постійно зростають. Основне завдання - пошук найбільш ефективного з точки зору деякого критерію маршруту для обслуговування споживачів.

II. ДАНІ ТА МЕТОДИ

Розглянемо застосування методу імітації відпалу [1] в задачі пошуку маршрутів доставки за допомогою розв'язання задачі комівояжера з урахуванням кількості наявних транспортних засобів, кількості заявок для розподілу, габаритів вантажу та вікон бажаного часу доставки. Введемо деякі позначення:

$V=(v_1,...,v_N)$ – список транспортних засобів для формування маршрутів, де N – кількість транспортних засобів для розв'язання задачі, $R=(r_1,...,r_N)$ – список сформованих маршрутів, $r_j \in v_j$, $j=\overline{1,N}$, $D=(d_1,...,d_M)$ – список заявок на доставку, де M – кількість заявок на доставку, які потрібно розподілити за маршрутами R. Кожна заявка d_k, $k=\overline{1,M}$, має параметри, такі, як вага, очікуваний час доставки, вікно доставки (заданий проміжок часу, вказаний клієнтом), t_{fin} – значення «температури», при якому завершується робота методу відпалу, $C_{\max}$ – максимальна кількість доставок (заявок) на одному маршруті, $W=(w_{kj})$, $k,j=\overline{1,M}$ – матриця $M\times M$, яка містить дані про часову відстань розміщення точок заявок між усіма парами пунктів, заданих списком заявок, $KPI_{du}(s)$ – критерій оптимізації, який відповідає за величину запізнення при доставці заявок за всіма сформованими маршрутами у стані s, $KPI_{dist}(s)$ – критерій оптимізації, який відповідає за загальну величину часу всіх маршрутів у стані s, s^0 – найкращій розв'язок задачі оптимізації, $E(s)=KPI_{du}(s)+KPI_{dist}(s)$ – цільова функція. Для обчислення ймовірності прийняття нового стану s' у методі імітації відпалу запропоновано формулу:

$$h(\Delta E,t_i)= KPI_{dist}(s)*t_i \,/\, KPI_{dist}(s')*t_1 . \quad (1)$$

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

Запропоновано алгоритм, на початку роботи якого здійснюється формування початкового стану s_0. Транспортні засоби отримують заявки послідовно, відбувається заповнення маршруту заявками шляхом знаходження найближчої за часом заявки у матриці W до крайньої доданої точки заявки у маршрут. При формуванні початкового стану s_0 існує ймовірність, що частина заявок не прив'язується до транспортних засобів і залишається незавантаженою (список D_{unload}). Для кожного маршруту розраховується час, за яким має оброблена перша заявка, оцінюється приблизний час доставки для усіх заявок у маршруті, а також можна обчислити критерії $KPI_{dist}(s_0)$ та $KPI_{du}(s_0)$ і записати початковий стан s_0 як поточний розв'язок s та найкращий розв'язок s^0. Новий стан розв'язку s' генерується на основі методу відпалу.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У статті розглянуто задачу моделювання процесів доставки на основі пошуку розв'язку задачі комівояжера з урахуванням кількості наявних транспортних засобів, кількості заявок для розподілу, габаритів вантажу та вікон бажаного часу доставки. Для оптимального перерозподілу заявок запропоновано використання методу відпалу. Розроблено підхід, що базується на розподілі заявок за маршрутами: заявка розміщується у маршруті, який відповідає умовам – задовольняє обмеженням за вагою і кількості заявок у маршруті. Для обчислення ймовірності прийняття нового стану системи у методі імітації відпалу використовується спеціальний показник. Проведено чисельні розрахунки на основі запропонованого підходу. Зроблено висновок, що наповнення маршруту суттєво залежіть від початкового стану, який складається з повністю заповнених сформованих маршрутів і невеликої частини маршрутів з невеликою кількістю заявок.

ДЖЕРЕЛА

1. Івохін Є.В., Гавриленко В.В., Івохіна К.Е., Рудоман Н.В. (2022) Про підхід до розв'язання нечіткої задачі комівояжера на основі методу імітації відпалу. Автомобільні дороги та дорож. будівництво, 112, 46-51.



ЄВГЕН ІВОХІН
д.ф.-м.н., професор кафедри інтелектуальних програмних систем факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-5826-7408
E-mail: ivohin@knu.ua
Наукові інтереси — моделі оптимізації транспортних та мережевих потоків, методи моделювання інформаційного розповсюдження, нечіткі моделі.



ДМИТРО ІВОХІН
інженер кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка, Київ, Україна
E-mail: divohin@ukr.net
Наукові інтереси — комп'ютерне моделювання транспортних та мережевих потоків

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА EDTECH-ПЛАТФОРМ ТА UI-АНАЛІЗАТОРІВ

Карина Конвісар, Анна Пилипенко

Анотація. *У дослідженні узагальнено сучасні підходи до порівняльної оцінки EdTech-платформ (LMS і MOOC) та інструментів автоматизованого UI-аналізу. На основі наукових джерел 2022-2025 рр. структуровано критерії відбору платформ та визначено класи UI-аналізаторів. Показано, що автоматизовані аналізатори суттєво прискорюють аудит, але потребують поєднання з людиноцентричними методами для зменшення ризиків хибних спрацювань і «сліпих зон» оцінювання.*

Ключові слова: EdTech; LMS; MOOC; UX/UI; автоматизована оцінка доступності.

I. ВСТУП

Різноманіття EdTech-платформ – від інституційних LMS до MOOC-сервісів – ускладнює вибір цифрового навчального середовища. Формалізовані рамки оцінювання дозволяють здійснювати системний відбір: зокрема, підхід SQTL демонструє можливість порівняння LMS за групами критеріїв (інтероперабельність/стандарти, доступність, комунікація, навчальні та продуктивні інструменти, безпека/сертифікації) [1]. Водночас порівняння Moodle і Google Classroom показує, що функціональна насиченість не гарантує низького порогу входу та зручної навігації, тому відбір доцільно доповнювати UX-параметрами реального використання [2]. Для MOOC-платформ у кількісних зіставленнях переважають показники масштабу й умов навчання (каталог, рівні, вартість/сертифікація, навчальні опції) [3]. Окремо зростає значення цифрової доступності та якості інтерфейсу; автоматизований UI-аналіз прискорює аудит, але потребує прозорого пояснення меж перевірок і коректної інтерпретації результатів [5], [6].

