

# Information technologies in economics and environmental sciences



**No 2 / 2025**

# **Information Technologies in Economics and Environmental Sciences**

## **Founder:**

National University of Life and Environmental Sciences of Ukraine

Faculty of Information Technologies

Year of foundation: 2017

Published 2 times a year

## **Media identifier – R40-02287**

The National Council of Television and Radio Broadcasting of Ukraine

Decision No. 2543 of 20 November 2025, protocol No. 25.

## **Editors office address:**

National University of Life and Environmental Sciences of Ukraine

03041, 15 Heroiv Oborony Str., Kyiv, Ukraine

E-mail: [it-journal@nubip.edu.ua](mailto:it-journal@nubip.edu.ua)

<https://journals.nubip.edu.ua/index.php/Inf/en/>

# **Інформаційні технології в економіці та природокористуванні**

## **Засновник журналу:**

Національний університет біоресурсів і природокористування України

Факультет інформаційних технологій

Рік заснування: 2017

Виходить 2 рази на рік

## **Ідентифікатор медіа – R40-06595**

Рішення Національної Ради України з питань телебачення і радіомовлення від  
20.11.2025 р. № 2543, протокол № 25

## **Адреса редакції:**

Національний університет біоресурсів і природокористування України

03041, вул. Героїв Оборони, 15, м. Київ, Україна

E-mail: [it-journal@nubip.edu.ua](mailto:it-journal@nubip.edu.ua)

<https://journals.nubip.edu.ua/index.php/Inf/uk>

## EDITORIAL BOARD

### *Editor-in-Chief*

**Hlazunova Olena** | D.Sc. (Pedagogical Sciences), Professor, National University of Life and Environmental Sciences of Ukraine

### *Deputy Editor-in-Chief*

**Kravchenko Volodymyr** | D.Sc. (Economics), Associate Professor, National University of Life and Environmental Sciences of Ukraine

### *Editorial Board Members*

**Bolbot Igor** | D.Sc. (Technical Sciences), Professor, National University of Life and Environmental Sciences of Ukraine

**Fedoryshyn Roman** | D.Sc. (Technical Sciences), Professor, Lviv Polytechnic National University

**Gusev Borys** | Ph.D. (Technical Sciences), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Holub Bella** | Ph.D. (Technical Sciences), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Holub Tetiana** | Ph.D. (Technical Sciences), National University "Zaporizhzhia Polytechnic", Ukraine

**Ivanchenko Yevheniia** | Ph.D. (Technical Sciences), Professor, National Aviation University, Ukraine

**Kovalenko Oleksiy** | D.Sc. (Technical Sciences), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Lobanchykova Nadiia** | Ph.D. (Technical Sciences), Associate Professor, Zhytomyr Polytechnic State University, Ukraine

**Mokriev Maksym** | Ph.D. (Economics), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Nikitenko Yevheniy** | Ph.D. (Physics and Mathematics), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Oliinyk Andrii** | D.Sc. (Technical Sciences), Professor, National University "Zaporizhzhia Polytechnic", Ukraine

**Sahun Andrii** | Ph.D. (Technical Sciences), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Svatko Vitaliy** | Ph.D. (Technical Sciences), Associate Professor, National University of Life and Environmental Sciences of Ukraine

**Semko Viktor** | D.Sc. (Technical Sciences), Professor, National University of Life and Environmental Sciences of Ukraine

<b>Skrupsky Stepan</b>	Ph.D. (Technical Sciences), Associate Professor, National University "Zaporizhzhia Polytechnic", Ukraine
<b>Smolij Viktorija</b>	D.Sc. (Technical Sciences), Professor, National University of Life and Environmental Sciences of Ukraine
<b>Khilenko Volodymyr</b>	D.Sc. (Technical Sciences), Professor, National University of Life and Environmental Sciences of Ukraine
<b>Shvydenko Mykhailo</b>	Ph.D. (Economics), Associate Professor, National University of Life and Environmental Sciences of Ukraine
<b>Shkarupylo Vadym</b>	D.Sc. (Technical Sciences), Associate Professor, National University of Life and Environmental Sciences of Ukraine

### *International Members of the Editorial Board*

<b>Akhmetov Bakhytzhhan</b>	D.Sc. (Technical Sciences), Professor, Turan University, Kazakhstan, Almaty
<b>Jamil Abedalrahim Jamil Alsayaydeh</b>	Ph.D., Universiti Teknikal Malaysia Melaka (UTeM)
<b>Zherlitsyn Dmytro</b>	D.Sc. (Economics), Professor, Institute of Entrepreneurship, University of National and World Economy, Bulgaria, Sofia
<b>Mikulecky Peter</b>	Ph.D., Professor, RNDr., University of Hradec Kralove, Czech Republic, Hradec Kralove

## РЕДАКЦІЙНА КОЛЕГІЯ

### *Головний редактор*

**Глазунова Олена Григорівна** | доктор педагогічних наук, професор, Національний університет біоресурсів і природокористування України

### *Заступник головного редактора*

**Кравченко Володимир Миколайович** | доктор економічних наук, доцент, Національний університет біоресурсів і природокористування України

### *Національні члени редколегії*

**Болбот Ігор Михайлович** | доктор технічних наук, професор, Національний університет біоресурсів і природокористування України

**Голуб Белла Львівна** | кандидат технічних наук, доцент, Національний університет біоресурсів і природокористування України

**Голуб Тетяна Василівна** | кандидат технічних наук, Національний університет «Запорізька політехніка»

**Гусєв Борис Семенович** | кандидат технічних наук, доцент, Національний університет біоресурсів і природокористування України

**Іванченко Євгенія Вікторівна** | кандидат технічних наук, професор, Національний авіаційний університет

**Коваленко Олексій Єпіфанович** | доктор технічних наук, доцент, Національний університет біоресурсів і природокористування України

**Лобанчикова Надія Миколаївна** | кандидат технічних наук, доцент, Державний університет «Житомирська політехніка»

**Мокрієв Максим Володимирович** | кандидат економічних наук, доцент, Національний університет біоресурсів і природокористування України

**Нікітенко Євгеній Васильович** | кандидат фізико-математичних наук, доцент, Національний університет біоресурсів і природокористування України

**Олійник Андрій Олександрович** | доктор технічних наук, професор, Національний університет «Запорізька політехніка»

**Сагун Андрій Вікторович** | кандидат технічних наук, доцент, Національний університет біоресурсів і природокористування України

**Сватко Віталій Володимирович** | кандидат технічних наук, доцент, Національний університет біоресурсів і природокористування України

**Семко Віктор Володимирович** | доктор технічних наук, професор, Національний університет біоресурсів і природокористування України

**Скрупський Степан Юрійович** | кандидат технічних наук, доцент, Національний університет «Запорізька політехніка»

<b>Смолій Вікторія Миколаївна</b>	доктор технічних наук, професор, Національний університет біоресурсів і природокористування України
<b>Федоришин Роман Миронович</b>	доктор технічних наук, професор, Національний університет «Львівська політехніка»
<b>Хиленко Володимир Васильович</b>	доктор технічних наук, професор, Національний університет біоресурсів і природокористування України
<b>Швиденко Михайло Зіновійович</b>	кандидат економічних наук, доцент, Національний університет біоресурсів і природокористування України
<b>Шкарупило Вадим Вікторович</b>	доктор технічних наук, доцент, Національний університет біоресурсів і природокористування України

### *Міжнародні члени редколегії*

<b>Ахметов Бахитжан Сражатдінович</b>	доктор технічних наук, професор, університет Туран (м. Алмати, Казахстан)
<b>Жаміль Абедалярахім Жаміль Альсяядех</b>	PhD, Технічний університет Малайзії, Мелака (UTeM)
<b>Жерліцин Дмитро Михайлович</b>	доктор економічних наук, професор, Інститут підприємництва Університету національної та світової економіки (м. Софія, Болгарія)
<b>Мікулецький Пітер</b>	PhD, професор, RNDr., Університет Градець-Кралове (м. Градець-Кралове, Чехія)

## CONTENTS

Smolij Viktorija, Smolij Natan

MACHINE VISION MODULE FOR OBJECT DETECTION IN IMAGES AND VIDEO STREAMS .....9

Nikolaienko Dmytro, Li Yulong

SEMANTIC SEGMENTATION OF FETAL BRAIN ULTRASOUND IMAGES BASED ON A GENERAL FULLY CONVOLUTIONAL DISCRIMINATOR..... 18

Borodkina Iryna, Borodkin Heorhii, Milovidov Yurii

PROGRAMMING LANGUAGE SELECTION FOR INTELLIGENT FOREST MONITORING AND FIRE-FIGHTING SYSTEMS USING THE ANALYTIC HIERARCHY PROCESS.....28

Vaskivskyi Vadym, Gorovyi Iaroslav, Smolii Victor

DIGITAL TWINS TECHNOLOGIES IN AGRICULTURAL PROJECT MANAGEMENT SYSTEMS .....36

Nazarenko Volodymyr, Ostroushko Bogdan

MODELING EVALUATION FRAMEWORK FOR ROBOTICS AND DIGITAL TWIN SIMULATION PLATFORMS WITH AN UNREAL ENGINE 5 WAREHOUSE CASE STUDY .....45

Lakhno Valerii, Kasatkin Dmytro

A FUZZY-LOGICAL MODEL FOR ASSESSING THE STATUS OF AN INFORMATION SYSTEM DURING DDOS ATTACKS..... 56

Nikitenko Yevheniy, Gladkij Anatolij

SPECIALIZED MODULE BASED ON ARDUINO FOR A CAR SECURITY SYSTEM .....63

Sahun Andrii, Panasko Olena

TRENDS IN INCREASING THE CRYPTO-STRENGTH OF SYMMETRIC BLOCK CIPHERS IN THE CONTEXT OF THE MODERN CRYPTOSYSTEMS DEVELOPMENT .....72

## ЗМІСТ

Смолій Вікторія Миколаївна, Смолій Натан Вікторович МОДУЛЬ МАШИННОГО ЗОРУ ДЛЯ ВИЯВЛЕННЯ ОБ’ЄКТІВ НА ЗОБРАЖЕННЯХ І У ВІДЕОПОТОЦІ .....	9
Ніколаєнко Дмитро Володимирович, Лі Юйлун СЕМАНТИЧНА СЕГМЕНТАЦІЯ УЛЬТРАЗВУКОВИХ ЗОБРАЖЕНЬ МОЗКУ ПЛОДА НА ОСНОВІ ЗАГАЛЬНОГО ПОВНІСТЮ ЗГОРТКОВОГО ДИСКРИМІНАТОРА .....	18
Бородкіна Ірина Лаврентіївна, Бородкін Георгій Олексійович, Міловідов Юрій Олегович ВИБІР МОВИ ПРОГРАМУВАННЯ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ МОНІТОРИНГУ ЛІСІВ І ПРОТИДІЇ ПОЖЕЖАМ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЙ.....	28
Васьківський Вадим Олександрович, Горовий Ярослав Миколайович, Смолій Віктор Вікторович ТЕХНОЛОГІЇ DIGITAL TWINS У СИСТЕМАХ УПРАВЛІННЯ АГРАРНИМИ ПРОЕКТАМИ .....	36
Назаренко Володимир Анатолійович, Остроушко Богдан Павлович ВІРТУАЛЬНА СИСТЕМА МОДЕЛЮВАННЯ ДЛЯ РОБОТОТЕХНІКИ ТА ПЛАТФОРМ СИМУЛЯЦІЇ ЦИФРОВИХ ДВІЙНИКІВ З ПРИКЛАДОМ СКЛАДСЬКОЇ СИСТЕМИ В UNREAL ENGINE 5 .....	45
Лахно Валерій Анатолійович, Касаткін Дмитро Юрійович НЕЧІТКО-ЛОГІЧНА МОДЕЛЬ ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІД ЧАС DDOS-АТАК .....	56
Нікітенко Євгеній Васильович, Гладкий Анатолій Михайловичі СПЕЦІАЛІЗОВАНИЙ МОДУЛЬ НА БАЗІ ARDUINO ДЛЯ АВТОМОБІЛЬНОЇ СИСТЕМИ БЕЗПЕКИ .....	63
Сагун Андрій Вікторович, Панаско Олена Миколаївна ТЕНДЕНЦІЇ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ МІЦНОСТІ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ У КОНТЕКСТІ СУЧАСНОГО РОЗВИТКУ КРИПТОСИСТЕМ.....	72

УДК 004.3

**Смолій Вікторія Миколаївна***доктор технічних наук, професор, професор кафедри інформаційних систем та технологій, Національний університет біоресурсів і природокористування України*ORCID: <https://orcid.org/0000-0002-1268-7837>E-mail: [vmsmolij@nubip.edu.ua](mailto:vmsmolij@nubip.edu.ua)**Смолій Натан Вікторович***здобувач спеціальності «Інформаційні системи та технології», Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»*ORCID: <https://orcid.org/0009-0002-3763-6726>E-mail: [hoibbitizukrainy@gmail.com](mailto:hoibbitizukrainy@gmail.com)**МОДУЛЬ МАШИННОГО ЗОРУ ДЛЯ ВИЯВЛЕННЯ ОБ'ЄКТІВ НА ЗОБРАЖЕННЯХ І У ВІДЕОПОТОЦІ**

***Анотація.** Робота присвячена актуальній тематиці створення та застосування інтелектуальних методів комп'ютерного зору для автоматизованого виявлення й сегментації об'єктів захисного спорядження на зображеннях і у відеопотоці. Мета роботи полягає у визначенні об'єктів заданого типу на зображеннях, отриманих із відеокамери, а також розробці моделі детекції, яка зможе ефективно ідентифікувати та локалізувати ці об'єкти в різних умовах освітлення, масштабу та перспективи. В матеріалі статті досліджено досліджено процес підготовки даних, зокрема застосування методів аугментації для підвищення репрезентативності вибірки, а також виконано порівняльний аналіз параметрів, швидкодії та результатів роботи моделей SAM і YOLO. Наведено результати експериментальних досліджень, які свідчать про позитивний вплив збільшення обсягу та різноманітності датасету на збалансованість даних і узагальнювальну здатність моделей комп'ютерного зору. Запропоновані підходи окремого навчання моделей для задач сегментації та класифікації підтвердили свою ефективність у контексті автоматизованої обробки зображень. В роботі для реалізації завдання сегментації зображень було сформовано спеціалізований датасет для об'єктів захисного спорядження. На етапі підготовки до тренування моделі до цього набору даних було застосовано процедури аугментації, зокрема віддзеркалення, обертання, масштабування та зміну яскравості, що дозволило суттєво підвищити різноманітність навчальних прикладів. Збільшення розміру датасету забезпечило більш збалансоване представлення даних і підвищило узагальнювальну здатність моделі. Отримані в роботі результати підтверджують доцільність і ефективність запропонованого авторами для даної проблеми окремого навчання моделей для сегментації та класифікації зображень. До перспектив подальших розвідок слід віднести розширення датасету, оптимізацію обчислювальної складності моделей і дослідження їх застосування в режимі реального часу для відеоаналітики.*

***Ключові слова:** виявлення об'єктів, модель детекції, сегментація зображень, попереднє навчання моделі, процедури аугментації, донавчання, бінарні маски об'єктів.*

**Вступ.** Актуальність тематики зумовлена стрімким зростанням обсягів візуальних даних, що надходять із систем відеоспостереження, безпілотних платформ, автономних транспортних засобів та інтелектуальних інформаційних систем. Сучасні задачі аналізу зображень і відеопотоків потребують автоматизованих методів обробки, здатних працювати в режимі реального часу з високою точністю та надійністю. Методи глибокого навчання, зокрема нейронні мережі для детектування об'єктів, демонструють суттєву перевагу над класичними алгоритмами комп'ютерного зору в складних умовах освітлення, зашумлення та часткових перекриттів об'єктів. Практична значущість таких підходів полягає у їх широкому застосуванні в системах безпеки, моніторингу навколишнього середовища, медичній діагностиці та робототехніці. Отже, дослідження та вдосконалення методів виявлення об'єктів на основі глибокого навчання є важливим і своєчасним науково-практичним завданням.

**Огляд літератури.** Сучасний стан розвитку технологій штучного інтелекту значно розширює спектр завдань, які можуть бути вирішені за допомогою робототехніки [1], [2]. Найбільш необхідні напрямки автоматизації для галузі БПЛА включають такі завдання, як скорочення часу виконання місій, більш ефективно використання обчислювальних

потужностей та скорочення часу втручання людини в процеси управління БПЛА [3], [4], [5]. Патрулювання важкодоступних або небезпечних територій, пошук, ідентифікація та класифікація знайдених об'єктів на їх поверхні за допомогою традиційних методів – це складний процес з високими вимогами до часу та обчислювальних потужностей, який потребує вдосконалення завдяки впровадженню різних сучасних методів, таких як штучний інтелект [6], [7], [8].

Для сучасних безпілотних літальних апаратів велика різноманітність завдань, таких як: класифікація, спостереження, дослідження та класифікація, перенаправляється на певні автоматизовані підсистеми, що може підвищити продуктивність завдяки додатковим обчислювальним модулям, що залучаються. Організація та принципи роботи подібних систем наведені в [9], [10], [11]. Такий підхід є доцільним та поширеним завдяки наявності на ринку польотних контролерів [12], [13].

Доступні опції передбачають велику різноманітність роз'ємів для зовнішніх пристроїв для різних цілей: обмін даними GPS, фрагментами даних телеметрії та іншими типами повідомлень, визначених через MavLink. Такі дані можна кластеризувати в набори даних для різних цілей: пріоритетне черги завдань та процедури обробки даних [14], [15]. Системи комп'ютерного зору реалізують різні алгоритми машинного навчання та складні методи обробки даних для завдань обробки зображень та локалізації. Складність структури системи комп'ютерного зору може змінюватися залежно від типу завдання та набору використовуваних технологій [16], [17].

Завдання дослідження певних територій та виявлення й ідентифікації певних об'єктів залежить від взаємодії з нейронною мережею, детальна робота, архітектура та навчання якої обговорюються в [20]. Для цієї конкретної нейронної мережі необхідно розробити інструменти для створення бортового журналу польотів та створення звітів про виявлені об'єкти. Для взаємодії з моделлю було обрано API Ultralytics. Крім того, важливо зазначити, що для обробки зображень було використано бібліотеку OpenCV завдяки її здатності легко переходити від обробки тестових даних з медіафайлів до даних камери в режимі реального часу [25].

Робота присвячена розробці та дослідженню методів виявлення об'єктів на зображеннях і у відеопотоці з використанням сучасних технологій глибокого навчання. Основна увага приділяється створенню, навчанню та практичному застосуванню моделей детектування об'єктів на основі нейронних мереж, що забезпечують високу точність і швидкість обробки візуальних даних [18].

**Мета статті** полягає в визначенні об'єктів заданого типу на зображеннях, отриманих із відеокамери, а також розробці моделі детекції, яка зможе ефективно ідентифікувати та локалізувати ці об'єкти в різних умовах освітлення, масштабу та перспективи.

**Матеріали і методи дослідження.** Для досягнення поставленої мети було використано попередньо натренований детектор, проведено його донавчання (fine-tuning) на спеціалізованій вибірці даних і адаптовано модель до конкретних умов задачі [24, 26]. Отримані результати моделювання та навчання підлягають оцінюванню на тестовій вибірці, що дозволяє проаналізувати точність, повноту та швидкодію моделі, а також визначити можливі напрямки її подальшої оптимізації та вдосконалення.

У межах дослідження було застосовано модель YOLOv11s для сегментації зображень, що містять об'єкти захисного спорядження. Проведено порівняльний аналіз якості результатів між підходами з попереднім навчанням моделі та zero-shot learning. Тестування моделей здійснювалося у середовищі Ultralytics із використанням мови програмування Python 3.11.

Для реалізації завдання сегментації зображень було сформовано спеціалізований датасет, що складався із 150 початкових зображень, на яких представлені об'єкти захисного спорядження. На етапі підготовки до тренування моделі до цього набору даних було застосовано процедури аугментації, зокрема віддзеркалення, обертання, масштабування та зміну яскравості, що дозволило суттєво підвищити різноманітність навчальних прикладів.

Донавчений сегментатор на основі моделі YOLO було порівняно з моделлю SegmentAnythinModel (SAM). Архітектури моделей наведені в табл. 1.

Таблиця 1 – Архітектури моделей SAM та YOLO

SAM	YOLOv11s
Backbone: Vision Transformer (ViT-B) Розмір: Base (B) Кількість шарів ViT: 12 Розмір вектору ознак (hidden size): 768 Кількість голів у self-attention: 12 Кількість параметрів: ~63 млн Тип сегментаційного голови: Mask decoder із трансформерною архітектурою	Single-stage, anchor-free детектор з підтримкою сегментації Кількість шарів: 113 Кількість параметрів: 2,868,664 (~2.87 млн) GFLOPs: ~9.7 GFLOPs

Архітектура SAM базується на Vision Transformer (ViT-B) з трансформерним декодером масок, має значно більшу кількість параметрів (~63 млн) і орієнтована на високоточну сегментацію завдяки моделюванню глобальних залежностей. YOLOv11s є одностадійним anchor-free детектором із підтримкою сегментації, який містить суттєво менше параметрів (~2,87 млн) та характеризується низькою обчислювальною складністю (~9,7 GFLOPs). Таким чином, SAM забезпечує вищу гнучкість і якість сегментації ціною значних обчислювальних витрат, тоді як YOLOv11s оптимізований для швидкодії та застосувань у реальному часі.