Мета дослідження: систематизувати критерії порівняння LMS і MOOC, подати типологію інструментів автоматизованого UI-аналізу та обґрунтувати їх спільне використання для оцінювання і вдосконалення цифрового навчального середовища.

II. ДАНІ ТА МЕТОДИ

Корпус дослідження становлять наукові публікації 2022–2025 рр. українською й англійською мовами, які містять критерії, метрики або емпіричні результати щодо порівняння EdTech-платформ та/або автоматизованого UI-аналізу.

Застосовано порівняльно-аналітичний підхід у двох площинах:

- Для EdTech-платформ критерії згруповано за типом платформи. Для LMS використано рамку SQTL як базову систему критеріїв [1] і доповнено UX-показниками, описаними в дослідженнях порівняння навчальних платформ (легкість опанування, навігація, робота з помилками, задоволеність) [2]. Для MOOC застосовано набір показників, типовий для кількісних зіставлень (масштаб каталогу, рівні/складність, сертифікація/вартість, навчальні опції) [3].
- Для UI-аналізаторів побудовано порівняльну матрицю класів інструментів за вхідними даними, типом результату, перевагами та ризиками. Ознаки матриці обґрунтовано емпіричними порівняннями автоматичних тестерів доступності та роботами про прозорість/інтерпретованість результатів, а також дослідженнями AI-підходів до критики й оцінювання UI [5]-[10].

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На рівні EdTech-платформ узагальнення джерел показує, що для LMS доцільною є рамка з шести груп критеріїв, узгоджених із SQTL: інтероперабельність/стандарти; доступність; комунікаційні інструменти; інструменти керування навчанням; навчальні інструменти; безпека/сертифікації [1]. Для прикладного відбору її доцільно доповнювати UX-параметрами реального використання (швидкість опанування, зрозумілість навігації, типові помилки під час виконання навчальних дій), які впливають на сприйняття ефективності роботи з платформою [2].

Для MOOC-платформ характерна інша логіка порівняння: вибір здебільшого визначається асортиментом курсів, рівнями складності, вартістю та умовами сертифікації, а також навчальними опціями (наприклад, тестами); при цьому покриття тематики може суттєво різнитися між майданчиками [3].

Критерії інтерфейсної якості є значущими для обох класів платформ: систематичний огляд UX/UI для e-learning підкреслює роль юзабіліті та інтерфейсного дизайну як умов якісного навчального досвіду [4]. Практичні відмінності ілюструє порівняння Moodle та Google Classroom: Moodle забезпечує розгортання повного віртуального освітнього середовища (структуровані ресурси, тестування, підтримка змішаного навчання), але може мати вищий поріг опанування та потребувати підтримки налаштувань; натомість Google Classroom характеризується мінімалістичним інтерфейсом і нижчим порогом входу, однак має обмежені можливості кастомізації та уніфікації складних сценаріїв [2].

На рівні UI-аналізаторів узагальнення публікацій дозволило виокремити три напрями автоматизації:

- Перший – правилові інструменти доступності, що виконують перевірки за заданими критеріями. Емпіричні порівняння фіксують варіативність результатів між інструментами (за покриттям критеріїв, кількістю виявлених проблем і залежністю від типу сторінок), що обґрунтовує використання кількох аналізаторів і обережність в інтерпретації висновків одного інструмента [5]-[7].
- Другий – інструменти з акцентом на прозорість, які пояснюють межі перевірки та логіку результатів; користувачам важливо розуміти, які критерії підтримуються, чому сформовано конкретний висновок і як трактувати розбіжності між інструментами, зокрема в умовах сучасних практик веброзробки [5], [6].
- Третій – AI/LLM-орієнтовані підходи, що генерують текстову критику макетів або виконують кількісне оцінювання та порівняння дизайн-варіантів; продемонстровано можливості швидкого фідбеку на макетах і розвиток моделей оцінювання якості UI на основі великих наборів інтерфейсів і людських оцінок (наприклад, UIClip) [8]-[10].

Як показано в Таблиці 1, класи інструментів відрізняються типом вхідних даних і формою результату, що визначає їх роль у життєвому циклі EdTech-продукту: від автоматизованих перевірок у процесі розробки до аналізу макетів на етапі дизайну та порівняння альтернатив після релізу.

Автоматизовані інструменти доцільно розглядати як засіб підтримки рішень: для контекстних сценаріїв взаємодії їх результати слід доповнювати експертними та користувацькими методами оцінювання [5]-[7].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Порівняння EdTech-платформ і UI-аналізаторів доцільно розглядати як єдиний підхід до забезпечення якості цифрового навчального середовища, а не як два відокремлені рішення. Якщо LMS/MOOC визначають педагогічні сценарії та технологічні можливості, то

UI-аналізатори надають засоби контролю якості взаємодії користувача з інтерфейсом і дозволяють масштабувати аудит без пропорційного зростання витрат.

***Таблиця 1**. Порівняльні характеристики класів UI-аналізаторів*

Клас UI-аналізатора	Тип вхідних даних	Результат	Переваги	Обмеження
Автоматичні тестери вебдоступності	DOM/HTML, CSS, інколи JS-контекст	Перелік помилок/попереджень; інколи прив'язка до критеріїв	Швидкість, масштабованість, регулярний аудит	Неповне покриття; залежність від технологій/шаблонів
Інструменти перевірки доступності з акцентом на прозорість результатів	DOM/візуальне відображення сторінки та метадані правил перевірки	Звіт із поясненнями: що саме перевірено, що не перевірено, і за якими правилами	Вища інтерпретованість; коректні очікування користувачів	Потребують оновлення; не замінюють ручну перевірку складних випадків
Алгоритмічні моделі кількісного оцінювання доступності	Дані вебсторінки, автоматично виділені структурні та візуальні ознаки	Інтегральний показник доступності та/або класифікація рівня; можливе порівняння з іншими оцінками	Узагальнена оцінка; зручно для порівняння	Чутливість до вибору ознак і порогів
LLM-критика UI-макетів	Макет/скриншот або експорт із дизайн-інструмента	Текстові рекомендації та евристичні зауваження	Швидкий фідбек на ранніх етапах	Можливі пропуски/неточності; потрібна верифікація
Моделі оцінювання якості UI	Скриншоти інтерфейсів; інколи текстовий опис/контекст	Оцінка якості та/або ранжування альтернатив; рекомендації щодо покращення	Підтримує порівняння рішень, пошук референсів, напівавтоматизований огляд якості	Високі вимоги до якості й репрезентативності навчальних даних; ризик доменної упередженості
Моделі автоматизованого оцінювання візуальної естетики	Скриншоти інтерфейсів	Оцінка естетичної якості (наближена до людських суджень)	Дає можливість кількісно порівнювати естетичні варіанти; корисно для відбору альтернатив	Естетика не тотожна юзабіліті; переносимість між доменами потребує окремої перевірки

Результати проведеного аналізу дозволяють виокремити такі висновки:

По-перше, відбір LMS доцільно здійснювати за SQTL-подібними критеріями з доповненням UX-показниками реального використання [1], [2].

По-друге, для автоматизованого UI-аудиту ключовою є прозорість: інструменти повинні пояснювати межі перевірки та причини висновків, інакше користувачі неправильно інтерпретуватимуть результати або відмовлятимуться від застосування через несумісні між собою звіти [5]-[7].

По-третє, AI/LLM-інструменти корисні для швидкого фідбеку й порівняння дизайн-альтернатив, однак потребують верифікації результатів у конкретному навчальному контексті [8]–[10].

ДЖЕРЕЛА

1. Sanchez, L., Penarreta, J., & Soria Poma, X. (2024). Learning management systems for higher education: a brief comparison. Discover Education, 3(1). https://doi.org/10.1007/s44217-024-00143-5
2. Крестьянполь, Л., & Верхолюк, А. (2023). ПОРІВНЯЛЬНИЙ АНАЛІЗ ІНТЕРФЕЙСУ КОРИСТУВАЧА ПЛАТФОРМ ДЛЯ ДИСТАНЦІЙНОГО НАВЧАННЯ. Physical and Mathematical Education, 38(1), 28–35. https://doi.org/10.31110/2413-1571-2023-038-1-004
3. Sharova, T., Filatova, O., Kavun, L., Zemlianska, A., & Donii, V. (2023). The Quantitative Analysis of Massive Open Online Courses (MOOC) for Learning English. International Journal of Information and Education Technology.
4. Miya, T. K., & Govender, I. (2022). UX/UI design of online learning platforms and their impact on learning: A review. International Journal of Research in Business and Social Science (2147-4478), 11(10), 316–327. https://doi.org/10.20525/ijrbs.v11i10.2236
5. Manca, M., Palumbo, V., Paternò, F., & Santoro, C. (2023). The transparency of automatic Web accessibility evaluation tools: Design criteria, state of the art, and user perception. ACM Transactions on Accessible Computing, 16(1), 1–36. https://doi.org/10.1145/3556979
6. Iannuzzi, N., Manca, M., Paternò, F., & Santoro, C. (2024). Usability and transparency in the design of a tool for automatic support for web accessibility validation. Universal Access in the Information Society, 23(1), 435–454. https://doi.org/10.1007/s10209-022-00948-x
7. Ратушняк, Т. В., Омельчук, А. А., Гладченко, О. В., Хом'як, А. В., & Хоцкіна, С. М. (2024). ІНКЛЮЗИВНИЙ ВЕБДИЗАЙН: СТАНДАРТИ ТА ЦИФРОВІ ІНСТРУМЕНТИ ТЕСТУВАННЯ ДОСТУПНОСТІ ВЕБСАЙТУ. Applied Questions of Mathematical Modeling, 7(2), 189–206. https://doi.org/10.32782/mathematical-modelling/2024-7-2-17
8. Duan, P., Warner, J., Li, Y., & Hartmann, B. (2024). Generating automatic feedback on UI mockups with large language models. Proceedings of the CHI Conference on Human Factors in Computing Systems, 1–20.
9. Wu, J., Peng, Y.-H., Li, X. Y. A., Swearngin, A., Bigham, J. P., & Nichols, J. (2024). UIClip: A data-driven model for assessing user interface design. Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology, 1–16.
10. Lima, A. L. de S., et al. (2024). A deep learning model for the assessment of the visual aesthetics of mobile user interfaces. Journal of the Brazilian Computer Society, 30(1), 102–115. https://doi.org/10.5753/jbcs.2024.3255



КАРИНА КОНВІСАР
студентка 4 курсу бакалаврату інформаційних технологій у Київському національному університеті імені Тараса Шевченка
E-mail: konvisar_karina@knu.ua
Науковий інтерес: проєктування EdTech-платформ і цифрових навчальних середовищ; методи оцінювання якості інтерфейсів (UX/UI) та цифрової доступності.



АННА ПИЛИПЕНКО
к.т.н., доцент кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0002-6343-4469
E-mail: anna.pylypenko@knu.ua
Науково-педагогічний стаж становить понад 20 років. Має практичний досвід роботи з даними у сфері освітніх аналітичних проєктів та у фінансово-промисловому секторі, а також досвід участі у соціологічних дослідженнях. Наукові інтереси охоплюють машинне навчання, аналіз даних та моделювання інформаційних систем.