**Результати обговорення.** В спеціалізованому датасеті для вирішення завдання сегментації розподіл об'єктів на зображеннях по класах має вигляд, наведений на рис. 1.

COLOR	CLASS NAME	COUNT
Orange	gloves	98
Purple	helmet	326
Red	mask	32
Blue	safety_vest	244
Green	suit	19

Рисунок 1 – Розподіл об'єктів за кількістю по зображеннях датасету

Найбільшу кількість прикладів має клас helmet (326), що свідчить про його домінування у навчальній вибірці. Значну представленість також має клас safety\_vest (244), тоді як класи gloves (98) і mask (32) представлені помірно та слабо відповідно. Найменшу кількість зразків зафіксовано для класу suit (19), що вказує на суттєвий дисбаланс даних. Така нерівномірність розподілу класів може впливати на якість навчання моделі та потребує застосування методів балансування або зважування класів. Детальне описання аугментації та розподіл зображень між тренувальним, тестовим та валідаційним датасетами наведено на рис. 2.

Загальний обсяг вибірки становить 390 зображень, що відображено разом із прикладами анованих кадрів. Датасет поділено на навчальну, валідаційну та тестову підвибірки у співвідношенні 92 %, 6 % та 2 % відповідно. Навчальна вибірка містить 360 зображень і використовується для безпосереднього налаштування параметрів моделі. Валідаційна вибірка складається з 23 зображень і призначена для контролю якості навчання та підбору гіперпараметрів. Тестова вибірка включає 7 зображень і застосовується для остаточної оцінки узагальнювальної здатності моделі.

На рис. 3 відображено динаміку якості навчання моделі в процесі тренування за показниками Validation Mean IoU та функції втрат.

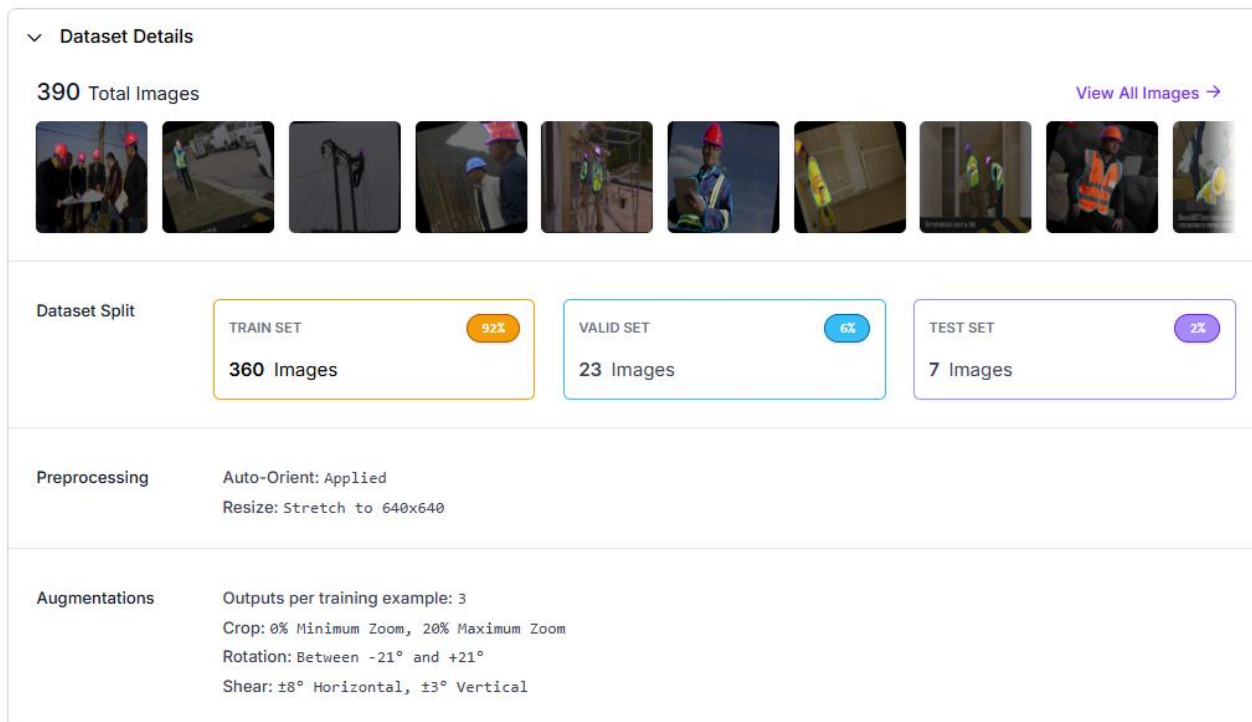


Рисунок 2 – Характеристика кроків аугментації даних та розподіл зображень між розділами датасету

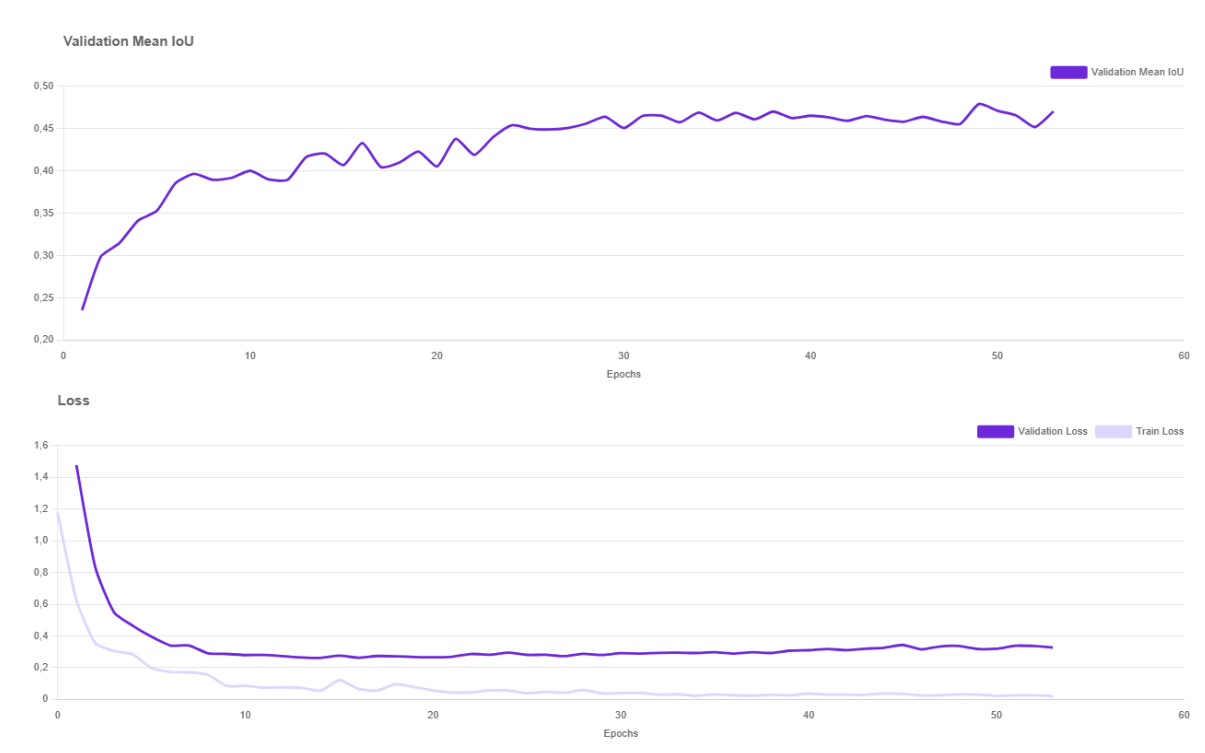


Рисунок 3 – Функції оцінки якості створеної моделі

Значення Validation Mean IoU демонструє стале зростання на початкових епохах із подальшим виходом на плато на рівні приблизно 0,46–0,48, що свідчить про досягнення моделлю стабільної якості сегментації. Крива функції втрат для навчальної вибірки різко зменшується на перших епохах і надалі повільно спадає, що вказує на ефективну оптимізацію параметрів моделі. Водночас значення Validation Loss зменшується до певного мінімуму, після

чого спостерігаються незначне поступове зростання, що може свідчити про необхідність передчасної зупинки навчання. Така поведінка кривих свідчить про відсутність суттєвого перенавчання та коректну узагальнювальну здатність моделі на валідаційних даних.

Після збалансованого представлення даних і підвищення узагальнювальної здатності моделі, були оброблені зображення із сформованого датасету, зокрема деякі подано на рис. 4.



Рисунок 4 – Приклад зображення із сформованого датасету

На рис. 4.а наведено зображення працівника на будівельному майданчику з анотацією елементів засобів індивідуального захисту, що ілюструє приклад детекції захисного шолома, жилета та рукавиць у виробничому середовищі. На рис. 4.б представлено сцену з групою людей у громадському просторі, на якій виконано розмітку обличь та захисних масок, що демонструє здатність датасету охоплювати різні умови освітлення, ракурси та щільність об'єктів. Наведені приклади демонструють репрезентативність сформованого датасету та його придатність для навчання моделей комп'ютерного зору з метою розпізнавання засобів індивідуального захисту в реальних умовах. Ненавчена модель виявилася малоприсадоною для прямого порівняння з донавченою, оскільки попереднє тренування було орієнтоване на розпізнавання базових категорій об'єктів. Для оцінювання ефективності роботи моделі в межах створеного датасету було проаналізовано графік зміни метрики IoU (Intersection over Union) протягом процесу навчання, що дало змогу відстежити динаміку покращення якості сегментації. Оскільки донавчання виконувалося у віддаленому середовищі, застосовувалися рекомендовані параметри, визначені розробниками сервісу [25]. Серед них ключову роль для задачі сегментації відіграють такі гіперпараметри: оптимізатор Stochastic Gradient Descent, швидкість навчання (learning rate) – 0.01, коефіцієнт моменту (momentum) – 0.937 та регуляризаційний параметр weight decay – 0.0005, які забезпечують стабільність і збіжність процесу оптимізації моделі.

Функція втрат у моделі сегментації формується як поєднання трьох складових компонентів. Box loss реалізовано у вигляді CIoU Loss (Complete IoU), який відповідає за точність регресії обмежувальних прямокутників. Classification loss базується на Binary Cross-Entropy (BCE) Loss і використовується для класифікації об'єктів за їх типами. Mask loss також побудовано на BCE Loss, що забезпечує коректну бінаризацію масок об'єктів на зображенні. Додатково для підвищення стабільності та точності сегментації застосовувався Dice loss, який покращує збалансованість між передбаченими та реальними областями об'єктів.

Zero-shot модель була застосована для розв'язання задачі сегментації зображень з метою виявлення елементів захисного будівельного спорядження, таких як жилети, маски та рукавиці. Робота SAM ґрунтується на принципі promptable segmentation, тобто модель отримує підказку (prompt) від користувача і виконує точну сегментацію обраного об'єкта на зображенні.

Архітектурно SAM побудована на Vision Transformer (ViT), який відповідає за витягнення ознак, та масковому предикторі, що генерує бінарні маски об'єктів. Результати сегментації, отримані за допомогою SAM, характеризуються високою точністю відтворення контурів і форм об'єктів, а також універсальністю — модель ефективно працює з будь-якими типами об'єктів без потреби у додатковому донавчанні.

Результати роботи моделі zero-shot підходу за наперед заданими точками та порівняння з YOLO наведені на рис. 5, лівий та правий стовбці відповідно.

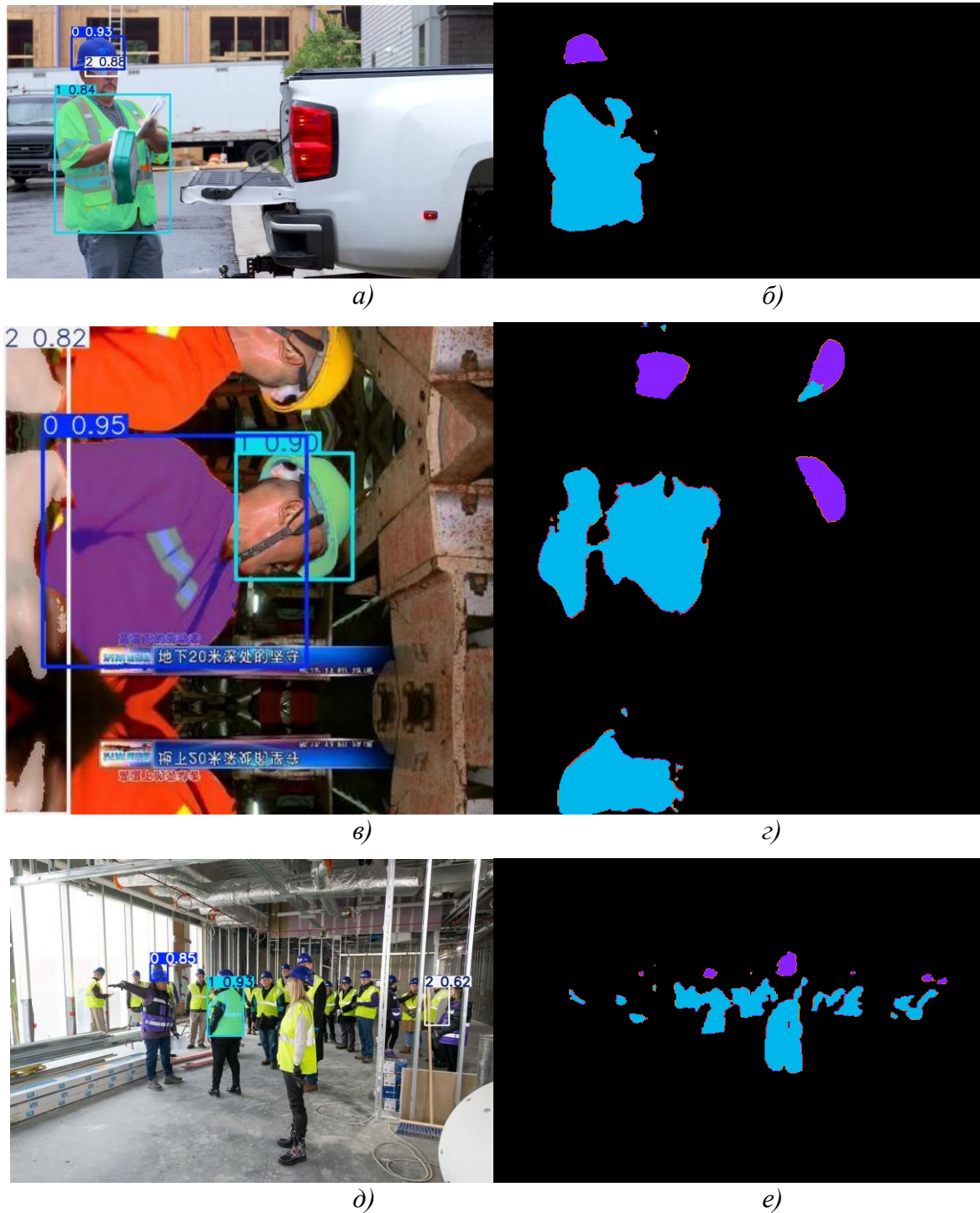


Рисунок 5 – Результати роботи моделі zero-shot підходу та порівняння з YOLO

Лівий стовбець (рис.5, а, в, д) ілюструє детекцію об’єктів із використанням обмежувальних рамок та ймовірнісних оцінок, що дозволяє ідентифікувати наявність засобів індивідуального захисту та локалізувати їх у межах зображення. Другий стовбець (рис.5, б, г, е) відображає піксельну сегментацію, де об’єкти класифіковано на рівні кожного пікселя, що забезпечує більш точне відокремлення форми людини та елементів екіпірування від фону. На відміну від підходу з рамками, сегментація дозволяє коректно враховувати складні контури та часткові перекриття

об'єктів. Водночас детекція з обмежувальними рамками є обчислювально простішою та більш придатною для застосувань у режимі реального часу.

Під час навчання моделі було застосовано спеціальний параметр, характерний для задач сегментації – `mask_ratio = 4`, який визначає ступінь наближення форми сегментованої області до графічних примітивів. У результаті значення метрики IoU (перетину з розміченими даними) досягло приблизно 40%, що свідчить про задовільну точність моделі для поставленого завдання.

У процесі попередньої обробки даних застосовано автоматичну орієнтацію зображень та масштабування до розміру  $640 \times 640$  пікселів зі збереженням пропорцій шляхом розтягування. Для підвищення різноманітності навчальних даних використано методи аугментації, які генерують по три вихідні зразки на одне навчальне зображення. Зокрема, реалізовано випадкове кадрування, обертання в діапазоні від  $-21^\circ$  до  $+21^\circ$  та зсуви за горизонталлю і вертикаллю, що сприяє підвищенню стійкості моделі до змін масштабу та положення об'єктів.

Порівняння швидкостей роботи моделей SAM та YOLO демонструють суттєву різницю у швидкості обробки між моделлю сегментації та моделлю детекції об'єктів. Для сегментації зображень розміром  $1024 \times 1024$  час інференсу становить приблизно 5–6,3 с на одне зображення у разі повної сегментації зображення та 120 мс у разі сегментації за наперед визначеними точками, що є обчислювально затратним і значно перевищує час обробки зображення моделлю YOLO з додатковими вимогами до знаходження точок, що відповідають приблизному знаходженню об'єкта. Натомість для детекції об'єктів на зображеннях меншого розміру ( $384 \times 640$  –  $640 \times 640$ ) час інференсу коливається в межах 43–88 мс, що на два порядки швидше. Попередня та післяобробка в обох випадках займають незначну частку загального часу й не є критичними для продуктивності. Таким чином, сегментація забезпечує детальніший результат ціною значного зниження швидкодії, тоді як детекція є суттєво ефективнішою з точки зору часу обробки. Отримані результати свідчать, що для задач реального часу доцільніше застосовувати детекційні моделі, тоді як сегментаційні підходи більше підходять для офлайн-аналізу. Результати сегментації демонструють високу точність країв і об'єктів різної форми.

**Висновки.** Було сформовано спеціалізований датасет для сегментації зображень об'єктів захисного спорядження, що забезпечив якісну основу для навчання моделей комп'ютерного зору. Застосування процедур аугментації, таких як віддзеркалення, обертання, масштабування та зміна яскравості, дозволило суттєво розширити обсяг і різноманітність даних, підвищивши їх репрезентативність. Детально порівняні параметри, швидкості та результати роботи моделей SAM та YOLO. Отримані результати свідчать, що збільшення обсягу датасету позитивно вплинуло на збалансованість даних і узагальнювальну здатність моделей. Проведене порівняння підтвердило ефективність використання підходу окремого навчання моделей для задач сегментації та класифікації. Таким чином, запропонований підхід може бути використаний як ефективне рішення для автоматизованої обробки зображень у завданнях виявлення об'єктів на зображеннях і у відеопотоці.

До перспектив подальших розвідок слід віднести розширення датасету, оптимізацію обчислювальної складності моделей і дослідження їх застосування в режимі реального часу для відеоаналітики.

### Список використаних джерел

1. Schunfelder, P., Stebel, F., Andreou, N., & Kunig, M. (2024). Deep learning-based text detection and recognition on architectural floor plans. *Automation in Construction*, 157, Article 105156. <https://doi.org/10.1016/j.autcon.2023.105156>.
2. Giakoumoglou, N., Pechlivani, E. M., & Tzovaras, D. (2023). Generate-paste-blend-detect: Synthetic dataset for object detection in the agriculture domain. *Smart Agricultural Technology*, 5, Article 100258. <https://doi.org/10.1016/j.atech.2023.100258>.
3. Ashourpour, M., Azizpour, G., & Johansen, K. (2024). Real-time defect and object detection in assembly line: A case for in-line quality inspection. In *Lecture Notes in Mechanical Engineering* (pp. 99–106). Springer. [https://doi.org/10.1007/978-3-031-38241-3\\_12](https://doi.org/10.1007/978-3-031-38241-3_12).

4. Azevedo, P., & Santos, V. (2024). Comparative analysis of multiple YOLO-based target detectors and trackers for ADAS in edge devices. *Robotics and Autonomous Systems*, 171, Article 104558. <https://doi.org/10.1016/j.robot.2023.104558>.
5. Sanjai Siddharthan, M., Aravind, S., & Sountharajan, S. (2024). Real-time road hazard classification using object detection with deep learning. In *Lecture Notes in Networks and Systems* (Vol. 789, pp. 479–492). Springer. [https://doi.org/10.1007/978-981-99-6586-1\\_33](https://doi.org/10.1007/978-981-99-6586-1_33).
6. Wei, Z., Zhang, Y., Wang, X., Zhou, J., Dou, F., & Xia, Y. (2024). A YOLOv8-based approach for steel plate surface defect detection. *Metallurgija*, 63(1), 28–30.
7. Wu, F., Zhang, Y., Wang, L., Hu, Q., Fan, S., & Cai, W. (2023). A deep learning-based lightweight model for the detection of marine fishes. *Journal of Marine Science and Engineering*, 11(11), Article 2156. <https://doi.org/10.3390/jmse11112156>.
8. Zhang, G., Tang, Y., Tang, H., Li, W., & Wang, L. (2023). A global lightweight deep learning model for express package detection. *Journal of Intelligent & Fuzzy Systems*, 45(6), 12013–12025. <https://doi.org/10.3233/JIFS-232874>.
9. Wang, J., Dai, H., Chen, T., Liu, H., Zhang, X., Zhong, Q., & Lu, R. (2023). Toward surface defect detection in electronics manufacturing by an accurate and lightweight YOLO-style object detector. *Scientific Reports*, 13, Article 33804. <https://doi.org/10.1038/s41598-023-33804-w>.
10. Li, A., Zhang, Z., Sun, S., Feng, M., & Wu, C. (2023). MultiNet-GS: Structured road perception model based on multi-task convolutional neural network. *Electronics*, 12(19), Article 3994. <https://doi.org/10.3390/electronics12193994>.
11. Han, L., Ma, C., Liu, Y., Jia, J., & Sun, J. (2023). SC-YOLOv8: A security check model for the inspection of prohibited items in X-ray images. *Electronics*, 12(20), Article 4208. <https://doi.org/10.3390/electronics12204208>.
12. Mao, J., Wang, L., Wang, N., Hu, Y., & Sheng, W. (2023). A novel method of human identification based on dental impression image. *Pattern Recognition*, 144, Article 109864. <https://doi.org/10.1016/j.patcog.2023.109864>.
13. Kara, E., Zhang, G., Williams, J. J., Ferrandez-Quinto, G., Rhoden, L. J., Kim, M., Kutz, J. N., & Rahman, A. (2023). Deep learning based object tracking in walking droplet and granular intruder experiments. *Journal of Real-Time Image Processing*, 20, 269–311. <https://doi.org/10.1007/s11554-023-01341-4>.
14. Zhou, S., Zhong, M., Chai, X., Zhang, N., Zhang, Y., Sun, Q., & Sun, T. (2024). Framework of rod-like crops sorting based on multi-object oriented detection and analysis. *Computers and Electronics in Agriculture*, 216, Article 108516. <https://doi.org/10.1016/j.compag.2023.108516>.
15. Shan, P., Yang, R., Xiao, H., Zhang, L., Liu, Y., Fu, Q., & Zhao, Y. (2023). UAVPNet: A balanced and enhanced UAV object detection and pose recognition network. *Measurement*, 222, Article 113654. <https://doi.org/10.1016/j.measurement.2023.113654>.
16. Talaat, F. M., & ZainEldin, H. (2023). An improved fire detection approach based on YOLOv8 for smart cities. *Neural Computing and Applications*, 35, 20939–20954. <https://doi.org/10.1007/s00521-023-08809-1>.
17. Liu, S., Fan, Q., Zhao, C., & Li, S. (2023). RTAD: A real-time animal object detection model based on a large selective kernel and channel pruning. *Information*, 14(10), Article 535. <https://doi.org/10.3390/info14100535>.
18. Smolii, V. M., Smolii, N. V., Kovalenko, O. Y., & Shvydenko, M. Z. (2025). Channel extractor for UAV PPM signals. *CEUR Workshop Proceedings*, 3917, 226–236. <https://ceur-ws.org/Vol-3917/>.
19. Su, Y., Tan, W., Dong, Y., Xu, W., Huang, P., Zhang, J., & Zhang, D. (2024). Enhancing concealed object detection in active millimeter wave images using wavelet transform. *Signal Processing*, 216, Article 109303. <https://doi.org/10.1016/j.sigpro.2023.109303>.
20. Liu, C., Wang, K., Li, Q., Zhao, F., Zhao, K., & Ma, H. (2024). Powerful-IoU: More straightforward and faster bounding box regression loss with a nonmonotonic focusing mechanism. *Neural Networks*, 170, 276–284. <https://doi.org/10.1016/j.neunet.2023.11.041>.

21. Xu, W., Liu, C., Wang, G., Zhao, Y., Yu, J., Muhammad, A., & Li, D. (2024). Behavioral response of fish under ammonia nitrogen stress based on machine vision. *Engineering Applications of Artificial Intelligence*, 128, Article 107442. <https://doi.org/10.1016/j.engappai.2023.107442>.
22. Dimauro, G., Barbaro, N., Camporeale, M. G., Fiore, V., Gelardi, M., & Scalera, M. (2024). DeepCilia: Automated, deep-learning-based engine for precise ciliary beat frequency estimation. *Biomedical Signal Processing and Control*, 90, Article 105808. <https://doi.org/10.1016/j.bspc.2023.105808>.
23. Zhao, X., & Song, Y. (2023). Improved ship detection with YOLOv8 enhanced with MobileViT and GSConv. *Electronics*, 12(22), Article 4666. <https://doi.org/10.3390/electronics12224666>.
24. Smolii, V. M., Smolii, N. V., & Sayapin, S. P. (2024). Search and classification of objects in the zone of reservoirs and coastal zones. *CEUR Workshop Proceedings*, 3666, 37–51. <https://ceur-ws.org/Vol-3666/paper04.pdf>.
25. Ultralytics. Train settings. In *Ultralytics Docs*. <https://docs.ultralytics.com/modes/train/#train-settings>.
26. Tang, J., Xie, N., Li, K., Liang, Y., & Shen, X. (2024). Trajectory tracking control for fixed-wing UAV based on DDPG. *Journal of Aerospace Engineering*, 37(2), Article 04024011. <https://doi.org/10.1061/JAEEZ.ASENG-5286>.

### Smolij Viktorija

*Doctor of Technical Sciences, Professor, Professor of the Department of Information Systems and Technologies,*

*National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0000-0002-1268-7837>

E-mail: [vmsmolij@nubip.edu.ua](mailto:vmsmolij@nubip.edu.ua)

### Smolij Natan

*Postgraduate Student of the specialty "Information Systems and Technologies",*

*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*

ORCID: <https://orcid.org/0009-0002-3763-6726>

E-mail: [hoibbitizukrainy@gmail.com](mailto:hoibbitizukrainy@gmail.com)

## MACHINE VISION MODULE FOR OBJECT DETECTION IN IMAGES AND VIDEO STREAMS

**Abstract.** *This work addresses the topical issue of developing and applying intelligent computer vision methods for the automated detection and segmentation of protective equipment objects in images and video streams. The aim of the work is to identify objects of a specified type in images captured by a video camera, as well as to develop a detection model capable of effectively identifying and localising these objects under various lighting conditions, scales and perspectives. The article examines the data preparation process, in particular the application of augmentation methods to improve the representativeness of the sample, and performs a comparative analysis of the parameters, performance and results of the SAM and YOLO models. The results of experimental studies are presented, demonstrating the positive impact of increasing the volume and diversity of the dataset on data balance and the generalisation ability of computer vision models. The proposed approaches to training separate models for segmentation and classification tasks have proven their effectiveness in the context of automated image processing. In this work, a specialised dataset of protective equipment items was created to address the image segmentation task. During the model pre-training phase, data augmentation techniques—including mirroring, rotation, scaling and brightness adjustment—were applied to this dataset, which significantly increased the diversity of the training examples. Increasing the size of the dataset ensured a more balanced representation of the data and improved the model's generalisation ability. The results obtained in this work confirm the feasibility and effectiveness of the authors' proposed approach to this problem, namely the separate training of models for image segmentation and classification. Prospects for further research include expanding the dataset, optimising the computational complexity of the models, and investigating their application in real-time for video analytics.*

**Keywords:** *Object Detection, Detection Model, Image Segmentation, Model Pre-Training, Augmentation Procedures, Fine-Tuning, Binary Object Masks.*

UDC 004.93:616-073.7

### Nikolaienko Dmytro

Senior Lecturer, Department of Computer Science,  
National University of Life and Environmental Sciences of Ukraine

ORCID: <https://orcid.org/0009-0008-4817-3951>

E-mail: [d.nikolaenko@nubip.edu.ua](mailto:d.nikolaenko@nubip.edu.ua)

### Li Yulong

PhD student in Computer Science,  
National University of Life and Environmental Sciences of Ukraine

ORCID: <https://orcid.org/0009-0004-2039-6919>

E-mail: [liyulong@dgut.edu.cn](mailto:liyulong@dgut.edu.cn)

## SEMANTIC SEGMENTATION OF FETAL BRAIN ULTRASOUND IMAGES BASED ON A GENERAL FULLY CONVOLUTIONAL DISCRIMINATOR

**Abstract.** *The fetal central nervous system (CNS) is one of the most common fetal congenital diseases in the world. It is of great significance to use deep learning methods to provide doctors with reliable auxiliary diagnosis methods. The area outside the skull halo in fetal brain ultrasound images contains a lot of irrelevant information and has fuzzy boundaries, which is not conducive to the classification or recognition tasks of ultrasound images. This paper aims to study the effect of generative adversarial networks based on universal fully convolutional discriminators on the automatic segmentation results of skull halo in fetal brain ultrasound images. This paper proposes a method for automatic segmentation of skull halo in fetal brain ultrasound images using a generative adversarial network based on a universal fully convolutional discriminator. Inspired by the concept of generative adversarial networks, a new semantic segmentation network based on a universal discriminator is constructed. To verify the universality of the discriminator, the semantic segmentation network uses both Deeplab\_v2 and Attention U-net networks as generators to generate probability maps of segmentation results. A universal fully convolutional discriminator is also designed to let it learn to distinguish whether the probability map input to the discriminator network is real data or segmentation results. Experimental results on the dataset of automatic measurement of fetal head circumference in ultrasound imaging demonstrate the effectiveness of the algorithm. Compared with the baseline of Deeplab\_v2, the segmentation accuracy is significantly improved, and the Attention U-net also has a similar improvement. Generative adversarial network based on universal fully convolutional discriminator can effectively improve the accuracy of automatic segmentation of skull halo in fetal brain ultrasound images.*

**Keywords:** *Fetal Central Nervous System, Generative Adversarial Networks, Deeplab\_V2, Attention U-Net.*

**Introduction.** The fetal central nervous system (CNS) is one of the most common congenital disorders in fetuses worldwide. With the continuous advancement of ultrasound technology, ultrasound examination of the fetal brain, known for its non-invasive nature, real-time capabilities, and cost-effectiveness, has become the preferred imaging modality for routine prenatal check-ups. However, the development of the fetal CNS is a highly complex process, and the pathological features of the fetal brain are particularly subtle and difficult to discern. Clinically, conducting fetal ultrasound examinations requires a comprehensive knowledge base and extensive practical experience. Experienced doctors can efficiently use ultrasound for diagnosis; however, in underdeveloped regions, there is a lack of experienced specialists and advanced ultrasound imaging equipment.

Therefore, it is highly significant to use deep learning methods to provide doctors with a reliable auxiliary diagnostic tool.

**Literature Review.** In recent years, deep learning (DL), particularly convolutional neural networks (CNNs), has rapidly become a research hotspot in medical image analysis. In 2015, Long et al. [1] introduced the Fully Convolutional Network (FCN) at CVPR 2015, achieving a major breakthrough in image semantic segmentation through end-to-end learning. This has led to increased research and improvements in the field. Due to the high performance of CNNs in various image processing tasks [2], there has been a growing body of research and achievements in fetal ultrasound image processing within the deep learning domain. Yu Z et al. [3] proposed a deep learning-based method for recognizing standard fetal ultrasound planes; Baumgartner et al. [4] used deep learning

methods to achieve real-time detection of standard planes to aid doctors as a clinical diagnostic tool. Currently, utilizing deep learning methods for fetal disease diagnosis will become the next research focus and challenge. Ye Hai et al. [5] proposed a fetal brain ultrasound image segmentation algorithm based on a fully convolutional network. Cerrolaza et al. [6] discussed the application of fully convolutional networks in skull segmentation of fetal 3D ultrasound images. Zahra Sobhaninia et al. [7] presented a multi-scale and deep neural network for estimating fetal biometric parameters. This network outperforms single-task networks in segmentation and ellipse optimization tasks.

However, the above methods insufficiently utilize boundary information in fetal brain images, and segmentation accuracy needs further improvement. To address these issues, this paper proposes a semantic segmentation network for fetal brain ultrasound images based on a generic fully convolutional discriminator. This network uses a discriminator to optimize local features of the segmentation network, fully utilizing boundary information and reducing data set requirements, effectively addressing the issue of limited medical image datasets. In this paper, the segmentation network is used as the generator in the GAN [8] framework. Unlike traditional generators that train to generate images from noise vectors, our segmentation network outputs a probability map of semantic labels for a given input image. In the discriminator network, we use a generic fully convolutional network. Experimental results on an automatic measurement dataset of fetal head circumference in ultrasound imaging have demonstrated the effectiveness and accuracy of the proposed semantic segmentation framework based on a generic fully convolutional discriminator GAN.

**Purpose.** This paper aims to study the effect of generative adversarial networks based on universal fully convolutional discriminators on the automatic segmentation results of skull halo in fetal brain ultrasound images.

**Materials and Methods.** This paper draws on the idea of generative adversarial networks and designs a generalized semantic segmentation network with a fully convolutional discriminator. The overall network structure is shown in Figure 1. The entire network structure consists of two modules: a semantic segmentation network and a discriminant network. Through this overall network structure, we can understand how this paper uses generative adversarial networks for training and obtains semantic segmentation results through generative adversarial learning.

First, drawing on the idea of generative adversarial networks, this paper uses semantic segmentation networks as generative networks. To verify the versatility of the designed discriminator, this paper selects Deeplab\_v2 [9] and Attention U-net [10], 2 networks as segmentation networks for training. At the same time, using the idea of generative adversarial learning, a discriminator is designed to conduct adversarial learning on the segmentation network, and the parameters of the segmentation network are continuously optimized, so as to achieve the purpose of optimizing the segmentation results. The advantage of this design is that it does not need to increase the network depth of the segmentation network, but can improve the segmentation accuracy, and does not need to add various post-processing methods like other segmentation networks to improve the segmentation accuracy.

This paper uses two segmentation networks, DeepLab-v2 and Attention U-net, to conduct experiments to verify the generalization ability of the designed discriminator.

The specific operations are as follows:

*(1) Using DeepLab\_v2 as the segmentation network*

The DeepLab\_v2 framework uses the ResNet-101[11] network. The pre-trained model is a model pre-trained using the MS COCO dataset [12]. However, the conditional random fields (CRFs) proposed in DeepLab\_v2 are not used to optimize the segmentation results. Instead, the last classification layer is deleted in this paper, and the last step size of the two convolutional layers is changed from 2 to 1, so that the resolution of the output feature map is actually 1/8 of the input image size. Finally, the upsampling layer and Softmax output are used to match the size of the input image. In other words, given an image of size  $H \times W \times 3$ , the input of the segmentation network can output a probability map of size  $H \times W \times C$ , where  $C$  is the number of semantic segmentation categories.

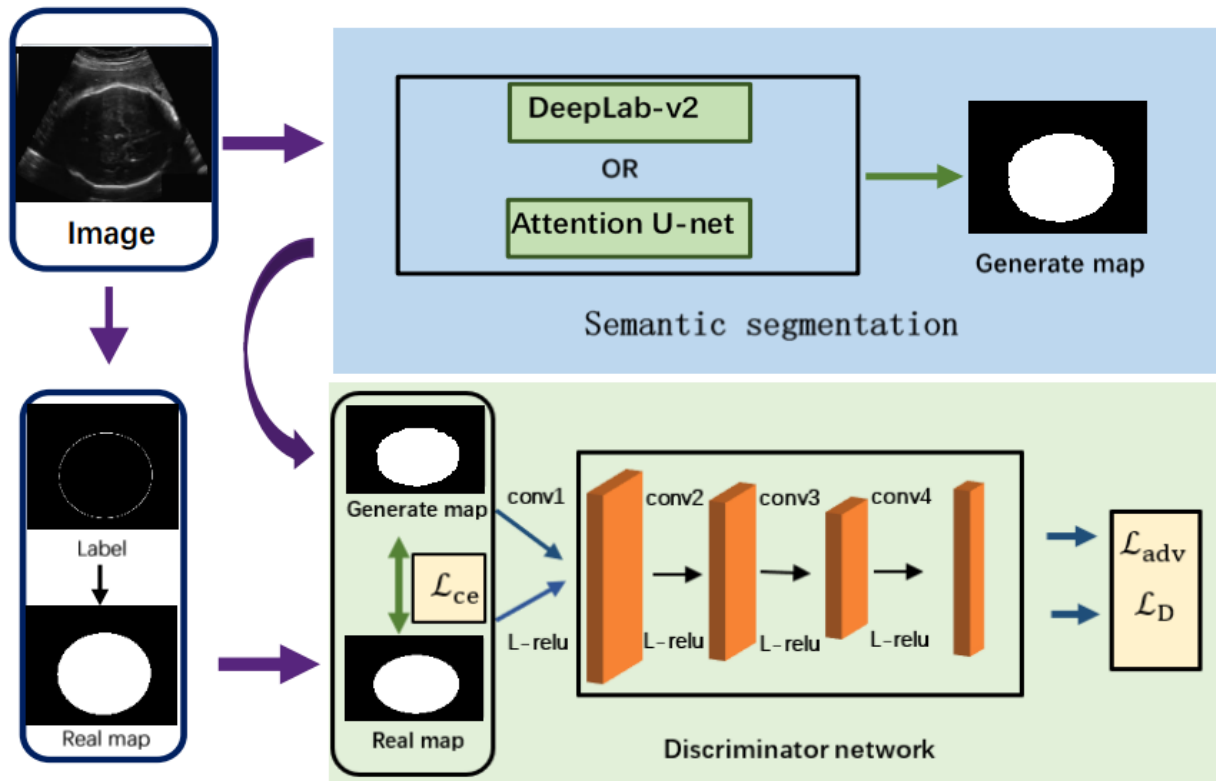


Figure 1 – An overview of the proposed semantic segmentation network based on a generative adversarial network with a generic full convolutional discriminator

In deeplab\_v2, Hollow Convolution and Atrous spatial pyramid pooling are used to expand the perceptual field of view, thereby improving the segmentation accuracy of the segmentation network.

(2) Using U-net Attention as the segmentation network

The Attention U-Net model is improved on the basis of the U-Net[13] model and also adopts a U-shaped structure. The difference between the two models is that Attention U-Net adds an attention module based on U-Net, and this attention module is used for skip connection. The original U-Net simply concatenates the features of the same layer of the downsampling layer directly to the upsampling layer, while the improved Attention U-Net uses the Attention module to process the feature map of the same layer of the downsampling layer and the feature map of the upper layer of the upsampling layer respectively, and then concatenates them with the feature map of the upsampling layer.

The discriminative network is based on FCN. The discriminative network consists of four convolutional layers with 4×4 kernels. Each convolutional layer is followed by a Leaky-ReLU [14] layer with a parameter of 0.2. The expression of Leaky-ReLU is:

$$y_i = \begin{cases} x_i & \text{if } x_i \geq 0 \\ \frac{x_i}{\alpha_i} & \text{if } x_i < 0 \end{cases} \quad (1)$$

where  $\alpha_i$  is a fixed parameter in the interval  $(1, +\infty)$ .

Finally, an upsampling layer is added to the last layer to scale the output to the large of the input mapping, thus constituting a fully convolved discriminator network, which allows the input image to be of arbitrary size.

This is done as follows, the discriminator network takes the segmentation probability map or the real data probability map generated by the segmentation network as input and outputs a spatial probability map of size  $H \times W \times 1$ . The discriminator outputs each pixel  $p$  of the map, when  $p=1$ , it

means that the pixel is from the real data label, when  $p=0$ , it means that the pixel is from the segmentation network.

In this paper, we are borrowing the idea of generative adversarial network to implement, for the generative network in GAN, we replace it with a segmentation network, in designing a fully convolutional discriminative network to optimize the segmentation network.

Given an input image  $X_n$  of size  $H \times W \times 3$ , denote the segmentation network by  $S(\bullet)$  and  $S(X_n)$  denotes the predictive probability map of size  $H \times W \times C$ , where  $C$  is the number of categories. We denote the full convolutional discriminator by  $D(\bullet)$ , which uses a probability map of input size  $H \times W \times C$ , where the discriminator network has two possible inputs: segmentation prediction  $S(X_n)$  or real data vector  $Y_n$ . and outputs a predicted probability map of size  $H \times W \times 1$  to discriminate whether the input probability map is from the segmentation network or from the real data.

Discriminative network: To train the discriminative network, the loss of spatial cross-entropy of the two classes is  $\mathcal{L}_D$  is minimized:

$$\mathcal{L}_D = -\sum_{h,w}(1-y_n) \log(1 - D(S(X_n))^{(h,w)}) + y_n \log(D(Y_n)^{(h,w)}). \quad (2)$$

Segmentation networks: we train segmentation networks by minimizing a multi-task loss function:

$$\mathcal{L}_{seg} = \mathcal{L}_{ce} + \lambda_{adv}\mathcal{L}_{adv}. \quad (3)$$

Among them  $\mathcal{L}_{ce}$  and  $\mathcal{L}_{adv}$  denote spatial multi-class cross entropy loss, adversarial loss, respectively.  $\lambda_{adv}$  are the weights of the adversarial loss function.