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ПІДТРИМКИ ІНВЕСТИЦІЙНИХ РІШЕНЬ У ЗАДАЧАХ ФОРМУВАННЯ ПОРТФЕЛЯ ВАЛЮТНИХ АКТИВІВ

Ярослав Кошулько, Ганна Красовська

Анотація. *У роботі досліджено застосування методів машинного навчання для підтримки прийняття інвестиційних рішень у задачах формування портфелів валютних активів. Запропоновано підхід, що поєднує прогнозування фінансових часових рядів за допомогою нейронних мереж типу LSTM із подальшою оптимізацією структури портфеля на основі моделі Марковіца. Розроблено програмний модуль, який реалізує аналіз історичних фінансових даних, прогнозування дохідності активів та формування рекомендацій щодо структури інвестиційного портфеля.*

Ключові слова: машинне навчання, фінансові часові ряди, нейронні мережі LSTM, портфельна оптимізація, валютні активи, підтримка інвестиційних рішень.

I. ВСТУП

В умовах глобальної економічної нестабільності особливої актуальності набуває проблема ефективного управління фінансовими ресурсами. Одним із доступних інструментів інвестування для широкого кола користувачів є валютні активи. Однак ефективне інвестування потребує аналізу динаміки фінансових ринків, оцінювання ризиків та формування обґрунтованих інвестиційних стратегій. Для інвесторів-початківців ці завдання є складними через необхідність обробки значних обсягів фінансових даних та використання спеціалізованих аналітичних методів.

У таких умовах важливого значення набувають системи підтримки інвестиційних рішень, що дозволяють автоматизувати процес аналізу фінансових даних та формування рекомендацій щодо структури інвестиційного портфеля. Сучасні підходи до аналізу фінансових ринків активно використовують методи машинного навчання та аналізу часових рядів, що дозволяють прогнозувати ринкову динаміку та оцінювати очікувану дохідність активів [1]. Останні дослідження також демонструють зростання інтересу до застосування методів глибинного навчання для задач оптимізації інвестиційних портфелів та управління фінансовими ризиками [2, 3].

Важливу роль у задачах формування інвестиційних портфелів відіграють методи оптимізації, зокрема портфельна теорія Марковіца, яка дозволяє визначати оптимальне співвідношення між ризиком та очікуваною дохідністю активів. Поєднання методів прогнозування фінансових часових рядів із методами портфельної оптимізації відкриває можливості для створення інтелектуальних систем підтримки інвестиційних рішень.

Метою роботи є підвищення ефективності формування інвестиційних портфелів валютних активів шляхом використання методів машинного навчання для прогнозування фінансових часових рядів та подальшої оптимізації структури портфеля.

II. ДАНІ ТА МЕТОДИ

У задачі формування портфеля інвестор розподіляє доступний капітал між набором фінансових активів з метою досягнення оптимального співвідношення між ризиком та очікуваною дохідністю. Для аналізу використовуються історичні дані фінансових ринків, що характеризують зміну вартості активів у часі.

Формально задачу формування інвестиційного портфеля можна описати в рамках моделі Марковіца. Нехай w_i – частка інвестицій у актив i, r_i – очікувана дохідність активу, а Σ – коваріаційна матриця доходностей. Тоді очікувана дохідність портфеля визначається як

$R_p = \sum_i^n w_i r_i$, а ризик портфеля оцінюється через дисперсію $\sigma_p^2 = w^T \Sigma w$, де $w -$ вектор ваг фінансових активів портфеля. Оптимальна структура портфеля визначається шляхом мінімізації ризику за умови нормування ваг активів.

Для прогнозування фінансових часових рядів у роботі використано рекурентні нейронні мережі типу LSTM (Long Short-Term Memory), які здатні моделювати довгострокові залежності у послідовних даних. Нейронні мережі цього типу широко застосовуються у задачах аналізу часових рядів, зокрема для прогнозування фінансових ринків [4].

Крім моделей машинного навчання, для аналізу фінансових часових рядів можуть використовуватися статистичні моделі, зокрема SARIMAX, які дозволяють враховувати сезонні та трендові компоненти даних. У роботі здійснюється порівняння результатів прогнозування різними моделями.

На основі отриманих прогнозів очікуваної дохідності активів формується інвестиційний портфель із використанням моделі Марковіца. У межах цієї моделі оптимізація структури портфеля здійснюється шляхом мінімізації ризику за заданого рівня очікуваної дохідності або максимізації дохідності при обмеженні ризику.

Запропонований у роботі підхід є гібридним і поєднує прогнозування фінансових часових рядів на основі нейронної мережі LSTM із подальшою оптимізацією структури портфеля відповідно до принципів сучасної портфельної теорії.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У результаті дослідження розроблено програмний модуль підтримки інвестиційних рішень, який реалізує процес прогнозування динаміки валютних активів та формування оптимального інвестиційного портфеля.

Програмний модуль включає кілька функціональних компонентів: підсистему збору та обробки історичних фінансових даних, модуль прогнозування часових рядів на основі нейронної мережі LSTM, а також модуль оптимізації структури інвестиційного портфеля відповідно до моделі Марковіца. Система дозволяє аналізувати динаміку валютних активів, прогнозувати їхню майбутню дохідність та формувати рекомендації щодо розподілу інвестиційного капіталу.

Для перевірки ефективності запропонованого підходу проведено експериментальні дослідження на основі історичних фінансових даних валютних активів. У ході експериментів здійснювався аналіз точності прогнозування часових рядів та оцінювання ефективності сформованих інвестиційних портфелів.

Отримані результати показали, що використання нейронної мережі LSTM дозволяє більш точно враховувати часові залежності у фінансових даних порівняно з класичними статистичними моделями. Поєднання прогнозних моделей із портфельною оптимізацією забезпечує формування більш збалансованих інвестиційних стратегій.