Given an input image, which has real data at  $Y_n$  and predictions at  $S(X_n)$ , the cross-entropy loss can be obtained:

$$\mathcal{L}_{ce} = -\sum_{h,w} \sum_{c \in C} Y_n^{(h,w,c)} \log(S(X_n)^{(h,w,c)}). \quad (4)$$

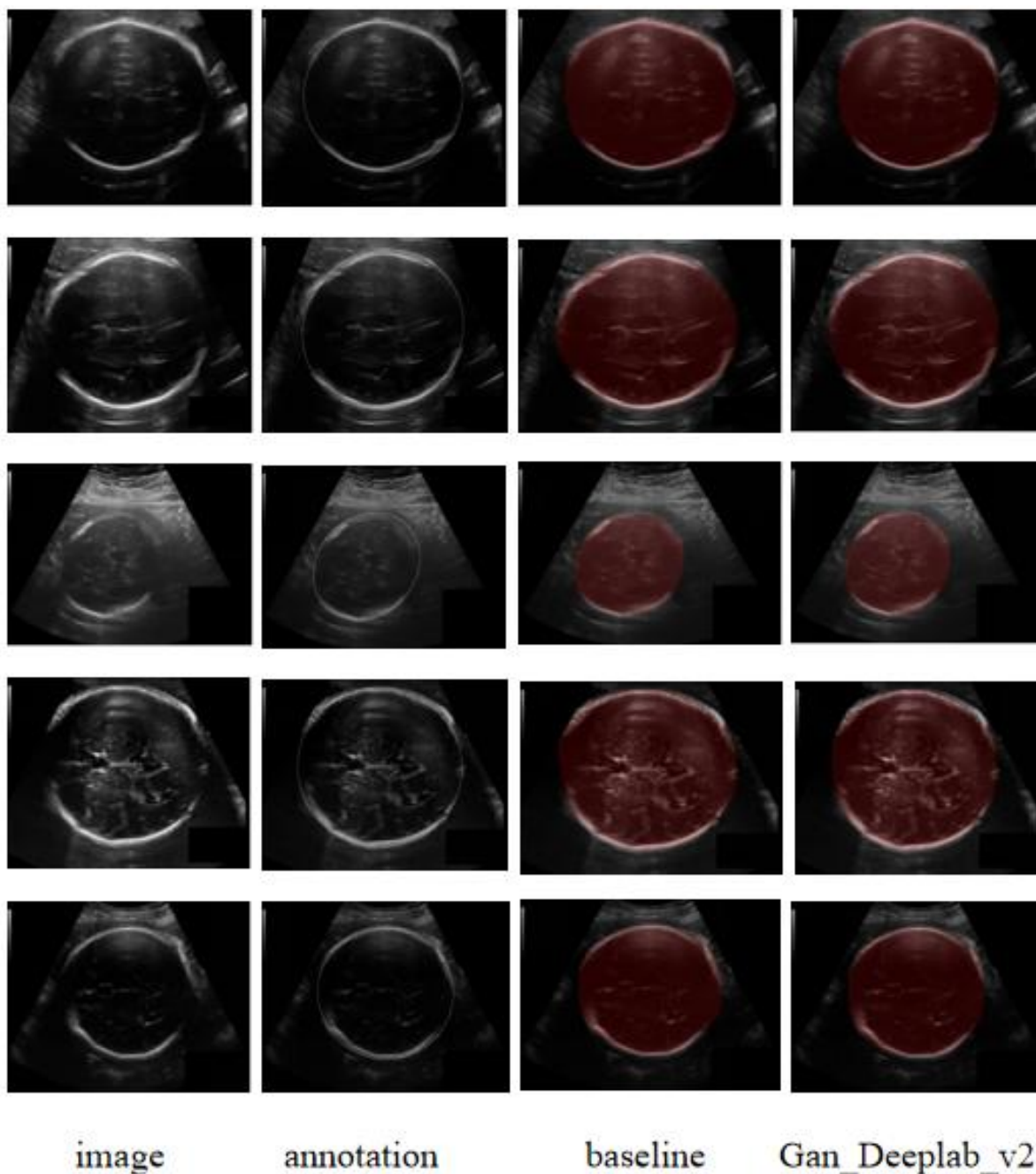
We do this by means of a loss  $\mathcal{L}_{adv}$  of an adversarial learning process to give a fully convolutional discriminative network  $D(\bullet)$ :

$$\mathcal{L}_{adv} = -\sum_{h,w} \log(D(S(X_n))^{(h,w)}). \quad (5)$$

Using this loss, we train the segmentation network to maximize the probability of the predictions produced in the segmentation network to deceive the discriminator.

At the same time, the experiment verifies the effectiveness of the algorithm according to the following results. As shown in Figure 2, the segmentation results obtained from the experiments conducted on Deeplab\_v2 network based on and not based on full convolutional discriminator with fetal head circumference dataset. Where the first column is the fetal head circumference image, the second column is the segmented image manually labeled on the fetal head circumference image, the third column is the segmented image obtained by training the Deeplab\_v2 network without full convolutional discriminator based, and the fourth column is the segmented image obtained by training the Deeplab\_v2 network based on the full convolutional discriminator.

As can be seen from Figure 2, when the discriminator is not used, although the results of fetal head circumference segmentation are very good, but for and manually labeled, its edge is still lacking. But when the discriminator is used, the segmentation results, it can be clearly seen that the edge is very close to the manual labeling, from which it can also be seen that the connection of a full convolutional discriminator can optimize the segmentation boundaries, for the edge of the information can be better utilized, and this discriminator structure for the segmentation of fetal ultrasound images is very advantageous.



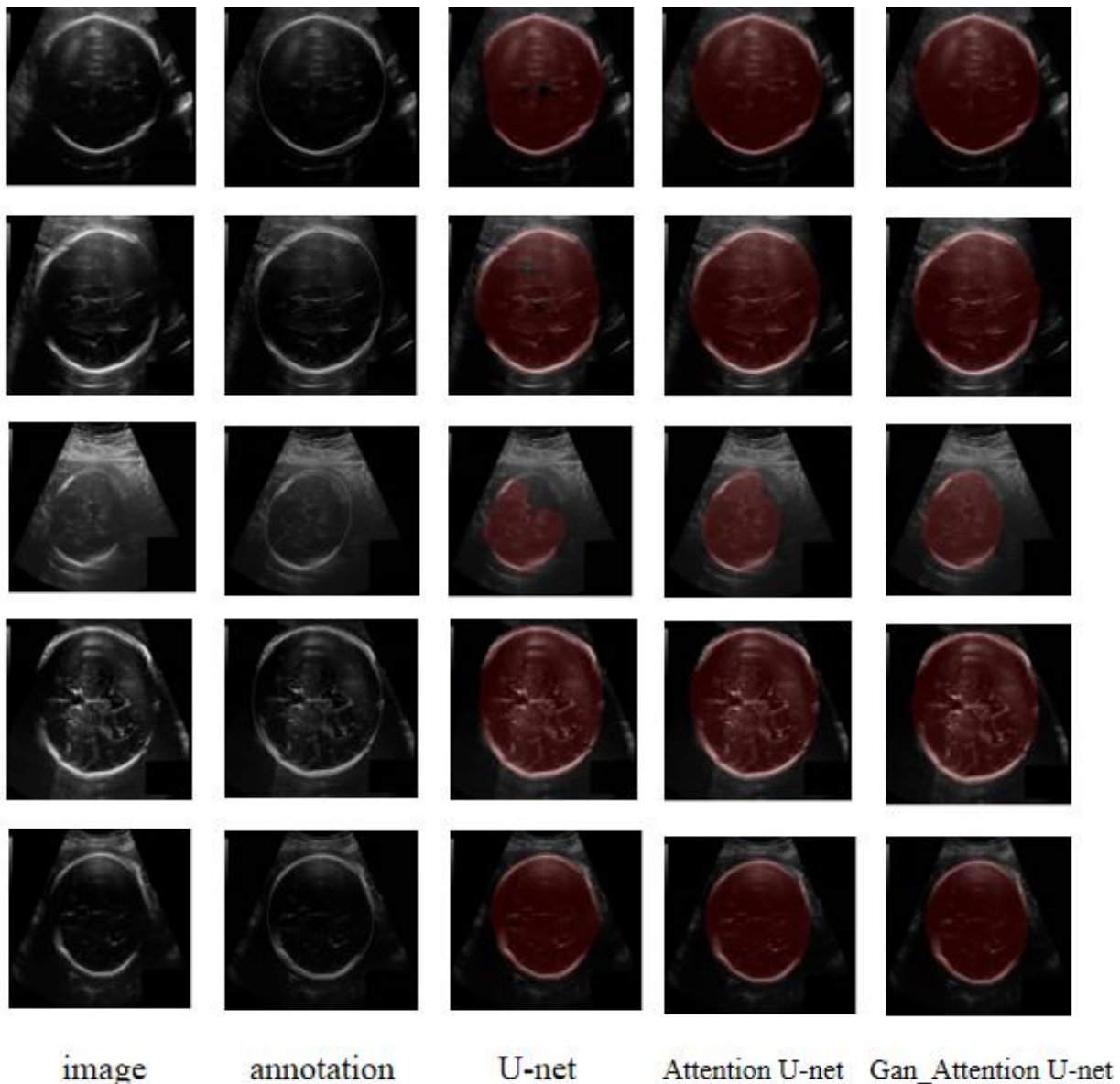
*Figure 2 – Comparison of Deeplab\_v2 network based and not based on full convolutional discriminator under fetal head circumference dataset*

Table 1 shows the comparison of the results of Deeplab\_v2 and Deeplab\_v2's baseline, based on the full convolutional discriminator, with the fetal head circumference dataset. From the data in the table, after using the discriminator, comparing with Deeplab\_v2's baseline, the IOU for the fetal head circumference validation set improves by 3.2% to 94.2%, and the DICE improves by 2.1% to 97.0%. This can be seen, this network for fetal head circumference dataset training and recognition segmentation effect is very good, at the same time, we are based on the idea of generative adversarial network, add the discriminator to optimize the segmentation results of this method, can be very good to improve the segmentation results, for the segmentation of the boundaries of the improvement is greater, the same discriminator can reduce the segmentation of the network for the dataset requirements, so this discriminator is very suitable for fetal ultrasound This discriminator is very suitable for fetal ultrasound images, and this structure is also suitable for other medical images.

*Table 1 – Results derived from fetal head circumference validation set under Deeplab\_v2 network*

<b>Method</b>	<b>IOU (%)</b>	<b>Dice (%)</b>
Baseline	91.0	94.9
GAN_DeepLab_v2	94.2	97.0

As shown in Figure 3, the segmentation results obtained from the experiments conducted on Attention U-net network based and not based on full convolutional discriminator with fetal head circumference dataset. Wherein the first column is the fetal head circumference image, the second column is the segmentation image manually labeled on the fetal head circumference image, the third column is the segmentation image obtained by training the U-net network, the fourth column is the segmentation image obtained by training the Attention U-net network not based on the full convolutional discriminator, and the fifth column is the segmentation image obtained by training the Attention U-net network based on the full convolutional discriminator.



*Figure 3 – Comparison of Attention U-net network with and without full convolutional discriminator based on fetal head circumference dataset*

As can be seen from Fig.3, the segmentation results obtained by using U-net directly are not good, and some of them have problems with poor class recognition and poor results of edge segmentation. By adding an attention mechanism, the segmentation results are directly greatly improved, but there are still some edges of the image of fetal head circumference where the segmentation is not very good. After adding a discriminator to the network, the segmentation results can be clearly seen that the corresponding segmentation boundaries have been greatly improved, making them closer to the manually labeled segmented images.

Table 2 shows the comparison of the results of U-net family of networks under fetal head circumference dataset. From the data in the table, it can be seen that after using an attention mechanism, comparing to U-net, the IOU of the fetal head circumference validation set is improved by 10% to 89.2% and the DICE is improved by 7% to 94% . After continuing to add a full convolutional discriminator, comparing to U-net, the IOU of the fetal head circumference validation set improves by 11% to 90.2%, and the DICE improves by 7.6% to 94.6% ; comparing to Attention U-net, the IOU of the fetal head circumference validation set improves by 1%, and the DICE improves by 0.6%. This can be seen that adding a full convolutional discriminator can continue to increase the segmentation accuracy even further, and at the same time can optimize the segmentation edges to be closer to the results of manual segmentation. This can be a good solution to the problem of blurred boundaries in fetal ultrasound images.

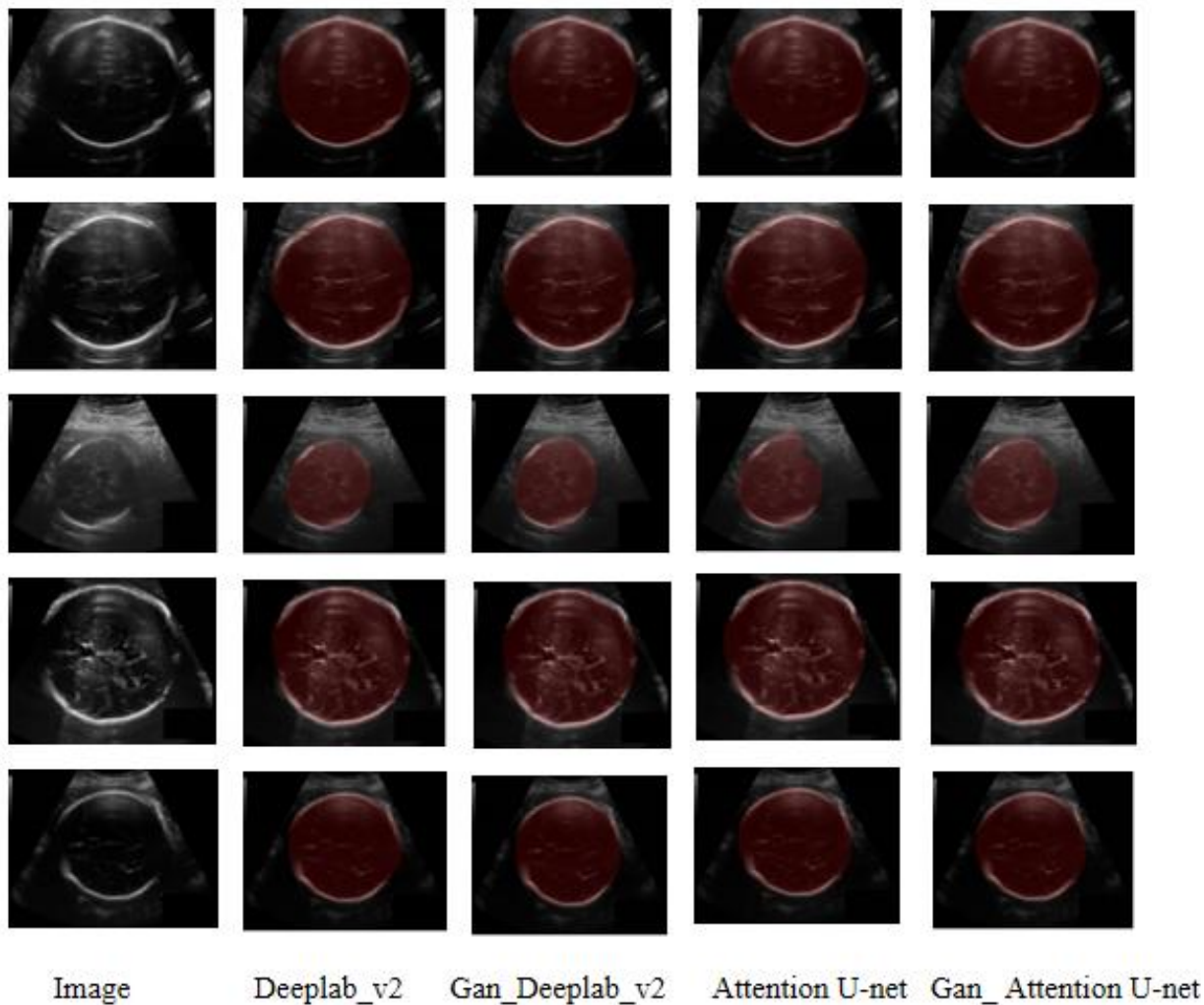
*Table 2 – Results derived from fetal head circumference validation set under U-net series network*

<b>Method</b>	<b>IOU (%)</b>	<b>Dice (%)</b>
U-net	79.2	87.0
Attention U-net	89.2	94.0
GAN Attention U-net	90.2	94.6

As shown in Figure 4, the segmentation results obtained from experiments conducted with Deeplab\_v2 and Attention U-net networks, under the fetal head circumference dataset. Where the first column is the fetal head circumference image, the second column is the segmentation image obtained by training the Deeplab\_v2 network without full convolutional discriminator, the third column is the segmentation image obtained by training the Deeplab\_v2 network with full convolutional discriminator, the fourth column is the segmentation image obtained by training the Attention U-net network without full convolutional discriminator, and the fifth column is the segmentation image obtained by training the Attention U-net network with full convolutional discriminator. Attention U-net network training with full convolutional discriminator.

From Figure 4 and combining with Table 2, Table 3, it can be seen that Deeplab\_v2 and Attention U-net networks after using the discriminator, the IOU of Deeplab\_v2 is improved by 3.2% and the DICE is improved by 2.1%; Attention U-net network's IOU is improved by 1.0% and the DICE is improved by 0.6%. It can be seen that the use of discriminators for segmentation networks will have different degrees of improvement; at the same time, the discriminators are significantly better than Attention U-net for Deeplab\_v2, which can also be concluded that for the deeper the semantic segmentation network, the discriminators play a better role in the semantic segmentation network, and the segmentation effect will be improved more. By adding a full convolutional discriminator, this can improve the segmentation results of fetal ultrasound images by using a deeper network when processing fetal ultrasound images.

**Conclusions.** This paper presents a semantic segmentation network for fetal brain ultrasound images based on a generalized fully convolutional discriminator. The proposed method uses the scheme of Generative Adversarial Networks (GANs), which consists of a segmentation network and a discriminator. In this paper then Deeplab\_v2 and Attention U-net are used as the segmentation network to verify the generalization of this full convolutional discriminator.



*Figure 4 – Comparison of Deeplab\_v2 and Attention U-net network under fetal head circumference dataset*

The discriminator uses a fully convolutional network to distinguish between the input map which is a probability map of the real data and the probability map of the segmentation result of the segmentation network. Through the generative confrontation between this discriminator and the segmentation network, the discriminator continuously optimizes the model parameters of the segmentation network, so as to improve the segmentation accuracy of the segmentation network. And in this process of adversarial learning, the network depth of the segmentation network does not increase. A large number of experiments were conducted on the fetal head circumference data set to verify the effectiveness of the algorithm, and also proved that the scheme of adding a fully convolutional discriminator is very suitable for fetal ultrasound images, which can further optimize the edge segmentation of fetal ultrasound images and reduce the data requirements of the segmentation network.

### References

1. Long, J., Shelhamer, E., & Darrell, T. (2015). Fully convolutional networks for semantic segmentation. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 3431–3440). <https://doi.org/10.48550/arXiv.1411.4038>.
2. Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., van der Laak, J. A. W. M., van Ginneken, B., & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, 42, 60–88. <https://doi.org/10.1016/j.media.2017.07.005>.

3. Yu, Z., Ni, D., Chen, S., et al. (2016). Fetal facial standard plane recognition via very deep convolutional networks. In 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 1–4). IEEE. <https://doi.org/10.1109/EMBC.2016.7590780>.
4. Baumgartner, C. F., Kamnitsas, K., Matthew, J., Fletcher, T. P., Smith, S., Koch, L. M., Kainz, B., Rueckert, D., & Glocker, B. (2017). SonoNet: Real-time detection and localization of fetal standard scan planes in freehand ultrasound. *IEEE Transactions on Medical Imaging*, 36(11), 2204–2215. <https://doi.org/10.1109/TMI.2017.2712367>.
5. Ye, H., Feng, K.-P., & Xie, H.-N. (2019). Fetal brain ultrasonic image segmentation algorithm based on fully convolution network. *Modern Computer*, (27), 43–47.
6. Cerrolaza, J. J., Sinclair, M., Matthew, J., et al. (2018). Deep learning with ultrasound physics for fetal skull segmentation. In 2018 IEEE 15th International Symposium on Biomedical Imaging (ISBI 2018) (pp. 564–567). IEEE. <https://doi.org/10.1109/ISBI.2018.8363639>.
7. Sobhaninia, Z., Rafiei, S., Emami, A., Karimi, N., Najarian, K., & Samavi, S. (2019). Fetal ultrasound image segmentation for measuring biometric parameters using multi-task deep learning. In 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 6545–6548). IEEE. <https://doi.org/10.1109/embc.2019.8856981>.
8. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, & K. Q. Weinberger (Eds.), *Advances in Neural Information Processing Systems* (Vol. 27). <https://proceedings.neurips.cc/paper/2014/hash/f033ed80deb0234979a61f95710dbe25-Abstract.html>.
9. Chen, L.-C., Papandreou, G., Kokkinos, I., Murphy, K., & Yuille, A. L. (2018). DeepLab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(4), 834–848. <https://doi.org/10.48550/arXiv.1606.00915>.
10. Oktay, O., Schlemper, J., Folgoc, L. L., Lee, M. C. H., Heinrich, M., Misawa, K., Mori, K., McDonagh, S., Hammerla, N. Y., Kainz, B., Glocker, B., & Rueckert, D. (2018). Attention U-Net: Learning where to look for the pancreas [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.1804.03999>.
11. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 770–778). <https://doi.org/10.48550/arXiv.1512.03385>.
12. Lin, T.-Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., & Zitnick, C. L. (2014). Microsoft COCO: Common objects in context. In D. Fleet, T. Pajdla, B. Schiele, & T. Tuytelaars (Eds.), *Computer Vision – ECCV 2014* (pp. 740–755). Springer. [https://doi.org/10.1007/978-3-319-10602-1\\_48](https://doi.org/10.1007/978-3-319-10602-1_48).
13. Ronneberger, O., Fischer, P., & Brox, T. (2015). U-Net: Convolutional networks for biomedical image segmentation. In N. Navab, J. Hornegger, W. M. Wells, & A. Frangi (Eds.), *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015* (pp. 234–241). Springer. [https://doi.org/10.1007/978-3-319-24574-4\\_28](https://doi.org/10.1007/978-3-319-24574-4_28).
14. Maas, A. L., Hannun, A. Y., & Ng, A. Y. (2013). Rectifier nonlinearities improve neural network acoustic models. In *Proceedings of the 30th International Conference on Machine Learning, Deep Learning Workshop*. [https://ai.stanford.edu/~amaas/papers/relu\\_hybrid\\_icml2013\\_final.pdf](https://ai.stanford.edu/~amaas/papers/relu_hybrid_icml2013_final.pdf).