Крім того, розроблений програмний модуль дозволяє автоматизувати процес аналізу інвестиційних можливостей та формування рекомендацій щодо структури портфеля, що значно спрощує прийняття рішень для інвесторів із недостатнім досвідом роботи на фінансових ринках.

IV. ВИСНОВКИ

У роботі досліджено можливості застосування методів машинного навчання для підтримки прийняття інвестиційних рішень у сфері валютних інвестицій. Проведений аналіз показав, що поєднання моделей прогнозування фінансових часових рядів із методами

портфельної оптимізації дозволяє підвищити ефективність формування інвестиційних портфелів.

Запропонований гібридний підхід, що поєднує нейронну мережу LSTM та модель Марковіца, дозволяє враховувати як прогнозовану дохідність активів, так і ризики, пов'язані з їх включенням до портфеля. Це забезпечує більш обґрунтоване формування інвестиційних стратегій у порівнянні з традиційними методами аналізу.

Практична значущість роботи полягає у створенні програмного модуля підтримки інвестиційних рішень, який може бути використаний як основа для розроблення інтелектуальних фінансових асистентів та систем аналізу інвестиційних портфелів.

Подальші дослідження можуть бути спрямовані на вдосконалення моделей прогнозування фінансових часових рядів, розширення набору фінансових інструментів та інтеграцію додаткових методів оптимізації інвестиційних портфелів.

ДЖЕРЕЛА

1. Sezer O. B., Gudelek M. U., Ozbayoglu A. M. (2020) Financial time series forecasting with deep learning: A systematic literature review. Applied Soft Computing, 90, 106181. https://doi.org/10.1016/j.asoc.2020.106181
2. Chen X., Li Y., Wang Z. (2024) Deep learning approaches for portfolio optimization and financial forecasting. Electronic Research Archive, 32(4), 239–256. https://doi.org/10.3934/era.2024239
3. Buehler H., Gonon L., Teichmann J., Wood B. (2019) Deep hedging. Quantitative Finance, 19(8), 1271–1291. https://doi.org/10.1080/14697688.2019.1571683
4. Fischer T., Krauss C. (2018) Deep learning with long short-term memory networks for financial market predictions. European Journal of Operational Research, 270(2), 654–669. https://doi.org/10.1016/j.ejor.2017.11.054



ЯРОСЛАВ КОШУЛЬКО
студент 4 курсу бакалаврату освітньої програми «Комп'ютерні науки» у Київському національному університеті імені Тараса Шевченка.
E-mail: yaroslavkoshylko@knu.ua
Студент Київського національного університету імені Тараса Шевченка.
Наукові інтереси – машинне навчання, інтелектуальний аналіз фінансових даних, прогнозування часових рядів, оптимізація інвестиційних портфелів.



ГАННА КРАСОВСЬКА
к.т.н., доцент, доцент кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
ORCID: 0000-0003-1986-6130
E-mail: hanna.krasovska@knu.ua
Фахівець у галузі інтелектуальних технологій. Має багаторічний досвід науково-педагогічної діяльності та підготовки фахівців з комп'ютерних наук, зокрема у сфері систем штучного інтелекту. Наукові інтереси – інтелектуальні технології підтримки прийняття рішень, моделювання та аналіз складних систем.

ТИПОЛОГІЯ ПОМИЛОК МАШИННОГО ПЕРЕКЛАДУ В ІГРОВИХ ТЕКСТАХ ТА СТРАТЕГІЇ ЇХ ПОСТРЕДАГУВАННЯ (PEMT)

Ольга Солодка

Анотація. *У роботі буде проаналізовано специфіку застосування нейромережевого машинного перекладу в локалізації відеоігор. Дослідження окреслить основні виклики ігрового дискурсу та представить типологію помилок NMT на основі моделі MQM, зокрема: гендерну інтерференцію, технічні збої в обробці змінних та термінологічну неузгодженість. Велика увага буде приділена обґрунтуванню стратегій постредагування (PEMT), що дозволять оптимізувати процес підготовки контенту без втрати імерсивності. У висновках буде визначено нову роль перекладача як оператора інтелектуальних систем у сучасному циклі локалізації.*

Ключові слова: локалізація відеоігор, нейромережевий машинний переклад (NMT), постредагування (PEMT), контроль якості, типологія помилок, MQM.

I. ВСТУП

Сучасна індустрія інтерактивних розваг перебуває на етапі інтенсивної глобалізації, що докорінно змінює підходи до підготовки контенту. Перехід до бізнес-моделі simultaneous shipment, яка передбачає одночасний реліз цифрового продукту на десятках ринків, ставить перед локалізаційними відділами безпрецедентні вимоги щодо швидкості обробки даних. Враховуючи, що обсяг текстового наповнення у сюжетно-орієнтованих AAA-проєктах (жанри RPG, Adventure) часто перевищує 1 мільйон слів, виключне використання традиційного людського перекладу (Human Translation – HT) стає економічно нерентабельним і часозатратним. Це спонукає розробників та локалізаційні агенції (LSP) до інтеграції систем нейромережевого машинного перекладу у виробничі процеси [1].

Однак ігровий дискурс є специфічним гетерогенним середовищем, що поєднує ознаки художнього наративу, розмовного стилю та елементи програмного коду. Нейромережі, які зазвичай навчаються на корпусах загальної лексики або офіційно-ділових текстів, стикаються з унікальними викликами при обробці фрагментованих ігрових рядків. Метою даної роботи є аналіз специфічних помилок NMT у відеоіграх, класифікація їх причин та обґрунтування ефективних стратегій постредагування (PEMT), що дозволять зберегти баланс між автоматизацією та якістю.

II. ДАНІ ТА МЕТОДИ

Аналіз ефективності NMT у сфері розваг вимагає відмови від суто кількісних підходів. Стандартні автоматичні метрики оцінки якості, такі як BLEU (Bilingual Evaluation Understudy) або TER (Translation Edit Rate), фокусуються на лексичній відповідності еталонному перекладу, але ігнорують семантичні та прагматичні аспекти. Для ігрового тексту критично важливими є функціональність (чи вміщується текст у кнопку, чи працюють змінні) та імерсивність (чи відповідає стиль атмосфері гри) [2].