**Ніколаєнко Дмитро Володимирович**

*старший викладач кафедри комп'ютерних наук,*

*Національний університет біоресурсів і природокористування України*

ORCID: <https://orcid.org/0009-0008-4817-3951>

E-mail: [d.nikolaenko@nubip.edu.ua](mailto:d.nikolaenko@nubip.edu.ua)

**Лі Юйлун***аспірант кафедри комп'ютерних наук,**Національний університет біоресурсів і природокористування України*ORCID: <https://orcid.org/0009-0004-2039-6919>E-mail: [liyulong@dgut.edu.cn](mailto:liyulong@dgut.edu.cn)**СЕМАНТИЧНА СЕГМЕНТАЦІЯ УЛЬТРАЗВУКОВИХ ЗОБРАЖЕНЬ МОЗКУ ПЛОДА НА ОСНОВІ ЗАГАЛЬНОГО ПОВНІСТЮ ЗГОРТКОВОГО ДИСКРИМІНАТОРА**

**Анотація.** Ураження центральної нервової системи (ЦНС) плода є одним з найпоширеніших вроджених захворювань плода у світі. Використання методів глибокого навчання має велике значення для забезпечення лікарів надійними допоміжними методами діагностики. Область за межами ореолу черепа на ультразвукових зображеннях головного мозку плода містить багато нерелевантної інформації та має нечіткі межі, що не сприяє вирішенню задач класифікації або розпізнавання ультразвукових зображень. Метою роботи є дослідження впливу генеративних змагальних мереж на основі універсальних повністю згорткових дискримінаторів на результати автоматичної сегментації ореолу черепа на ультразвукових зображеннях головного мозку плода. У статті запропоновано метод автоматичної сегментації ореолу черепа на ультразвукових зображеннях головного мозку плода з використанням генеративної змагальної мережі на основі універсального повністю згорнутого дискримінатора. На основі концепції генеративних змагальних мереж побудовано нову семантичну мережу сегментації на основі універсального дискримінатора. Для перевірки універсальності дискримінатора мережа семантичної сегментації використовуються мережі Deeplab\_v2 та Attention U-net як генератори для генерації карт ймовірностей результатів сегментації. Універсальний повністю згортковий дискримінатор також розроблено для того, щоб він міг навчитися розрізняти, чи є карта ймовірностей на вході мережі дискримінатора реальними даними або результатами сегментації. Експериментальні результати на наборі даних автоматичного вимірювання окружності голівки плода при ультразвуковому дослідженні демонструють ефективність алгоритму. Порівняно з базовою лінією Deeplab\_v2, точність сегментації значно покращилася, і Attention U-net також має аналогічне покращення. Генеративна змагальна мережа на основі універсального повністю згорткового дискримінатора може ефективно підвищити точність автоматичної сегментації ореолу черепа на ультразвукових зображеннях мозку плода.

**Ключові слова:** центральна нервова система плода, генеративні змагальні мережі, Deeplab\_v2, Attention U-net..

УДК 004.415.2:[004.89:504.064.36]:519.816

**Бородкіна Ірина Лаврентіївна**

кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук,  
Національний університет біоресурсів і природокористування України

ORCID: <https://orcid.org/0000-0003-3667-3728>

E-mail: [i.borodkina@nubip.edu](mailto:i.borodkina@nubip.edu)

**Бородкін Георгій Олексійович**

старший викладач кафедри комп'ютерних наук,  
Національний університет біоресурсів і природокористування України

ORCID: <https://orcid.org/0000-0002-6488-6512>

E-mail: [heorhii.borodkin@nubip.edu.ua](mailto:heorhii.borodkin@nubip.edu.ua)

**Міловідов Юрій Олегович**

старший викладач кафедри комп'ютерних наук,  
Національний університет біоресурсів і природокористування України

ORCID: <https://orcid.org/0009-0000-5705-3590>

E-mail: [yurii\\_milovidov@nubip.edu.ua](mailto:yurii_milovidov@nubip.edu.ua)

## ВИБІР МОВИ ПРОГРАМУВАННЯ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ МОНІТОРИНГУ ЛІСІВ І ПРОТИДІЇ ПОЖЕЖАМ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЙ

**Анотація.** Робота присвячена розв'язанню актуальної науково-практичної задачі — обґрунтуванню вибору мови програмування для створення інтелектуальних систем екологічного моніторингу в режимі реального часу. У дослідженні наголошується на переході від пасивного спостереження до активного використання алгоритмів штучного інтелекту (комп'ютерного зору, глибокого навчання) для раннього виявлення лісових пожеж. Наукова новизна полягає у застосуванні математичного апарату методу аналізу ієрархій (MAI) для мінімізації суб'єктивізму при виборі технологічного стека. Авторами побудовано ієрархічну модель оцінювання чотирьох альтернатив: Python, C++, Rust та Lisp. Для порівняльного аналізу обрано п'ять ключових критеріїв: швидкість обробки, точність розпізнавання, автономність (енергоефективність), масштабованість та вартість розробки. Розрахунок вагових коефіцієнтів критеріїв продемонстрував пріоритетність точності детекції (43%) та продуктивності роботи системи (28%). За результатами обчислення інтегральних показників виявлено перевагу мови Rust (8,54), яка випередила C++ (7,82) та Python (7,16). Встановлено, що Rust є найбільш збалансованим рішенням для реалізації концепції Edge Computing, оскільки забезпечує безпеку пам'яті та високу швидкість обробки безпосередньо на автономних пристроях. У підсумку запропоновано оптимальну стратегію побудови гібридної архітектури: використання Rust для низькорівневих модулів детекції та Python для хмарної аналітики даних.

**Ключові слова:** метод аналізу ієрархій, інтелектуальні системи моніторингу, моніторинг лісових пожеж, штучний інтелект, мова програмування Rust, мова програмування Python, глибоке навчання, обробка в реальному часі, Edge Computing, багатокритеріальне прийняття рішень, багатокритеріальний аналіз.

**Актуальність.** Сучасний етап розвитку систем екологічної безпеки характеризується переходом від пасивного спостереження та фіксації результатів до активного моніторингу із використанням інтелектуальних систем у режимі реального часу.

У цій сфері одним із найскладніших завдань є раннє виявлення різноманітних нестандартних ситуацій, зокрема лісових пожеж та інших екологічно небезпечних явищ, де кожна хвилина затримки реагування може призвести до стрімкого зростання економічних і екологічних збитків.

Для вирішення цих проблем необхідно створювати системи, які здатні здійснювати безперервний моніторинг стану довкілля в реальному часі та оперативно приймати відповідні рішення. Створення таких систем потребує інтеграції складних алгоритмів штучного інтелекту (Computer Vision, Deep Learning) з апаратними засобами, що розбудовані зокрема на базі бездротових технологій і безпілотних літальних апаратів.

На етапі проєктування та обґрунтування вибору інструментальних засобів розробки інтелектуальних систем моніторингу надзвичайно важливою є проблема вибору мови програмування. Це питання не зводиться до простого порівняння характеристик різних мов, а передбачає розв'язання багатокритеріальної задачі, що потребує балансування між високою швидкістю обробки потоків даних і обмеженою енергоефективністю автономних пристроїв. Крім того, необхідно враховувати гнучкість реалізації сучасних нейромережових моделей.

На сьогодні відсутня єдина методика оцінювання програмного інструментарію, що часто призводить до застосування суб'єктивних підходів, що в свою чергу, знижує загальну надійність та ефективність інтелектуальних систем моніторингу довкілля.

**Аналіз останніх досліджень та публікацій.** Теоретичним фундаментом розв'язання задачі багатокритеріального вибору можна вважати роботи Saaty T. L., у яких було запропоновано метод аналізу ієрархій [1], [2]. Цей математичний апарат базується на обчисленні власних значень матриць попарних порівнянь і на сьогодні залишається одним із стандартних підходів у системній інженерії [3].

Сучасні модифікації та адаптації цього методу для цифрових екосистем запропоновано в роботах Goerel K. D., де акцентується увага на важливості узгодженості експертних суджень під час оцінювання програмних засобів [4]. Останні дослідження також підтверджують ефективність використання методу аналізу ієрархій у задачах вибору програмного забезпечення та інтелектуальних систем, зокрема в умовах невизначеності та багатокритеріальності. В роботі [6] розглянуто методологічні засади, які пов'язані з процесами побудови аналітичної ієрархії, зокрема, розглядаються питання, що пов'язані з моделюванням проблем, попарними порівняннями, шкалами оцінювання.

Методи багатокритеріального прийняття рішень (MCDM) можуть використовуватись в різних типах застосувань. В [7] проведено огляд поширених методів багатокритеріального прийняття рішень, розглянуто їх переваги та недоліки. В результаті, цю роботу можна вважати керівництвом, яке допомагає визначити, як методи MCDM слід використовувати в конкретних ситуаціях.

В роботі [8] автори стверджують, що вибір конкретного методу багатокритеріального прийняття рішень та способу нормалізації даних критично впливає на надійність результатів. Вони пропонують оцінювати інженерні рішення через компроміс між 5 вимірами: продуктивністю, екологічним впливом, економічним впливом, соціальним впливом та циклічністю.

Іншим аспектом, на який слід звернути увагу під час розробки інтелектуальних систем моніторингу є специфіка побудови таких систем залежно від сфери застосування. Так, питання, що пов'язані з виявленням пожеж детально досліджуються в роботах López et al., де автори наголошують на перевагах концепції Edge Computing (прикордонні або периферійні обчислення) для мінімізації часу реакції. Питання точності розпізнавання пожеж на базі глибокого навчання (Deep Learning) є центральними у дослідженнях В. Jahne [9], який вказує на пряму залежність ефективності алгоритмів від обчислювальної архітектури обраної мови.

В роботі [10] автори наголошують на необхідності переходу від класичних алгоритмів до алгоритмів глибокого навчання і зазначають, що інтеграція глибокого навчання в системи моніторингу лісів дозволила значно підвищити точність ідентифікації пожеж, зокрема автори доводять, що саме Deep Learning мінімізує кількість хибних спрацювань. Проте такий підхід висуває нові вимоги до архітектури обчислювальної системи.

Питання обробки відеопотоків в реальному часі розглядаються в [11], де автори наголошують на необхідності високої обчислювальної потужності, що прямо вказує на важливість використання відповідних програмних засобів і, зокрема, мов програмування.

Разом з тим, аналіз літературних джерел свідчить про наявність розриву між теоретичними дослідженнями алгоритмів штучного інтелекту та практичними рекомендаціями щодо вибору системних мов програмування для їх реалізації. Традиційні порівняння мов програмування не завжди враховують специфічні особливості саме систем екологічного моніторингу, такі як автономність та масштабованість у диких природних

умовах. Це зумовлює необхідність проведення комплексного аналізу мов програмування на основі математичних методів прийняття рішень.

**Мета дослідження** полягає в математичному обґрунтуванні вибору оптимального інструментарію програмування для розробки інтелектуальних систем моніторингу лісових пожеж шляхом застосування методу аналізу ієрархій. Цей підхід дозволить забезпечити баланс між високою точністю розпізнавання екологічно небезпечних ситуацій та продуктивністю обробки даних у реальному часі. Він може стати підґрунтям для переходу від суб'єктивного вибору мови програмування до об'єктивного математичного розрахунку, який базується на критичних вимогах безпеки.

**Матеріали і методи дослідження.** Вибір мови програмування як інструменту реалізації проєкту – це більша частина складової успіху проєкту. Скористаємось методом багатокритеріального аналізу рішень (MCDA), а саме методом аналізу ієрархій [1]. Цей метод являє собою структурований математичний апарат для прийняття складних рішень. Він розбиває проблему на ієрархію (мета, критерії, альтернативи) і за допомогою парних порівнянь дозволяє визначити найкращий варіант на основі кількісної оцінки суб'єктивних думок експертів. Таке попарне порівняння критеріїв суттєво зменшує суб'єктивну похибку.

Сформулюємо задачу вибору мови програмування як функцію корисності  $U$ , яку потрібно максимізувати.

$$U(L) = \sum_{i=1}^n w_i * c_i(L), \quad (1)$$

де  $L$  – конкретна мова програмування (Python, C++, Julia, Rust або інша);

$w_i$  – ваговий коефіцієнт  $i$ -го критерію, який визначає, наскільки цей критерій важливий для оцінювання;

$c_i(L)$  – оцінка мови  $L$  за  $i$ -м критерієм (зазвичай її значення береться від 0 до 1).

Для інтелектуальних систем основними критеріями зазвичай використовують:

$c_1$  – наявність бібліотек;

$c_2$  – продуктивність (особливо для систем, що працюють в реальному часі);

$c_3$  – швидкість розробки (тут слід враховувати лаконічність синтаксису та простоту прототипування);

$c_4$  – доступність документації та готових рішень;

$c_5$  – можливість інтеграції у вже існуючі системи.

Покроково алгоритм розрахунку ваги критеріїв має наступний вигляд.

**Крок 1.** Будуємо матрицю попарних порівнянь. Це квадратна матриця розміром  $n * n$ , де  $n$  – кількість критеріїв. Кожний елемент цієї матриці  $a_{ij}$  показує ступінь переваги критерію  $i$  над критерієм  $j$  за шкалою Сааті (значення 2, 4, 6, 8 є проміжними):

1 – однакова важливість,

3 – помірна перевага одного над іншим,

5 – суттєва перевага,

7 – значна перевага,

9 – абсолютна перевага.

У разі побудови матриці попарних порівнянь працює правило зворотної симетрії: якщо критерій  $A$  в 3 рази важливіший критерія  $B$ , то критерій  $B$  важливіший за  $A$  в  $1/3$  рази. На діагоналі матриці порівнянь завжди стоять одиниці.

**Крок 2.** Розраховуємо вагу кожного критерію. Для цього розраховуємо суму елементів у кожному стовпці матриці пріоритетів, нормуємо матрицю, розділивши кожний елемент матриці на суму його стовпця, та обчислюємо середнє арифметичне для кожного рядка отриманої на попередньому кроці нормованої матриці.

$$w_i = \frac{1}{n} \sum_{j=1}^n \frac{a_{ij}}{\sum_{k=1}^n a_{kj}}$$

В результаті буде отримано набір значень ваги критеріїв  $w_i$  сума яких дорівнює одиниці.

*Крок 3.* Перевіряємо отримані результати на узгодженість. Скориставшись алгоритмом, наведеним в [12] та он-лайн калькулятором для МАІ [5], розраховуємо головне власне число  $\lambda_{max}$  та знаходимо індекс узгодженості  $CI$ :

$$CI = \frac{\lambda_{max} - n}{n - 1}. \quad (2)$$

Та відношення узгодженості  $CR$ :

$$CR = \frac{CI}{RI} \quad (3)$$

В цьому випадку  $RI$  – табличне значення випадкової узгодженості для матриці заданого розміру. Якщо  $CR \leq 0,1$  (10%) то ваги критеріїв  $w_i$  вважаються прийнятними, якщо  $CR$  приймає більше значення, то матрицю порівнянь слід переглянути через те, що надані експертом судження є суперечливими.

**Результати дослідження та їх обговорення.** Побудуємо матрицю порівнянь для вибору мови програмування для інтелектуальної системи моніторингу лісів та боротьби з пожежами. В такій системі є критично важливою швидкість обробки даних в реальному часі (це забезпечить виявлення вогню за лічені секунди) та можливість інтеграції системи з наявним апаратним обладнанням (дрони, супутники, тепловізійні пристрої). Це означає, що критерії, за якими ми будемо обирати оптимальну мову програмування, мають бути такими:

$C_1$  – швидкість обробки в реальному часі (характеризує здатність мови програмування обробляти відеопотік з мінімальною затримкою).

$C_2$  – точність розпізнавання (вона забезпечується наявністю в мові програмування оптимізованих бібліотек для нейромережових обчислень);

$C_3$  – автономність (в процесі моніторингу необхідно забезпечити мінімальне споживання енергії та ресурсів пам'яті апаратним модулем);

$C_4$  – вартість розробки (в цьому критерії слід враховувати наявність фахівців та швидкість написання коду).

$C_5$  – масштабованість (цей критерій відповідає за стабільність роботи системи у разі розширення мережі пристроїв).

Пріоритетність критеріїв була визначена виходячи зі специфіки систем екологічної безпеки, де вирішальними факторами є час виявлення пожежі та надійність ідентифікації пожежі, яка на пряму пов'язана з мінімізацією хибних спрацювань. Таким чином, в нашому дослідженні домінуючими є критерії  $C_1$  та  $C_2$ .

Для організації процедури порівняння була побудована матриця  $A = [a_{ij}]$ , де  $a_{ij}$  – ступінь переваги  $i$ -го критерію над  $j$ -м за дев'ятибальною шкалою Сааті. За цих умов матриця попарних порівнянь має вигляд, що наведений у табл. 1.

Для отримання вектору локальних пріоритетів  $w$  був використаний метод нормалізації геометричного середнього:

$$w_i = \frac{\sqrt[n]{\prod_{j=1}^n a_{ij}}}{\sum_{k=1}^n \sqrt[n]{\prod_{j=1}^n a_{kj}}}$$

Таблиця 1 – Матриця попарних порівнянь з розрахованою вагою критеріїв  $w_i$ 

Критерії	C <sub>1</sub>	C <sub>2</sub>	C <sub>3</sub>	C <sub>4</sub>	C <sub>5</sub>	Вага ( $w_i$ )
<b>C<sub>1</sub> (Швидкість)</b>	1	1/2	3	5	4	<b>0.28</b>
<b>C<sub>2</sub> (Точність)</b>	2	1	4	7	5	<b>0.43</b>
<b>C<sub>3</sub> (Автономність)</b>	1/3	1/4	1	3	2	<b>0.13</b>
<b>C<sub>4</sub> (Вартість)</b>	1/5	1/7	1/3	1	1/2	<b>0.06</b>
<b>C<sub>5</sub> (Масштабованість)</b>	1/4	1/5	1/2	2	1	<b>0.10</b>

На наступному кроці для верифікації моделі було розраховано головне власне число  $\lambda_{max} = 5,21$  нашої матриці, що дозволило обчислити індекс узгодженості  $CI$ . Для цього була використана формула (2) для  $n=5$ , де  $n$  – розмірність матриці.

$$CI = \frac{5,21 - 5}{5 - 1} = 0,0525.$$

Для підтвердження достовірності результатів за формулою (3) було розраховане відношення узгодженості

$$CR = \frac{0,0525}{1,12} = 0,046, \text{ або } 4,6\%. \text{ (для } n = 5, \text{ значення } RI = 1,12).$$

Оскільки  $CR < 10\%$ , то отримані значення ваги вважаються достовірними.

Тепер можна перейти до порівняльного аналізу мов програмування. Альтернативами, серед яких будемо обирати, розглянемо такі мови програмування: Python, C++, Rust, Lisp. Проведемо оцінювання цих альтернатив за кожним із п'яти критеріїв. Узагальнені результати такого оцінювання за 10-бальною шкалою наведено в табл. 2.

Таблиця 2 – Матриця оцінювання альтернатив за шкалою (1-10)

Критерій	Python	C++	Rust	Lisp
<b>Точність (0.43)</b>	10	7	8	9
<b>Швидкість (0.28)</b>	3	10	10	5
<b>Автономність (0.13)</b>	4	9	10	4
<b>Масштабованість (0.10)</b>	9	6	7	6
<b>Вартість (0.06)</b>	10	4	5	5

Розрахуємо інтегральний показник (1) для кожної з альтернатив:

$$U(\text{Python}) = 10*0,43+3*0,28+4*0,13+9*0,10+10*0,06 = 7,16$$

$$U(\text{C++}) = 7*0,43+10*0,28+9*0,13+6*0,10+4*0,06 = 7,82$$

$$U(\text{Rust}) = 8*0,43+10*0,28+10*0,13+7*0,10+5*0,06 = 8,54$$

$$U(\text{Lisp}) = 9*0,43+5*0,28+4*0,13+6*0,10+5*0,06 = 6,69.$$

Згідно з розрахунками, мова Rust отримала найвищий інтегральний показник (8.54), випередивши C++ (7.82) та Python (7.16). Найнижчий показник продемонструвала мова програмування Lisp (6.69), що пояснюється її меншою придатністю для систем реального часу з обмеженими апаратними ресурсами.

Аналіз отриманих інтегральних показників (U) дозволяє глибше зрозуміти ієрархію вибору мови програмування для інтелектуальних систем екологічного моніторингу з критично важливими факторами, як-то виявлення пожеж. Отримані результати підтверджують гіпотезу про те, що для інтелектуальних систем реального часу технічні характеристики виконання програмного коду переважають над зручністю розробки.

Найвищий інтегральний показник мови Rust пояснюється її унікальною архітектурою. В процесі дослідження виявлено, що за критеріями «Швидкість» (C<sub>1</sub>) та «Автономність» (C<sub>3</sub>) мова програмування Rust не поступається C++, проте значно випереджає її за безпекою. У системах, що працюють в режимі Edge computing (на дронах або на автономних вежах), помилка переповнення буфера в C++ може призвести до повної зупинки пристрою. Rust виключає такі помилки на етапі компіляції, що робить систему більш живучою без втручання людини. Хоча мова програмування Python посіла загальне третє місце з інтегральним показником 7.16, вона отримала найвищий бал за критерієм «Точність» (C<sub>2</sub>). Це зумовлено наявністю зрілих бібліотек (PyTorch, TensorFlow). При цьому спостерігається чіткий розрив між зручністю розробки в Python та можливістю його запуску на малопотужному обладнанні. Це обґрунтовує необхідність переписування навчених моделей на мови системного рівня (Rust/C++) для їх реалізації безпосередньо в місці моніторингу.

Критерій «Автономність» (C<sub>3</sub>) став вирішальним для відсіювання мови програмування Lisp та зниження рейтингу мови Python. Для систем моніторингу лісів, де живлення здійснюється від сонячних батарей або акумуляторів, використання інтерпретованих мов є неефективним через високе енергоємне навантаження на процесор. Перехід на мови з прямим керуванням пам'яттю дозволяє подовжити термін роботи автономного вузла на 25-40% при тій самій ємності батареї.

Отже, на основі наведених вище міркувань можна запропонувати відійти від концепції використання лише однієї мови програмування для розробки інтелектуальних систем моніторингу лісів та боротьби з пожежами і запропонувати таку стратегію: для детекції (Edge) доцільно використовувати мову Rust, яка забезпечить максимальну швидкість та економію енергії; для обробки підтверджених даних доцільно використовувати мову Python, яка характеризується максимальною гнучкістю алгоритмів.

**Висновки і перспективи.** В результаті проведеного дослідження було розв'язано науково-практичну задачу обґрунтування вибору мови програмування для інтелектуальних систем моніторингу лісів та боротьби з пожежами на основі методу аналізу ієрархій. Застосування цього методу дозволило зробити нижче зазначені висновки.

Для систем екологічної безпеки критичними критеріями є точність розпізнавання (43%) та швидкість обробки даних у реальному часі (28%). Економічні чинники, такі як вартість розробки (6%), мають вторинне значення в контексті мінімізації ризиків розпізнавання масштабних лісових пожеж. Це означає, що для обрання мови програмування технічні характеристики повинні бути більш пріоритетними за зручністю програмування та інші чинники.

Застосування методу ієрархій дозволило сформувати рейтинг програмного інструментарію. За інтегральним показником ефективності перше місце посіла мова програмування Rust з інтегральним показником 8,54. Вона виявилася найбільш збалансованим рішенням, яке поєднує продуктивність системного рівня із сучасними механізмами безпеки використання оперативної пам'яті, що є критичним для автономних пристроїв.

Оцінено роль альтернативних мов програмування. Встановлено, що C++ (інтегральний показник 7.82) залишається потужним конкурентом для низькорівневих модулів, тоді як Python (інтегральний показник 7.16) є оптимальним вибором для верхнього рівня архітектури (хмарна аналітика). Lisp (інтегральний показник 6.69) продемонстрував потенціал для

складної логіки планування, проте наразі є обмеженим у застосуванні парадигми Edge computing, тобто у разі перенесення обробки даних із віддалених серверів (хмари) безпосередньо на пристрій, який ці дані збирає (камеру, дрон або датчик).

Сформульовано рекомендації до системної архітектури. Для досягнення максимальної ефективності рекомендовано впровадження гібридної моделі розробки: використання Rust для прошивки датчиків та дрон-систем первинної детекції, та Python – для централізованої обробки даних і візуалізації результатів моніторингу.

Практичне значення отриманих результатів полягає у можливості використання запропонованої математичної моделі розробниками складних ІТ-систем для об'єктивного вибору технологічного стека, що дозволяє уникнути архітектурних помилок на етапі проектування.

### Список використаних джерел

1. Saaty, T. L. (1980). *The analytic hierarchy process*. McGraw-Hill.
2. Saaty, T. L. (2003). Decision making with the analytic hierarchy process: Why is the principal eigenvector necessary. *European Journal of Operational Research*, 145(1), 85–91. [https://doi.org/10.1016/S0377-2217\(02\)00227-8](https://doi.org/10.1016/S0377-2217(02)00227-8).
3. Saaty, T. L. (2008). *Decision making for leaders: The analytic hierarchy process for decisions in a complex world* (Rev. ed.). RWS Publications.
4. Goepel, K. D. (2013). Implementing the analytic hierarchy process as a standard method for multi-criteria decision making in corporate enterprises. In *Proceedings of the International Symposium on the Analytic Hierarchy Process*. BPMMSG.
5. Goepel, K. D. (n.d.). *Analytic hierarchy process (AHP) tutorial*. Business Performance Management Singapore. Retrieved October 24, 2023, from <https://bpmsg.com/ahp-introduction/>
6. Ishizaka, A., & Labib, A. (2011). Review of the main developments of the analytic hierarchy process. *Expert Systems with Applications*, 38(11), 14036–14039. <https://doi.org/10.1016/j.eswa.2011.04.143>.
7. Velasquez, M., & Hester, P. T. (2021). An analysis of multi-criteria decision making methods. *International Journal of Operations Research*, 10(2), 56–66.
8. Malefaki, S., Markatos, D., Filippatos, A., & Pantelakis, S. G. (2025). A comparative analysis of multi-criteria decision-making methods and normalization techniques in holistic sustainability assessment for engineering applications. *Aerospace*, 12(2), 100. <https://doi.org/10.3390/aerospace12020100>.
9. Jähne, B. (2022). *Digital image processing: Concepts, algorithms, and scientific applications* (3rd ed.). Springer. <https://doi.org/10.1007/978-3-662-03174-2>.
10. Saleh, A., Zulkifley, M. A., Harun, H. H., Gaudreault, F., Davison, I., & Spraggon, M. (2024). Forest fire surveillance systems: A review of deep learning methods. *Heliyon*, 10(1), Article e23127. <https://doi.org/10.1016/j.heliyon.2023.e23127>.
11. Bustamante, A., Belmonte, L. M., Morales, R., Pereira, A., & Fernández-Caballero, A. (2022). Video Processing from a Virtual Unmanned Aerial Vehicle: Comparing Two Approaches to Using OpenCV in Unity. *Applied Sciences*, 12(12), 5958. <https://doi.org/10.3390/app12125958>.
12. Vargas, R. V. (2010). Using the analytic hierarchy process (AHP) to select and prioritize projects in a portfolio. In *Paper presented at PMI® Global Congress 2010—North America*, Washington, DC. Project Management Institute. <https://www.pmi.org/learning/library/analytic-hierarchy-process-prioritize-projects-6608>.

### Borodkina Iryna

*Candidate of Engineering Sciences, Associate Professor, Department of Computer Science, National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0000-0003-3667-3728>

E-mail: [i.borodkina@nubip.edu.ua](mailto:i.borodkina@nubip.edu.ua)

**Borodkin Heorhii**

Senior Lecturer of the Department of Computer Science,  
National University of Life and Environmental Sciences of Ukraine

ORCID: <https://orcid.org/0000-0002-6488-6512>

E-mail: [heorhii.borodkin@nubip.edu.ua](mailto:heorhii.borodkin@nubip.edu.ua)

**Milovidov Yuri**

Senior Lecturer of the Department of Computer Science,  
National University of Life and Environmental Sciences of Ukraine

ORCID: <https://orcid.org/0009-0000-5705-3590>

E-mail: [yurii\\_milovidov@nubip.edu.ua](mailto:yurii_milovidov@nubip.edu.ua)

## **PROGRAMMING LANGUAGE SELECTION FOR INTELLIGENT FOREST MONITORING AND FIRE-FIGHTING SYSTEMS USING THE ANALYTIC HIERARCHY PROCESS**

**Abstract.** This paper addresses the critical issue of selecting the optimal programming language for developing intelligent environmental monitoring systems operating in real-time. The study emphasizes the transition from passive observation to the active use of artificial intelligence algorithms (Computer Vision, Deep Learning) for the early detection of forest fires. The scientific novelty lies in the application of the mathematical framework of the Analytic Hierarchy Process (AHP) to minimize subjectivity in the selection of the technology stack. The authors constructed a hierarchical evaluation model for four alternatives: Python, C++, Rust, and Lisp. For the comparative analysis, five key criteria were selected: processing speed, recognition accuracy, autonomy (energy efficiency), scalability, and development cost. The calculation of the criteria weight coefficients demonstrated the priority of detection accuracy (43%) and real-time system performance (28%). Based on the integral indicators, the Rust language (8.54) showed clear superiority over C++ (7.82) and Python (7.16). It was established that Rust is the most balanced solution for implementing the Edge Computing concept, as it ensures memory safety and high processing speeds directly on autonomous devices. Consequently, an optimal hybrid architecture strategy is proposed: utilizing Rust for low-level detection modules and Python for cloud data analytics and visualization. This approach allows for a shift from subjective tool selection to objective mathematical justification based on critical safety requirements.

**Keywords:** Analytic Hierarchy Process, Intelligent Monitoring Systems, Forest Fire Monitoring, Artificial Intelligence, programming language Rust, programming language Python, Deep Learning, Real-time Processing, Edge Computing, Multi-Criteria Decision Making.

УДК 004.67

**Васьківський Вадим Олександрович**

аспірант кафедри комп'ютерних систем, мереж та кібербезпеки,  
Національний університет біоресурсів і природокористування України  
ORCID: <https://orcid.org/0009-0006-8969-7781>  
E-mail: [v.vaskivskiy@nubip.edu.ua](mailto:v.vaskivskiy@nubip.edu.ua)

**Горовий Ярослав Миколайович**

аспірант кафедри комп'ютерних систем, мереж та кібербезпеки,  
Національний університет біоресурсів і природокористування України  
ORCID: <https://orcid.org/0009-0002-7494-2538>  
E-mail: [iar.gorovyi@nubip.edu.ua](mailto:iar.gorovyi@nubip.edu.ua)

**Смолій Віктор Вікторович**

кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,  
Національний університет біоресурсів і природокористування України  
ORCID: <https://orcid.org/0000-0003-2834-6989>  
E-mail: [v-smolii@nubip.edu.ua](mailto:v-smolii@nubip.edu.ua)

## ТЕХНОЛОГІЇ DIGITAL TWINS У СИСТЕМАХ УПРАВЛІННЯ АГРАРНИМИ ПРОЕКТАМИ

***Анотація.** Протягом останніх кількох десятиліть глобальний ринок та життєві процеси показали, що багато різних аспектів людської діяльності тісно пов'язані. Це призводить до Стратегії сталого розвитку, спрямованої на збалансований взаємозв'язок довкілля (землі, атмосфера, екосистеми), суспільства (культура, освіта та охорона здоров'я) та економіки, в цілому. Такий комплексний підхід потребує нових інструментів для розробки та оцінки проектів у всіх сферах діяльності. Поточна робота присвячена потенційним напрямкам розвитку таких інструментів. У роботі розглянуто та проаналізовано можливі принципи побудови систем розробки проектів для сільськогосподарських підприємств на основі сучасних технологій цифрових двійників (Digital Twins), механізму онтологій та мережесервісів в умовах підвищення вимог Сталого Розвитку і загальних тенденцій раціонального та ощадливого використання ресурсів планети. У аналізі відзначено потенційно високу ефективність та універсальність запропонованого підходу не тільки для вирішення питань зі створення проектів, але й подальшого керування ними та моніторингу відповідності цільовим функціям. На умовному прикладі використання певної земельної ділянки розглянуто особливості та загальні підходи формування структури інформаційної моделі предметної області та суміжних інформаційних ресурсів. Визначено, також, два основні напрямки подальшого руху – створення бази для уніфікованої реалізації цифрових двійників та систем з автоматизованого аналізу онтологій представлених у форматах OWL та генерації на їх основі нових складних моделей-фреймворків. Робота є попереднім обґрунтуванням концепції створення нових систем управління життєвим циклом економічних та господарських проектів у аграрній сфері.*

***Ключові слова:** аграрний проект, Digital Twins, онтологія, OWL, сталий розвиток.*

**Актуальність.** Актуальним напрямком у світовому суспільстві стало завдання сталого розвитку [1] як наслідок швидкої індустріалізації та неконтрольованого впливу на оточуюче середовище. Зростання енергоємного виробництва з використанням викопних вуглеводнів призвело до ефекту глобального потепління зі зміною кліматичних умов у напрямку їх погіршення. Аналіз цих процесів показав необхідність найскорішого прийняття системи відповідних мір у всіх напрямках життєдіяльності людини та, як наслідок, прийняття стратегії сталого розвитку. Основними напрямками цієї стратегії [2] стали "...економічне зростання, соціальна справедливість та захист оточуючого середовища...", які ґрунтуються на п'яти принципах:

- 1) відповідальності та відданості країн виконанню цієї стратегії;
- 2) інтеграції економічної, соціальної та природозахисної політик у всіх сферах, на всіх територіях та на всіх етапах розвитку;

- 3) широкій залученості та ефективному партнерству;
- 4) розвитку відповідного потенціалу та сприятливого середовища;
- 5) зосередженість на результатах та засобах з їх реалізації.

Отже, навіть поверхневий аналіз цих принципів вказує на основну мету, яку можна сформулювати як застосування всебічно зважених та передбачуваних шляхів розвитку у всіх напрямках діяльності на основі розробки та застосуванні відповідних інструментів системного аналізу та прогнозування процесів на всіх етапах їх життєвого циклу.

Така постановка загальної задачі, відповідно, вказує на необхідність розробки нових принципів та моделей наскрізного керування суспільно-соціальними об'єктами та процесами, об'єктами та процесами у промисловості, аграрництві та такою новою компонентою як оточуюче середовище. Одним з перспективних інструментів, здатних допомогти вирішити значну кількість з проблем, які при цьому виникають, є технологія Digital Twins (DT) – “Цифрових Двійників”.

У базовому тлумаченні DT – це [3,4] “... Віртуальна модель фізичного об'єкта чи системи для точного відображення властивостей. Він охоплює життєвий цикл об'єкта...”. У більш широкому тлумаченні, під цифровим двійником можуть розуміти [5] не тільки фізичні об'єкти, а також технологічні, природні або соціальні процеси. Важливим фактором є акцентуація на повному життєвому циклі, тобто від “народження ідеї” до закінчення фізичного існування матеріального об'єкту або переведення інформаційного (програмного) об'єкту у стан “архівачії”.

Другим важливим фактором є тісний та постійний зв'язок інформаційної моделі об'єкту з інформаційною моделлю всесвіту, майже у прямому сенсі – її місце та зв'язки з моделями інших об'єктів, які мають безпосередній або непрямий вплив на об'єкт спостереження або від нього – наприклад, для DT поля це можуть бути DTs сільськогосподарської техніки, оточуючих екосистем, спільноти що використовує це поле, атмосфера та інші об'єкти всесвіту. Крім цього, процес взаємодії між інформаційними моделями відповідних об'єктів повинен відбуватися на всіх стадіях життєвого циклу також. Ще на стадії проектування, таким чином, здійснюється моделювання можливої поведінки об'єктів при взаємних впливах та вибір таких значень відповідних проектних параметрів, які не тільки мають позитивний вплив на створюваний об'єкт, а ще й за можливістю покращують стан оточуючого середовища або, що найменше, не шкодять йому.

У поєднанні з концепцією Сталого Розвитку, створення нового об'єкту або використання об'єкту повинні задовольняти вже не одній цільовій функції оптимізації процесу існування, а комплексу з функцій взаємодії усіх пов'язаних об'єктів не тільки з об'єктом спостереження, але й між собою, що зі структурної точки зору призводить до створення повно-графової інформаційної моделі, яка на сьогодні залишається найбільш складною для застосування у процесах не тільки моделювання, але й звичайного моніторингу. Слід, також, відзначити можливість виникнення інформаційних систем з наперед не визначеною або динамічною гнучкою топологією внутрішніх зв'язків. Практично, кожен об'єкт із навколишнього середовища може стати компонентою, включеною у процес аналізу та застосування. Такий підхід робить неможливим використання “класичних” підходів як з контролю та керування поточними процесами, так і процесів проектування та аналізу, оскільки не існує таких узагальнених моделей. Недостатньо досліджено, наприклад, процеси у екологічних системах та їх реалізація у рамках однієї системи проблематична за наявними обчислювальними ресурсами. У такій парадигмі створюваний об'єкт чи процес, таким чином, може перестати бути найбільш значущим фактором у визначенні кінцевої цільової функції при проектуванні або моніторингу.

Наявність таких особливостей, крім усього, буде обмежувати й використовувані методи проектування, оскільки з точки зору системного підходу на первинному етапі виникає завдання розробки підходів для створення системи гетерогенних моделей з динамічною змінною структурою внутрішньої топології та довільним рівнем масштабування ресурсів. Відповідно, методи проектування системи “зверху вниз” стають мало прийнятними за

наявності великої кількості невизначеностей. При використанні методів проектування знизу-вверх, спочатку визначаються принципи та вимоги функціонування компонентів низького рівня, а потім вже методи їх інтеграції. Тобто, система буде деталізуватися за ходом появи нових об'єктів у “моделі всесвіту” створюваного об'єкту. На наш погляд, в умовах сьогодення, проектування знизу вверху відносно глобальної вирішуваної задачі має більше переваг з наступних причин:

- окремі об'єкти та системи досить ретельно вивчені, описані та автоматизовані;
- для проектування та прогнозування роботи таких об'єктів накопичено багато знань та розроблено відповідні моделі;
- як за правило, наявні технічні засоби моніторингу, які у DT-моделі створюють потік початкових даних для аналізу поведінки об'єктів та оперативного коригування характеристик і параметрів моделі у реальному часі.

До основних труднощів реалізації слід віднести наступні фактори:

- сучасні моделі об'єктів мають бути розширені для врахування впливу та взаємодії з зовнішніми об'єктами та системами;
- відсутні підходи та технології для створення моделей “екосистем всесвіту” в які повинні інтегруватися об'єкти призначення;
- відсутні технології та технічні/програмні системи для реалізації наскрізного життєвого циклу як окремих об'єктів так і її “екосистем” в цілому.

Але, на наш погляд, той самий принцип будови “знизу вверху” можливо ефективно застосувати для вирішення цих питань та інтеграції наявних інструментальних та алгоритмічних засобів. Для висвітлення можливих шляхів вирішення цих актуальних завдань, їх певні особливості та перспективні для застосування наявні технології будуть розглянуті нижче.

**Аналіз останніх досліджень та публікацій.** Класичні системи управління проектами [6-10] мають за більшістю своїх особливостей та можливостей багато спільного. Основні можливості складаються з реалізації наступних функціональних задач:

- створення проекту – опис завдання у економічних показниках з розподілом ресурсів у часі;
- планування робіт по виконавцях/ресурсах;
- створення календарів працівників;
- поточний контроль стану проекту у часі та коригування (за потребою);
- розрахунок економічних показників.

Додаткові функціональні можливості полягають у реалізації колективного доступу до проекту з різними привілеями та цілями, певні функціональні особливості для проектів у сфері створення програмного продукту (відслідковування помилок та моніторинг їх статусу, розподіл обов'язків), можливості взаємодії у паралельних проектах для співвиконавців.

Окремо слід відзначити можливості пропрієтарної системи Microsoft Project [11] яка містить, наприклад, такі додаткові інструменти з аналізу стійкості проекту та інших економічних характеристик проекту.

Але до недоліків подібних систем слід віднести їх “жорстку прив'язку” до параметрів вирішуваної задачі – так, наприклад, у процесі створення проекту та аналізу його характеристик немає можливості завдання “альтернатив” з реалізації тієї або іншої гілки проекту за використовуваними ресурсами або альтернатив для купи гілок з метою пошуку найбільш ефективних рішень в умовах наявності певних обмежень, що найбільш характерно для систем прийняття рішень. Тобто, при зміні одного параметру, практично необхідно створювати окремий проект для того щоб порівняти їх результати та характеристики.

Загальним недоліком таких систем, з огляду сучасних тенденцій з орієнтацією на Сталлий Розвиток, є повна відсутність відповідних компонентів для аналізу впливу проекту на основні напрямки сталості – соціальні фактори, екологію, здоров'я та інші.