У зв’язку з цим, методологічною основою дослідження варто обрати адаптовану модель MQM (Multidimensional Quality Metrics), оновлену для задач генеративного ШІ. Цей підхід дозволяє класифікувати помилки не лише за лінгвістичними рівнями, а й за ступенем їхньої критичності для користувацького досвіду (User Experience). Особлива увага приділяється категорії «critical errors» – помилкам, що можуть призвести до технічних збоїв гри або повного викривлення змісту квестів [3].

Важливою перевагою моделі MQM над автоматичними метриками є її ієрархічна структура, що дозволяє диференціювати помилки за їхнім впливом на геймплей. У контексті

відеоігор ми розглядаємо не лише граматичну правильність, а й технічну валідність рядків. Оскільки ігрові тексти часто існують у вигляді розрізнених сегментів у таблицях, традиційні системи NMT втрачають контекстуальні зв'язки. Застосування багатовимірних метрик дозволяє виявити випадки, де переклад є формально правильним, але функціонально непридатним для використання в інтерфейсі (наприклад, через перевищення ліміту символів або спотворення логіки квесту).

В основі аналізу лежить вивчення здатності алгоритмів розпізнавати специфічний ігровий жаргон та архаїзми, характерні для комп'ютерних ігор. Оскільки нейромережі базуються на статистичних імовірностях, вони схильні до помилок у випадках, коли ігровий термін має поширене загальновживане значення. Це створює необхідність глибшого вивчення механізмів семантичного аналізу, які використовують сучасні системи для обробки художньо-технічних текстів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

На основі порівняльного аналізу сирого машинного перекладу та фінальної локалізації виокремлено три ключові кластери проблем, притаманних застосуванню NMT в іграх:

1. Контекстуально-гендерна інтерференція. Найбільш поширеною проблемою при перекладі з англійської мови на флективні (зокрема українську) є втрата інформації про рід. Англійські звертання (*Champion, Hero, Wanderer*) та конструкції (*I am tired, You are dead*) є гендерно нейтральними. NMT-системи, працюючи на рівні ізольованого речення (sentence-level translation) і не маючи доступу до метаданих гри (стать обраного персонажа), за замовчуванням узгоджують переклад у чоловічому роді. Це призводить до грубих граматичних помилок у репліках жіночих персонажів (напр., «*I am lost*» → «*Я загубився*» замість «*Я загубилася*»). Такі помилки руйнують імерсію та викликають негативну реакцію гравців [4].

2. Технічні помилки обробки змінних. Ігрові тексти насичені елементами коду: плейсхолдерами ({Unit_Name}, %s), тегами форматування (
, <color=red>) та службовими символами. Нейромережі часто хибно ідентифікують їх як частину природної мови. Спостерігаються спроби перекладу назв змінних (напр., {Chest_ID} → {Скриня_ID}), їх транслітерації або зміни синтаксичного порядку слів, що розриває логіку коду. Наслідком таких помилок стають «game-breaking bugs» — ситуації, коли текст не відображається у грі, підтягує некоректні дані або викликає аварійне завершення роботи програми [2].

3. Термінологічна неузгодженість (Lore Inconsistency). Кожен ігровий проєкт має унікальну термінологічну базу (Lore) — назви локацій, рас, предметів, заклять. Без попереднього налаштування (fine-tuning) NMT схильний до синонімії. Один і той самий термін, наприклад «*Dungeon*», може бути перекладений у різних частинах гри як «*підземелля*», «*темниця*», «*льох*» або «*каземат*». Така варіативність дезорієнтує гравця, ускладнюючи виконання завдань, де точність назв є критичною [5].

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

Проведене дослідження підтверджує, що повна автоматизація локалізації сюжетно-орієнтованих ігор на поточному етапі розвитку технологій є неможливою через високу прагматичну складність ігрового дискурсу. Для нівелювання виявлених помилок і підвищення якості фінального продукту пропонується впровадження комплексної стратегії PEMT, яка базується на трьох рівнях оптимізації:

1. Пре-процесинг та системний захист даних. Необхідним етапом є автоматична обробка тексту до початку перекладу. Використання регулярних виразів дозволяє ідентифікувати змінні, плейсхолдери та теги, замінюючи їх на захищені токени, які

ігноруються нейромережею. Експериментально доведено, що такий підхід дозволяє усунути до 90% технічних помилок («game-breaking bugs») ще до втручання лінгвіста.

2. Категоризація та диференціація контенту (Content Triage). Враховуючи обсяги ААА-проєктів, доцільно застосовувати вибірковий підхід до постредагування. Технічні тексти, системні повідомлення та інструкції можуть піддаватися легкому постредагуванню (Light PE) для забезпечення базової зрозумілості. Натомість художні діалоги, сюжетні описи та елементи побудови ігрового всесвіту вимагають повного постредагування (Full PE) або повної творчої адаптації для збереження емоційного забарвлення та імерсивності.

3. Інтеграція динамічних глосаріїв та Lore-менеджмент. Підключення термінологічних баз безпосередньо до рушія NMT забезпечує консистентність ключових понять, назв локацій та імен персонажів. Це дозволяє уникнути синонімічної варіативності, яка дезорієнтує гравця.

Перспективи подальших досліджень полягають у вивченні можливостей контекстно-залежних LLM-моделей, які здатні враховувати метадані (стать персонажа, стиль мовлення) безпосередньо під час генерації перекладу. Це може частково розв'язати проблему гендерної інтерференції, яка зараз є найбільш критичною для флективних мов, зокрема української.