Функція підбору параметрів або налаштувань характерна, як було вказано, для систем прийняття рішень, але є найпоширенішою у системах автоматизованого/автоматичного керування (САК) процесами, які також базуються на моделях, але мають процедури коригування поведінки у залежності від поточного стану з реалізацією механізмів підтримання цільового значення контрольних параметрів. Інколи, для аналізу стану та реалізації керуючого впливу використовують не тільки поточне значення параметру, а його динаміку за сукупністю даних у “часовій серії”. Але для підтримки таких можливостей у САК включають пристрої зв’язку з об’єктами - систему сенсорів та виконавчих пристроїв.

Слід зазначити, що моделі використовувані у економічному проектуванні та САК є, найчастіше, взагалі різними, що також ускладнює реалізацію та контроль “сумісності” інформаційних моделей при реалізації різних задач. На цих етапах роботи використовують математичні формалізовані моделі, що пов’язують значення вихідного цільового параметру з набором похідних параметрів – у одному випадку економічні характеристики, у другому – оцифровані дані що отримані з об’єкту.

Подібна функція передбачена тільки у Microsoft Project. Але, вона передбачає ручне введення контрольних параметрів для визначення їх відхилення від проектних значень у відповідні контрольні часові точки, або зміну часових параметрів похідного проекту для оцінки відмінності очікуваних результатів від тих, що передбачалися початково. Тобто, контроль відповідності до цільової функції не здійснюється у автоматичному режимі та за виникненням відповідної події, або зміни її характеристик, що не відповідає контролю у реальному часі. Слід відзначити, що для вирішення більшості задач аграрної сфери не має такої необхідності. Але певні задачі потребують досить оперативного контролю та втручання при виникненні відхилень від планових показників, наприклад, поточних витрат пального при проведенні механізованої обробки сільськогосподарських угідь у напрямку їх збільшення.

З точки зору створення систем, що відповідають задачам сталого розвитку, подібні та інші зміни параметрів можуть мати значний вплив на суміжні процеси та сфери – вплив на екологічний стан (викиди забрудників чи зміна хімічного складу ґрунту, зміна структури насаджень), економічний – перерозподіл ресурсів підприємства, соціальний – залучення додаткових співробітників та інше.

Отже, основним недоліком майже усіх систем економічного проектування є їх орієнтованість на методи та алгоритми економічної оцінки, а не на проблемний об’єкт та оцінку його поведінки.

**Метою** статті є аналіз можливостей застосування технологій Digital Twins у системах управління аграрними проектами та обґрунтування підходів до побудови інтегрованих інформаційних моделей на основі онтологій і мережевих сервісів в умовах сталого розвитку.

**Матеріали і методи дослідження.** Для того, щоб можна було здійснити більш-менш універсальний та формалізований опис предметної області на сьогодні реалізовано спеціалізований інструмент – технологію “онтологій”, за допомогою якої здійснюється висвітлення як структури самого об’єкту так і його системне представлення з інформаційними та технологічними зв’язками. Для фіксації та збереження опису моделі використовують xml-подібну структуру мови OWL [12].

Основними особливостями формування онтології є її деревовидна структура [13] у вузлах якої знаходяться сутності (об’єкти) які характеризують певні властивості основної сутності, а зв’язки між ними – дію, яка характеризує особливість включення об’єкту нижнього рівня, наприклад: “АТМОСФЕРА” – характеризується – “СКЛАД” – містить – “КИСЕНЬ” – і далі “...”.

До інших особливостей слід віднести, що деревоподібний граф є ациклічним та направленим. Цей фактор є й позитивним фактором з точки зору складності інтерпретації можливого руху у напрямку досягнення цільового показника, але потребує додаткових операцій з представлення певних особливостей, наприклад, опис агротехніки вирощування певного виду рослин, з кількома одноманітними циклами, що складаються з послідовності різних операцій. У такому разі, ці цикли потрібно розгортати у довгий ланцюг.

Актуальний стан у цьому напрямку є таким, що на сьогодні створено доволі велику сукупність спеціалізованих онтологій та сервісів для їх зберігання та організації доступу до них. Велика кількість з них спрямована тако ж на аграрні задачі, у тому числі на рослинництво. Так, наприклад, [14] містить велику кількість посилань на онтології, пов'язані з основними сферами аграрництва, або Planteome [15] – спеціалізований на рослинництві ресурс, який містить як свою базу онтологій так і посилання на зовнішні ресурси подібного призначення, або Crop ontology tool [16] також спрямованого на описи онтологій рослинницьких культур.

Слід зазначити, що зараз онтології «як-такі» окрім накопичення знань у спеціалізованих предметних областях ще виконують важливу роль у створенні Semantic WEB, що дозволяє проводити автоматичну структурування інформації у мережі Інтернет та орієнтований, у першу чергу, на автоматичну машинну обробку даних пошуковими системами та роботу зі штучним інтелектом.

Але однією з найбільших проблем є створення повної сукупності онтологій суттєвостей, що мають формувати повну систему об'єктів та зв'язків, що формують модель за вимогами сталого розвитку – «онтології всесвіту». Ця проблема значною мірою обумовлена тим, що більшість зв'язків об'єктів із зовнішнім середовищем і ще більше із певними соціальними процесами на сьогодні є ще не визначеними. Так наприклад, ми не можемо точно вказати як та чи інша агротехніка впливає на навколишнє середовище – стан та якість ґрунтів не тільки за хімічним складом, а й за станом ґрунтових вод, ерозії, зміни клімату та мікроклімату, хімічного складу та якості атмосфери, структурний склад рослинності на прилеглих територіях, та інші подібні питання. А окрім цього є неявний соціо-культурний вплив та багато інших напрямків.

Подібні завдання сьогодні почали вирішуватися створенням «статистичних» моделей на основі накопичуваних даних та їх кореляційного аналізу відносно визначеного процесу або з використанням розпізнавання на основі штучного інтелекту (ШІ). У останньому випадку, на відміну від кореляційної моделі, результати можна описати певною математичною залежністю, але досить швидко можна використовувати для прогнозування очікуваних результатів.

Використання ШІ є, також, невід'ємною складовою у ДТ-моделях, оскільки за визначенням, така модель повинна постійно само-вдосконалюватися у поведінці та підвищенні точності прогнозованих результатів, що відповідає завданням навчання на попередніх результатах та коригування параметрів моделі на неперервному потоці нових вхідних даних. За цей потік даних відповідає сенсорна мережа відповідного об'єкту, бо у разі вирішення аграрних задач ми маємо справу з розгалуженими у просторі об'єктами, навіть якщо мова йде про засоби обробки, наприклад, сівалки або обприскувачі з індивідуально керованими форсунками, які формують ланку обробки з можливістю коригування поточного стану.

У подібному трактуванні, певний економічний проект має у своїй основі містити набір електронних аналогів ДТ-моделей усіх реальних компонентів, що охоплює проект. Але, самі ДТ-моделі за своїм визначенням вже є електронними моделями. З цієї точки зору, додавши режим та можливість «умовної дії», який полягатиме у здійсненні «фіктивної» зміни стану досліджуваного об'єкту при отриманні фіктивних, точніше модельних, даних або дій, ми можемо отримати систему моделювання для оцінки проекту. Крім того, великою перевагою отриманих результатів може бути цільна сукупність часової розгортки поведінки та характеристик усіх об'єктів, що входять до моделі.

Сам процес моделювання полягатиме в тім, щоб сформувати (на початку у інтерактивному режимі) розклад виконання певних операцій та подій, або налаштувати певний «шаблон» який вже є сформований. У останньому випадку, це може бути об'єкт, що описує технологічну послідовність (алгоритм, агротехніка вирощування і т.д.) що передбачається для реалізації. Система, що керує процесом моделювання, повинна у такому разі виконувати функції координації та синхронізації обміну даними між визначеними за моделлю об'єктами. Та ж сама система може виконувати і функції автоматизованої системи

керування але вже з використанням режиму «реального часу», раніше підготовленого у процесі моделювання розкладу подій (операцій, впливів) та реальних отримуваних сенсорною мережею даних.

До потенційних переваг подібного підходу відразу можна віднести високий рівень автоматизації процесів моделювання і керування, оскільки похідні дані можуть бути отримані безпосередньо від конкретної ДТ-моделі, вони враховують її індивідуальні особливості а не «узагальнені» як у звичайних моделях, та у процесі моделювання також враховують особливості індивідуальної «поведінки» об'єктів.

Основним обмеженням чи первинною вимогою для такої системи є, на наш погляд, основний використовуваний ресурс. Розглянемо потенційні особливості на прикладі земельних ресурсів при виробництві рослинної (наприклад овочевої) продукції.

Великі поля мають, у першу чергу, свої індивідуальні характеристики по конфігурації, просторовому розташуванні, ґрунтам, наявності водних ресурсів та інших параметрів. Слід відразу зазначити, що за рахунок великої просторової розподіленості поля не однорідні за своїми властивостями на всій своїй площі. Це, з огляду і раціональності використання і задач сталого розвитку вимагає його розбивки на ділянки з більш-менш сталими характеристиками та використання технологій точкового землеробства та моніторингу. Виходячи з цього, кожна складова ділянка буде мати свої індивідуальні характеристики (по усіх групах можливих параметрів), що є обов'язковим.

До більш загальних та незалежних характеристик слід віднести кліматичні та метеорологічні умови – загальні та добові коливання температури та вологості повітря, напрямки та швидкості вітру, соляризація та таке інше, у тому числі хімічний, фізичний та біологічний склад атмосфери.

З технологічної точки зору та агрономії, важливим є історія раніше вирощуваних агрокультур, що значною мірою буде впливати на наступні агротехнічні та біозахисні заходи.

**Результати дослідження та їх обговорення.** Враховуючи вище зазначене, можна запропонувати базову структуру онтології для полів, що представлено на рис. 1.

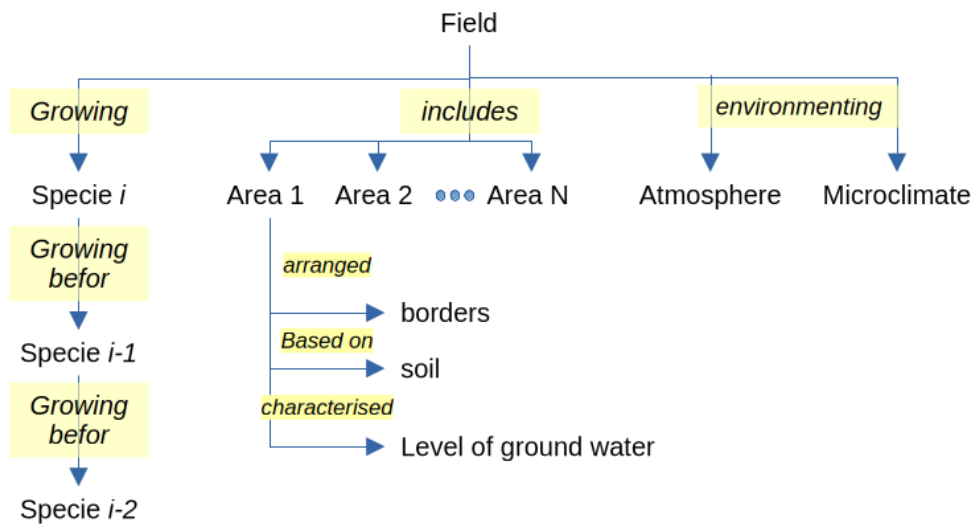


Рисунок 1 – Приклад базової онтології "Поле"

Чому саме інформаційна одиниця «Поле» обрана похідною у створенні проекту? Тому що її основні властивості впливатимуть на кейс можливих подальших рішень. Так основним чинником є ґрунт з його поточною структурою, хімічним та біологічним складом. Саме ці чинники впливають на те, що можна вирощувати на саме цьому ґрунті. Додатковими чинниками будуть рівень ґрунтових вод, мікроклімат та метеорологічні фактори які можуть коригувати впливові на технологію вирощування фактори упродовж сезону. Крім того при виборі агрокультури важливим є сівообіг, який дозволяє не тільки підвищити ефективність

рослинництва, але ще й зберегти чи відновити певні екологічні характеристики відповідних ділянок та поля цілком.

На наступному кроці, після підбору агрокультури, відповідно до особливостей онтології обраного виду рослин для системи моделювання з'явиться розклад агротехнічних операцій, що є невід'ємною характеристикою для певного виду рослин та відповідною компонентою обраної онтології. Подальший процес моделювання (з урахуванням на цьому етапі типової метеорологічної моделі) буде полягати у зчитуванні чергового кроку з типового розкладу, ідентифікації потрібних ресурсів та розподіленні (передачі) інформації по відповідних DT-моделях, що задіяні на поточному етапі. Після цього у моделі відбуваються певні зміни станів компонентів та, при необхідності та наявності зв'язків між цільовими компонентами — фіксація та обмін контрольними даними з певним кроком у часі до досягнення часу чергової події, після чого процес повторюється до завершення розкладу.

Для додаткового контролю необхідно (бажано) у DT-моделі агрокультури мати також, хоча б статистичну модель її поведінки, що відповідає типовим кліматичній та мікрокліматичній моделям. Це дозволить коригувати та попередньо синхронізувати «узагальнений» розклад до місцевих умов.

Отже, наведений підхід дозволяє попередньо сформувати інформаційно-структурну схему системи моделювання, яку представлено на рис. 2.

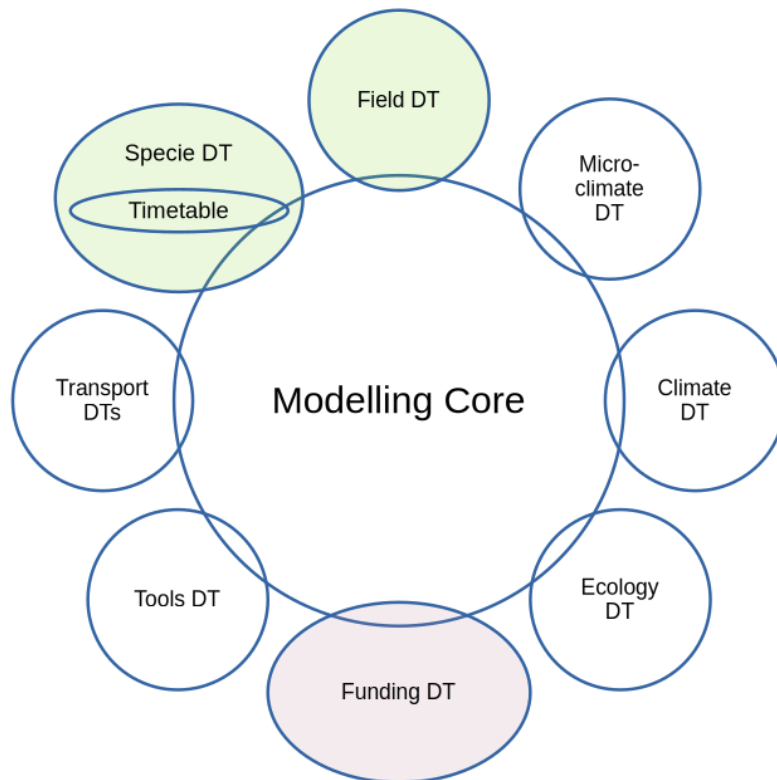


Рисунок 2 – Структурна системи моделювання аграрного проекту

Відповідно до описаної схеми взаємодії, обмін даними відбувається у двох напрямках — від системи моделювання до DT компонентів і, як відповідна реакція, у зворотному напрямі. Враховуючи особливості об'єктів які мають бути задіяні у процесі моделювання та подальшого моніторингу, можна стверджувати, що за своєю реалізацією система буде розгалуженою, а відповідні цифрові двійники можуть бути реалізовані на зовнішніх ресурсах інших організацій, наприклад у виробника відповідного технічного засобу, або місцевої метеорологічній службі. Такий характер, крім того, проявляється не тільки на цьому інформаційному рівні, а тако ж на рівні окремих двійників, оскільки дані про поточний стан

поля створюватиметься за рахунок сенсорних мереж окремих ділянок та зберіганням даних на спеціалізованих серверах баз даних.

**Висновки та перспективи.** Враховуючи наведені міркування, доцільною є реалізація окремих двійників у формі мережевих сервісів з відповідними двоспрямованими інтерфейсами. Такий підхід дозволить легко масштабувати модель та модифікувати її компоненти без втрати загальної функціональності та «властивостей».

Великою перевагою у створенні автоматизованої системи з розробки аграрних проектів на основі онтологій та DT-моделей є чітка та жорстка структурованість інформації у форматі xml, що дозволяє використовувати методи лінгвістичного аналізу при будові інформаційної структури проекту за прикладом компіляторів та конфігураційних систем спеціалізованих фреймворків. Головною проблемою, яка на сьогодні існує, є відсутність стандартів на структуру DT-моделей, інструментальних засобів з їх реалізації та сервісів для їх розгортання.

Отже, основними перспективними напрямками для подальшого розвитку систем автоматизованого проектування за вказаними вище підходами можна вказати наступні два напрямку: розробка підходів та інтерфейсів, алгоритмічного, програмного та технічного забезпечення для розгортання сервісів DT-моделей; розробка автоматизованих засобів з побудови інформаційних моделей на основі онтологій.

### Список використаних джерел

1. United Nations Development Programme. Sustainable development goals. Retrieved December 14, 2025, from <https://www.undp.org/sustainable-development-goals>.
2. United Nations Preparatory Committee for the World Summit on Sustainable Development (2nd sess. : 2002 : New York), & United Nations Department of Economic and Social Affairs, Division for Sustainable Development (Eds.). (2002). Guidance in preparing a national sustainable development strategy: Managing sustainable development in the new millennium. United Nations, Department of Economic and Social Affairs. <https://digitallibrary.un.org/record/459670>.
3. IBM. (2020). What is a digital twin? <https://www.ibm.com/think/topics/digital-twin>.
4. Amazon Web Services, Inc. What is digital twin technology? Retrieved March 10, 2024, from <https://aws.amazon.com/what-is/digital-twin/>.
5. McKinsey & Company. What is digital-twin technology? Retrieved December 14, 2025, from <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-twin-technology>.
6. SourceForge. (2019). OpenProj – Project management. <https://sourceforge.net/projects/openproj/>.
7. GanttPRO. GanttPRO як альтернатива Microsoft Project Online [GanttPRO as an alternative to Microsoft Project Online]. Retrieved September 29, 2025, from <https://ganttpro.com/ru/microsoft-project-online-alternative/>.
8. ProjectLibre. ProjectLibre AI. Retrieved September 29, 2025, from <https://www.projectlibre.com/>.
9. Wikipedia contributors. (2025). Redmine. In Wikipedia. <https://en.wikipedia.org/w/index.php?title=Redmine&oldid=1307913022>.
10. BarD Software s.r.o. GanttProject: Free project management tool for Windows, macOS and Linux. GanttProject. Retrieved September 29, 2025, from <https://www.ganttproject.biz>.
11. Microsoft. Keruvannia proektamy z povnym kontrolem protsesiv [Project management with full process control]. Retrieved September 29, 2025, from <https://www.microsoft.com/uk-ua/microsoft-365/project/project-management>.
12. World Wide Web Consortium. OWL – Semantic web standards. Retrieved December 14, 2025, from <https://www.w3.org/OWL/>.
13. Motik, B., Patel-Schneider, P. F., & Parsia, B. (Eds.). (2012). OWL 2 web ontology language: Structural specification and functional-style syntax (2nd ed.). World Wide Web Consortium. <http://www.w3.org/TR/2012/REC-owl2-syntax-20121211/>.

14. Aubert, C., & Arnaud, E. (2021). Ontologies most used in agriculture: Make your data interpretable and interoperable with ontologies (Version 1). Zenodo. <https://doi.org/10.5281/zenodo.6609666>.
15. Planteome. Planteome: Welcome. Retrieved October 6, 2025, from <https://browser.planteome.org/amigo>.
16. Crop Ontology. Crop ontology curation tool. Retrieved October 6, 2025, from <https://cropontology.org/>.