Інтеграція NMT у локалізацію відеоігор є незворотним процесом, зумовленим ринковими реаліями та потребою у simultaneous shipment. Проте роль перекладача не нівелюється, а трансформується: фахівець стає оператором інтелектуальних систем. Головним завданням лінгвіста в новій парадигмі є забезпечення тонкого балансу між технічною коректністю коду та високою художньою якістю адаптації, що наразі залишається недосяжним для алгоритмів.

ДЖЕРЕЛА

1. Bernal-Merino M. Á., Costales A. F. (2022) Video Game Localization: The role of Artificial Intelligence, Journal of Internationalization and Localization, vol. 9, no. 2, pp. 112–134.
2. Zhang X., Toral A. (2023) The Impact of Large Language Models on Game Localization Quality: A Comparative Study, Proceedings of the 24th Annual Conference of the European Association for Machine Translation, Tampere, p. 210–220.
3. Klubička F., Toral A., Sánchez Cartagena V. M. (2024) Quantitative Fine-Grained Human Evaluation of Machine Translation Systems: Adapting MQM for the AI Era, Machine Translation, vol. 38, pp. 45–72.
4. Savoldi B. et al. (2021) Gender Bias in Machine Translation: A Comprehensive Survey of the Latest Challenges, Transactions of the Association for Computational Linguistics, vol. 9, pp. 845–874.
5. Radicioni G. (2023) Post-editing in the Video Game Industry: New Workflows and Roles, Translation Spaces, vol. 12, is. 1, pp. 88–109.



ОЛЬГА СОЛОДКА
Студентка, Навчально-науковий інститут філології Київського національного університету імені Тараса Шевченка, Київ, Україна
ORCID: 0009-0006-6485-8227
E-mail: olya.sol.ck@gmail.com
Сфера наукових інтересів охоплює комп’ютерну лінгвістику, особливості локалізації відеоігрового контенту, стратегії постредагування (PEMT), а також акустичний аналіз та автоматичне розпізнавання емоцій у мовленні (SER).

МОДЕЛІ ТА МЕТОДИ АПРОКСИМАЦІЇ ДАНИХ З ВИКОРИСТАННЯМ ТРИГОНОМЕТРИЧНИХ СПЛАЙНІВ У ЗАДАЧАХ КОМП'ЮТЕРНОГО ЗОРУ

Ганна Терещук, Микола Пирог

Анотація. *У роботі досліджено моделі апроксимації даних на основі тригонометричних сплайнів для задач комп'ютерного зору. Проаналізовано вплив параметрів сплайнів на точність реконструкції контурів, стійкість алгоритмів та зменшення осциляційних ефектів, зокрема явища Гібса. Запропоновано підхід до згладжування сигналів із використанням L-підсумовування та згладжувальних множників. Результати демонструють підвищену точність апроксимації та ефективність у задачах сегментації, векторизації та попередньої обробки зображень.*

Ключові слова: тригонометричні сплайни, апроксимація сигналів, комп'ютерний зір, реконструкція контурів, явище Гібса.

I. ВСТУП

Стрімкий розвиток технологій комп'ютерного зору обумовлює необхідність створення ефективних математичних моделей для обробки та аналізу візуальних даних.

Сучасні системи комп'ютерного зору широко застосовуються у медичній діагностиці, автономних транспортних системах, робототехніці, системах відеоспостереження та автоматичному розпізнаванні об'єктів. Важливим компонентом систем комп'ютерного зору є алгоритми виділення контурів (edge detection), які забезпечують ідентифікацію структурних меж об'єктів на зображенні. Як показано у роботі [1], ефективність таких алгоритмів значною мірою залежить від якості попередньої апроксимації сигналів зображення та зменшення шумових і спектральних артефактів.

Однією з фундаментальних задач у цій галузі є побудова точних моделей апроксимації сигналів та геометричних структур, що описують контури, текстури та інші структурні характеристики зображень. У задачах комп'ютерного зору зображення доцільно розглядати як двовимірний дискретний сигнал, що містить області різкої зміни інтенсивності, які відповідають межам об'єктів. Така інтерпретація дозволяє застосовувати методи спектрального аналізу та апроксимації сигналів для моделювання контурів і структурних елементів зображення.

II. ДАНІ ТА МЕТОДИ

Традиційні підходи до апроксимації та інтерполяції даних, зокрема методи, що базуються на поліноміальних сплайнах і спектральних представленнях, широко застосовуються в задачах цифрової обробки сигналів та зображень [4]. Серед основних недоліків можна виділити виникнення осциляцій поблизу точок розриву (явище Гібса), складність коректного моделювання періодичних структур зображень та недостатню стійкість чисельних алгоритмів при обробці багатовимірних даних. Подібні осциляційні артефакти активно досліджуються у сучасних роботах з цифрової обробки зображень. Зокрема, у дослідженні [3] показано, що ефект Гібса може суттєво спотворювати профілі інтенсивності зображень та негативно впливати на точність реконструкції контурів і сегментації.

Це обмежує ефективність використання традиційних методів у задачах згладжування сигналів, відновлення контурів (edge reconstruction) та виділення ознак (feature extraction).

Перспективним напрямом розв'язання зазначених проблем є застосування тригонометричних сплайнів, які поєднують властивості періодичності, гладкості та високої апроксимаційної здатності. У сучасних дослідженнях також показано ефективність сплайнових моделей у задачах обробки та векторизації зображень. Зокрема, у роботі [5] запропоновано підхід до векторизації зображень на основі TCB-сплайнів, що дозволяє точно відтворювати контури об'єктів та їх геометричні характеристики у векторному представленні. Використання таких сплайнів дозволяє ефективно моделювати періодичні та квазіперіодичні структури зображень, зменшувати осциляційні ефекти та забезпечувати стабільність чисельних алгоритмів при обробці сигналів.

Крім того, сучасні моделі тригонометричних сплайнів з параметрами керування формою дозволяють гнучко регулювати гладкість апроксимації та властивості реконструкції сигналу [2]. Це створює передумови для використання таких моделей у задачах обробки зображень, зокрема при згладжуванні шумів та відновленні контурів об'єктів.

III. РЕЗУЛЬТАТИ ТА АНАЛІЗ

У межах проведеного дослідження розроблено математичні моделі використання парних та повних тригонометричних сплайнів для апроксимації даних, що виникають у задачах комп'ютерного зору.

Проведено аналіз впливу параметрів сплайнів на точність апроксимації та стабільність обчислювальних алгоритмів при обробці цифрових зображень. Варіювання параметрів тригонометричних сплайнів дозволяє адаптувати модель апроксимації до структурних особливостей сигналу зображення. Це забезпечує можливість контролю гладкості реконструкції та покращує відтворення контурів у областях із різкими змінами інтенсивності.

Особливу увагу приділено дослідженню апроксимації контурів об'єктів та структурних елементів зображення, що є важливим етапом у задачах сегментації та розпізнавання об'єктів.

Виконано порівняльний аналіз результатів апроксимації, отриманих за допомогою тригонометричних сплайнів та класичних чисельних методів.

Отримані результати демонструють підвищену точність апроксимації, швидшу збіжність алгоритмів та кращу стійкість до шумових спотворень зображення.

Додатково досліджено вплив розривів функцій та їх похідних на точність апроксимаційних моделей у задачах реконструкція контурів зображень.

Для зменшення впливу осциляційних ефектів при апроксимації сигналів запропоновано застосування різних методів L-підсумовування, що дозволяє ефективно згладжувати явище Гібса при інтерполяції дискретних даних. Чисельні експерименти показують, що використання згладжувальних множників дозволяє суттєво зменшити амплітуду осциляцій поблизу розривів сигналу. Це сприяє покращенню геометричної точності реконструкції контурів та підвищує ефективність алгоритмів подальшої обробки зображень.

Запропонований підхід забезпечує покращення якості реконструкції контурів та підвищує ефективність алгоритмів сегментації зображень.

Практична реалізація розроблених алгоритмів орієнтована на інтеграцію у програмні комплекси комп'ютерного зору для задач згладжування сигналів, відновлення геометричних характеристик об'єктів, аналізу текстур та попередньої обробки зображень.

Запропоновані методи можуть використовуватись як ефективний інструмент підвищення якості обробки візуальних даних у системах автоматичного аналізу зображень та відеопотоків.

IV. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У роботі розроблено та досліджено математичні моделі апроксимації даних на основі парних і повних тригонометричних сплайнів, орієнтовані на задачі комп'ютерного зору. Показано, що варіювання параметрів сплайнів дозволяє адаптувати апроксимацію до структурних особливостей зображень, забезпечуючи контроль гладкості та підвищення точності реконструкції контурів у зонах різких змін інтенсивності.

Доведено, що застосування методів L-підсумовування та згладжувальних множників ефективно зменшує осциляційні артефакти, зокрема прояви явища Гібса, що підтверджено чисельними експериментами. Порівняльний аналіз показав переваги тригонометричних сплайнів над класичними методами щодо точності, збіжності та стійкості до шумів.

Отримані результати підтверджують доцільність використання тригонометричних сплайнів у задачах реконструкції контурів, сегментації та попередньої обробки зображень. Подальші дослідження передбачають розробку багатовимірних моделей та інтеграцію запропонованих підходів у сучасні системи комп'ютерного зору.

ДЖЕРЕЛА

1. Jing, J., Wang, Z., Raheem, M. and Wang, X., 2022. Recent advances on image edge detection: A comprehensive review. Neurocomputing, 503, pp.259–276.
2. Munir, A., Samreen, S., Ghaffar, A. et al., 2024. A new cubic trigonometric Nu-Spline with shape control parameter and its applications. European Physical Journal Plus, 139, p.606.
3. Poggiali, D., Magri, L. and Biondi, A., 2022. Reducing the Gibbs effect in multimodal medical imaging by means of oversampling strategies. Results in Engineering, 13, p.100332.
4. Sun, Z. and Gao, W., 2022. High order multiquadric trigonometric quasi-interpolation method for solving time-dependent partial differential equations. Numerical Algorithms, 93, pp.1105–1130.
5. Zhu, H., Zhong, Z. and Wu, J., 2022. TCB-spline-based image vectorization. ACM Transactions on Graphics, 41(4), Article 109.



ГАННА ТЕРЕЩУК
асистент кафедри інформаційних систем та технологій, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0001-7573-9748
E-mail: tereshchukh@fit.knu.ua
Закінчила фізико-математичний факультет Національного технічного університету України «Київський політехнічний інститут» за спеціальністю «Математика». Сферою наукової діяльності є ІКТ в освіті, моделювання інформаційних систем.



МИКОЛА ПИРОГ
асистент кафедри інформаційних систем та технологій, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0003-2588-6066
E-mail: m.pyroh@knu.ua
Закінчив Приватний вищий навчальний заклад «Європейський університет» за спеціальністю «Інформаційні управляючі системи та технології». Сферою наукової діяльності є дослідження питання ІКТ в освіті, впровадження гнучких методологій в освітній процес.

Наукове видання

Матеріали
3-ї Міжнародної науково-практичної конференції
«Інформаційні системи та технології: результати і перспективи»
(IST 2026)

10 березня 2026 року

Друкується за авторською редакцією

Формат 60x84$^{1/16}$. Обл.-вид. арк. 36,33. Ум. друк. арк. 55,1. Зам. № 219-9319.
Гарнітура Times New Roman. Електронне видання.
Підписано до друку 26.03.26

Видавець і виготовлювач
ВПЦ "Київський університет"
Б-р Тараса Шевченка, 14, м. Київ, 01601, Україна
☎ (38044) 239 32 22; (38044) 239 31 58; (38044) 239 31 28
e-mail: vpc@knu.ua
http: vpc.knu.ua
Свідоцтво суб'єкта видавничої справи ДК № 1103 від 31.10.02