### **Vaskivskiy Vadym**

*PhD student in Computer Science,*

*National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0009-0006-8969-7781>

E-mail: [v.vaskivskiy@nubip.edu.ua](mailto:v.vaskivskiy@nubip.edu.ua)

### **Gorovyi Iaroslav**

*PhD student in Computer Science,*

*National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0009-0002-7494-2538>

E-mail: [iar.gorovyi@nubip.edu.ua](mailto:iar.gorovyi@nubip.edu.ua)

### **Smolii Victor**

*Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Systems, Networks, and Cybersecurity,*

*National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0000-0003-2834-6989>

E-mail: [v-smolii@nubip.edu.ua](mailto:v-smolii@nubip.edu.ua)

## **DIGITAL TWINS TECHNOLOGIES IN AGRICULTURAL PROJECT MANAGEMENT SYSTEMS**

**Abstract.** *In the last few decades, global market and life processes have shown that many different aspects of human activity are closely tied. This leads to the Sustainable Development Strategy targeted at the balanced interconnection of the environment (lands, atmosphere, ecosystems), society (cultural, educational and health) and economics, of course. Such complex approach needs a new tool for development and evaluation projects in all activity spheres. The current work is devoted to the potential directions for development such tools. The possible principles for developing project development systems in agriculture are considered and analysed in the research, which are based on modern technologies, including Digital Twins, Ontologies, and network services, in the context of increasing requirements for Sustainable Development and general trends towards rational and economical use of the planet's resources. The analysis demonstrates the potentially high efficiency and versatility of the proposed approach not only for solving issues of project creation, but also for their further management and monitoring of compliance with target functions. By examining the conditional example of a sowing field, the features and general approaches to forming the information model structure of the domain area and its connected environment are considered, based on determined and tied ontologies. Two main directions of further research are also identified: creating a base for the unified implementation of digital twins and automated analysis systems of ontologies presented in OWL formats, and generating new, complex framework models based on them. The paper consists of a preliminary justification for the concept of new system development for the life cycle of economic and business project management in the agricultural sector.*

**Keywords:** *Agrarian Project, Digital Twins, Ontology, OWL, Sustainable Development.*

UDC 004.3:004.5

**Nazarenko Volodymyr***Ph.D., Computer Systems, Networks and Cybersecurity Department, Faculty of Information Technologies, National University of Life and Environmental Sciences of Ukraine*ORCID: <https://orcid.org/0000-0002-7433-2484>E-mail: [volodnz@nubip.edu.ua](mailto:volodnz@nubip.edu.ua)**Ostroushko Bogdan***Assistant of the Department of Computer Systems, Networks, and Cybersecurity, National University of Life and Environmental Sciences of Ukraine*ORCID: <https://orcid.org/0009-0003-0849-8990>E-mail: [b.ostroushko@nubip.edu.ua](mailto:b.ostroushko@nubip.edu.ua)**MODELING EVALUATION FRAMEWORK FOR ROBOTICS AND DIGITAL TWIN SIMULATION PLATFORMS WITH AN UNREAL ENGINE 5 WAREHOUSE CASE STUDY**

**Abstract.** Digital twins and high-fidelity simulators are becoming central to the design, testing, and operation of modern robotic systems in industry, logistics, and human–robot interaction. However, existing comparative studies typically focus on a single robot type, task, or simulator, and rarely consider digital–twin–specific aspects, such as telemetry pipelines, operator interfaces, or cloud connectivity. This article proposes a unified evaluation framework for robotics-oriented digital twin platforms. It applies it across five representative use cases: (i) small UAV inspection, (ii) an industrial hand-robot cell, (iii) a warehouse logistics cell with autonomous mobile robots (AMRs), (iv) HCI/VR-based teleoperation of a mobile manipulator, and (v) a general indoor patrol and docking scenario.

The framework standardises inputs (robot and environment profiles, task definitions, digital-twin data contracts) and outputs (physics/task metrics, performance metrics, and DT metrics) and explicitly encodes task complexity via structured phases and control steps per episode. It is implemented on several widely used robotics simulators (Gazebo/gz-sim, Webots, NVIDIA Isaac Sim, CoppeliaSim) and on an Unreal Engine 5 (UE5)–based stack that combines Datasmith asset import, Chaos Physics, Blueprints/Control Rig, and UMG/VR interfaces.

As a detailed case study, we instantiate the warehouse logistics use case as a UE5-based digital twin and report quantitative results on order throughput, path lengths, real-time factor, frame times, telemetry bandwidth, and UI-to-actuation latency, along with observed bottlenecks such as Blueprint CPU overhead and visual-load–induced slowdowns. Across all platforms and use cases, the results highlight trade-offs between physical fidelity, scalability, interaction richness, and DT responsiveness, and lead to practical guidelines for selecting and composing simulation and digital-twin stacks for UAV, manipulation, logistics, and HCI-centric applications. The paper concludes with a discussion of limitations, including the simplification of physics and hardware dependence, and outlines future steps toward sim-to-real correlation and automated benchmarking.

**Keywords:** Digital Twin, Robotics Simulation, Unreal Engine 5, Gazebo, Webots, NVIDIA Isaac Sim, CoppeliaSim, Warehouse Logistics, UAV Inspection, Industrial Robot, VR/AR Teleoperation, Evaluation Framework.

**Introduction.** Digitalisation of physical assets and processes through robotics and digital twins (DTs) is transforming industrial production, logistics, and autonomous systems. A digital twin is typically defined as a dynamic virtual representation of a physical system that remains connected to it through data exchanges, enabling monitoring, prediction, and optimisation across the system lifecycle [1–3]. In robotics, DTs build upon simulation platforms that emulate kinematics, dynamics, sensors, and environments, while maintaining a bidirectional link to real hardware and industrial back-end systems. This combination allows engineers to prototype and validate control strategies, layouts, and interaction concepts safely and at lower cost than purely physical experimentation [4–6]. Over the past decade, a rich ecosystem of robotics simulators and DT-oriented platforms has emerged. Widely used open-source tools, such as Gazebo/gz-sim and Webots, provide ROS/ROS 2–integrated environments for mobile robots and manipulators, featuring configurable physics engines and sensor models [7–9]. CoppeliaSim (formerly V-REP) emphasizes flexible distributed control and multi-physics support, while NVIDIA Isaac Sim targets GPU-accelerated, photorealistic simulation and reinforcement learning workloads in logistics and industrial settings [10–12]. In parallel, general-purpose game engines such as Unity and Unreal Engine have become increasingly popular as

rendering and interaction layers in digital-twin architectures, offering high-quality graphics, VR/AR pipelines, and mature UI frameworks [13–15].

Existing comparative studies provide valuable insights but exhibit several limitations. Many works analyse a narrow set of simulators under a single application scenario, for example, a mobile robot navigating in a structured environment or a single industrial manipulator performing a pick-and-place task [16–19]. Others compare Unity or similar engines with robotics-oriented simulators such as Gazebo, focusing on visual fidelity, ROS integration effort, or development productivity in specific domains such as greenhouse robotics or small industrial workcells [20–22]. In most cases, the DT layer is treated as an implicit or secondary aspect: telemetry pipelines, latency, data volumes, and back-end integration are rarely measured explicitly, and human-in-the-loop interaction (e.g., VR teleoperation, 3D dashboards) is often only discussed qualitatively. As a result, practitioners planning multi-robot or multi-domain DT deployments still lack systematic guidance on how to select and compose platforms for different classes of tasks.

**Purpose.** The purpose of this study is to design and apply a unified, task-complexity-aware evaluation framework that compares modern robotics and digital twin simulation platforms including an Unreal Engine 5 based stack; across five representative use cases (UAV inspection, industrial manipulation, warehouse logistics, HCI/VR teleoperation, and general indoor patrol) in terms of physical fidelity, computational performance, and end-to-end digital-twin behaviour.

**Literature review.** Digital twin concepts have been widely adopted in manufacturing, logistics, and cyber-physical systems as a means of coupling high-fidelity virtual models with live data streams from physical assets. Foundational DT literature emphasises lifecycle integration, predictive analytics, and virtual commissioning as key benefits for complex industrial systems, often building on model-based engineering and IoT infrastructures [1–3]. In robotics, DTs are used to support virtual commissioning of robot cells, offline programming, and what-if analysis in flexible manufacturing systems, as well as mission planning and monitoring in domains such as aerospace and agriculture [4–6]. Recent applications include DTs of factories, aircraft production lines, and greenhouse environments, where 3D simulation and data-driven models are combined to evaluate layouts, control strategies, and maintenance regimes before or alongside deployment in the real plant [3,6,7].

A large body of work analyzes and compares robotics simulators as core components of such DT stacks. Quantitative comparisons of CoppeliaSim, Gazebo, MORSE, and Webots reveal that, even for a single mobile platform, the simulators differ substantially in terms of motion accuracy, resource usage, and modeling flexibility [8,9]. Other studies contrast V-REP/CoppeliaSim, Gazebo, ARGoS, and related tools, highlighting trade-offs in physics engines, sensor modelling, ROS integration, and scalability to multi-robot scenarios [10–12]. More recent comparative analyses focus on subsets of platforms (e.g., Webots, CoppeliaSim, and Gazebo) and provide feature-oriented discussions of ease of use, graphical interfaces, and programming support for education and industrial R&D [13,14]. While these works offer valuable guidelines for selecting simulators for specific robot types or tasks, they rarely explicitly model the digital twin layer. Metrics such as telemetry bandwidth, end-to-end latency between the back-end and simulator, or UI responsiveness are seldom included, and human-in-the-loop interaction is generally out of scope.

In parallel, there is growing interest in using game engines and high-fidelity visual platforms such as Unity and Unreal Engine for robotics and DT applications. Comparative studies of digital twins implemented in Unity and Gazebo for robotic arms or agricultural robots report that engines like Unity provide strong real-time rendering capabilities, VR support, and UI tooling. In contrast, Gazebo and similar simulators offer tighter ROS/ROS 2 integration and more mature physics and sensor pipelines for conventional robotics workflows [15–17]. Unity-based VR twins have been demonstrated for domains such as greenhouse monitoring and operator training, and several recent projects use Unreal Engine 5 with Datasmith, Chaos Physics, and custom APIs to build DTs of factories and AEC assets, including integration with external IoT and analytics platforms [7,18–20]. However, these works tend to present single use cases, focus either on visual quality or on integration effort, and seldom provide cross-domain, cross-platform benchmarks that combine physics, performance, and DT-specific metrics. The present study addresses this gap by treating robotics

simulators and a UE5-based stack as first-class DT platforms, evaluated under a unified framework across multiple robot types and interaction modalities.

**Methods.** The study adopts a mixed-methods approach that combines quantitative benchmarks with qualitative expert assessment. Five representative use cases are defined:

- Small UAV – quadrotor with onboard sensors performing waypoint navigation and basic perception.
- Industrial hand robot – 6-DoF manipulator (e.g., UR-type) executing pick-and-place and simple force-sensitive operations.
- Warehouse logistics – a small warehouse cell with conveyors, shelving, and 2–4 mobile robots (AGVs/AMRs).
- HCI interaction – a digital control station with 3D views, VR/AR interface, and interactive widgets for commanding a robot scenario.
- General case – an abstract mobile robot in a structured environment serving as a neutral reference.

For each use case, scenarios are implemented on a selected subset of platforms (e.g., Gazebo/gz-sim, Webots, Isaac Sim/Orbit, CoppeliaSim, and a Unity-based DT stack), using standard robot models and controller implementations as similar as possible. Platforms and configurations:

- Robotics-centric platforms - Gazebo/gz-sim, Webots, Isaac Sim/Orbit, CoppeliaSim.
- Game-engine-centric platform - Unity-based DT environment with ROS/ROS 2 bridge and networked data layer.
- Domain-specific UAV/logistics layers - XTDrone or equivalent PX4–Gazebo setup for UAVs; Isaac Sim warehouse modules for logistics.

All robots are described using URDF or USD (for Isaac), with calibration to ensure comparable masses, inertias, joint limits, and sensor characteristics across platforms. Controllers are implemented using ROS 2 nodes whenever possible, reusing the same trajectory planners and PID parameters, with platform-specific wrappers added only when necessary.

To interpret results coherently across all platforms and use cases, we employ a unified simulation comparison and evaluation framework. The framework treats each scenario as a parametrised experiment defined by a set of inputs (robot model, environment, controller, DT configuration) and a set of outputs (quantitative metrics and qualitative ratings). It explicitly accounts for task complexity and the number of steps in each episode, so that scores from a simple patrol task are not directly compared to those from a dense warehouse scenario without normalisation (Table 1).

*Table 1 – Simulation comparison framework: inputs, outputs, task complexity, and limitations per use\**

Scenario & task profile	Task complexity (qualitative)	Structured steps per episode (high-level phases)	Approx. Control steps per episode*
Small UAV inspection over six masts (300 s mission)	Medium–High (3D flight, multiple targets, continuous control)	1. Pre-flight & take-off; 2. Climb & transit to first mast; 3. Local inspection orbit at each mast; 4. Transit between masts; 5. Return-to-home; 6. Descent & landing	60,000 steps 200 Hz attitude/position control
Industrial hand robot pick-and-place cell (10 picks, 120 s)	High (contact-rich manipulation, conveyor tracking)	1. Initial homing; 2. Part detection; 3. Approach & grasp on moving conveyor; 4. Transfer to tray; 5. Release & retreat; 6. Return to safe pose (looped for 10 parts)	120,000 steps 1 kHz joint control
Warehouse logistics with 2 AMRs and three conveyors (1 h shift)	High (multi-agent navigation, resource contention)	1. Order creation; 2. Task allocation; 3. AMR navigation to rack; 4. Load/unload tote; 5. Packing delivery; 6. Return to idle/charging; 7. Exception handling (blocked path, timeouts)	180,000 steps 50 Hz fleet control (per AMR)

Table 1 (continued)

Scenario & task profile	Task complexity (qualitative)	Structured steps per episode (high-level phases)	Approx. Control steps per episode*
HCI / VR teleoperation of mobile manipulator (20 min session)	Medium–High (human-in-the-loop, VR constraints)	1. Session start & calibration; 2. Robot approach to panel; 3. Visual inspection; 4. Teleoperated valve operations; 5. Retreat & repositioning; 6. Session end	300,000 steps 250 Hz arm control + 50 Hz base control (robot), 108,000 steps 90 Hz HMD/controller tracking
General indoor patrol and docking (15 min episode)	Low–Medium (single robot, structured space)	1. Undock; 2. Patrol along waypoints; 3. Obstacle avoidance; 4. Return to dock; 5. Docking and idle	45,000 steps 50 Hz base control

\* prepared based on the author's work and public research data

**Results.** From an engineering perspective, this gap is a significant issue. Real deployments frequently combine heterogeneous subsystems, for example, small UAVs performing inspection around infrastructure, industrial arms executing manipulation tasks, autonomous mobile robots (AMRs) handling warehouse logistics, and human operators supervising and intervening via rich HMI or VR/AR interfaces. These subsystems share high-level DT requirements, such as reliable synchronisation, low-latency control paths, and scalable telemetry, but place very different demands on physics, sensing, and interaction. Choosing a simulation and digital-twin stack that remains coherent across various use cases requires understanding the trade-offs between physical fidelity, computational load, scalability in multi-robot scenarios, and the quality of operator-facing tools [4, 6, 11, 15].

In this work, we propose a cross-domain evaluation framework for robotics and DT simulation platforms and apply it to five representative use cases: (i) small UAV inspection, (ii) an industrial hand-robot cell, (iii) a warehouse logistics cell with AMRs and conveyors, (iv) HCI/VR-based teleoperation of a mobile manipulator, and (v) a general indoor patrol and docking scenario. The framework standardises inputs (robot and environment profiles, task definitions, digital-twin data contracts) and outputs (physics and task metrics, performance metrics, DT metrics). It introduces explicit descriptors of task complexity in terms of structured phases and control steps per episode. This design allows results to be compared within and across use cases and platforms on a sound basis, rather than only at the level of raw episode success or qualitative judgement (Table 2).

Table 2 – Example UE5 run summary for UC3 (warehouse logistics)\*

Metric	Symbol	Value (example)	Details
Orders completed per hour	$(Q_{\text{orders}})$	47.3 orders/h	Average over $3 \times 1$ h runs
Avg. AMR path length per order	$(L_{\text{path}})$	41.2 m	Pick -> rack -> packing -> idle/charge
Avg. AMR task time per order	$(T_{\text{task}})$	91.5 s	From task assignment to completion
Near-collision events (per hour)	$(N_{\text{nc}})$	2–4	Distances $< 0.5$ m between AMRs or AMR–avatar
Deadlock events are resolved automatically.	$(N_{\text{dl}})$	0–1	Resolved by local priority rules

Table 2 (continued)

Metric	Symbol	Value (example)	Details
Simulation real-time factor (median)	RTF	0.97	1.0 = real time; drops during congestion peaks
Avg. game frame time	( $t_{\text{frame}}$ )	17.8 ms	56 FPS; Chaos async physics enabled
Physics substep time (median)	( $t_{\text{phys}}$ )	1.4 ms	Per physics update at 60 Hz
CPU utilisation (simulation thread)	( $U_{\text{CPU}}$ )	52–68%	Across cores, 65% during peak traffic
GPU utilisation	( $U_{\text{GPU}}$ )	55–72%	With dynamic shadows and NI scenes
DT telemetry data rate	( $R_{\text{DT}}$ )	38 Mbit/s	AMR states, conveyor states, events, and overhead camera
DT round-trip latency (UI command -> AMR reaction)	( $T_{\text{RT}}$ )	68–95 ms	Measured from UI button press to AMR velocity change
Blueprint logic CPU share	—	9–11%	Task assignment, path planning, logging
DT HTTP error rate	—	< 0.1%	Occasional retries on burst loads

\* prepared based on the author's work and public research data

The framework is implemented on several widely used robotics simulators, Gazebo/gz-sim, Webots, NVIDIA Isaac Sim, CoppeliaSim, and on an Unreal Engine 5 (UE5)–based stack. In the UE5 case, 3D assets are imported via Datasmith. Chaos handles physics and vehicle dynamics, while control logic is implemented in Blueprints and Control Rig. DT interfaces are constructed using HTTP/REST plugins and UMG-based operator dashboards, with optional VR/AR front-ends [14, 15]. As a detailed case study, we instantiate the warehouse logistics use case (UC3) as a UE5-based digital twin and report quantitative metrics on order throughput, path lengths, real-time factor, frame times, telemetry bandwidth, and UI-to-actuation latency, alongside qualitative observations regarding Blueprint CPU overhead, navigation scalability, and the impact of visual settings on performance.

The main contributions of the paper are:

1. A unified, use-case-driven evaluation framework for robotics and digital-twin simulation platforms, covering small UAVs, industrial manipulators, warehouse logistics, HCI/VR teleoperation, and general patrol scenarios.
2. A cross-platform comparison that combines physics/task performance, computational metrics, and DT-specific indicators (data rates, latency, error rates), enabling more informed engineering decisions than simulator-only benchmarks.
3. A high-fidelity Unreal Engine 5 warehouse case study with detailed quantitative results, demonstrating how a game-engine-based stack behaves when used as a complete digital-twin platform rather than a pure visualisation layer.

The warehouse logistics use case (UC3) was instantiated as a high-fidelity digital twin in Unreal Engine 5.5, mirroring the logical scenario used across other platforms: two differential-drive AMRs operating in a  $30 \times 20 \times 5$  m warehouse with 24 rack locations, three conveyors, and two packing stations. The scene geometry (racks, building shell, major equipment) was imported via Datasmith from CAD/BIM sources, while smaller props and lighting were authored directly in UE5. AMRs were implemented as Chaos Vehicles with differential-drive configuration, conveyors as kinematic rigid bodies, and navigation meshes were baked-in-engine. Control logic for order handling, task allocation,

and AMR motion was implemented in Blueprints, and a REST/JSON plugin provided bidirectional communication with an external digital twin backend for orders, inventory, and telemetry logging.

Sample JSON payload:

```
{
  "robotId": "AMR_01",
  "timestamp": "2025-12-08T10:15:23.120Z",
  "pose": { "x": 12.4, "y": 5.3, "yaw": 1.57 },
  "taskId": "ORDER_10239",
  "state": "MOVING_TO_RACK",
  "battery": 0.76
}
```

On a representative mid-range workstation (16-core CPU, RTX-class GPU), the UE5 implementation achieved a mean order completion rate of 47.3 orders per hour across three one-hour runs, with an average task time per order of 91.5 seconds and a mean AMR path length of 41.2 meters from assignment to completion. These values are consistent with the scenario's spatial scale and the imposed safety and speed limits, illustrating that a purely UE5-based implementation can achieve practically useful throughput for a small fulfillment cell. Operational safety remained acceptable, with near-collision events (inter-agent spacing below 0.5 m) occurring 2–4 times per hour. Rare deadlocks (0–1 per hour) were resolved by local priority and replanning rules without manual intervention.

From a real-time performance perspective, the UE5 digital twin remained close to real-time under typical loads. The median real-time factor (RTF) across runs was 0.97, with transient dips during periods of dense traffic or heavy visual load. Median game-frame duration was 17.8 ms ( $\approx$ 56 FPS) with asynchronous Chaos physics enabled, and the median physics substep time was 1.4 ms at a 60 Hz physics tick. CPU utilisation on simulation-related threads varied between roughly 52% and 68%, while GPU utilisation typically remained within the range of 55%–72% for the chosen visual settings (dynamic shadows, moderate post-processing). These results indicate that, for the tested scale, the main bottleneck is not the raw physics step but the aggregate of rendering, Blueprint execution, and DT communication.

The digital-twin data pipeline introduced additional but manageable overheads. Aggregated over all AMRs, conveyors, and auxiliary sensors (e.g., an overhead camera), the effective telemetry rate to the DT back end was approximately 38 Mbit/s. Round-trip latency from an operator command in the UE5-based HMI (e.g., pause or reroute an AMR) to a visible change in robot motion remained in the range of 68–95 ms, including UI event handling, HTTP request handling, and the next physics/control step. HTTP error rates were below 0.1%, with occasional retries observed during short-lived bursts when multiple subsystems attempted to push updates concurrently. In practice, these characteristics were sufficient to preserve the responsiveness expected of a supervision-and-intervention interface for warehouse operations, while clearly delineating the latency budget available for more time-critical control loops.

Behaviour-level metrics confirm that the UE5 implementation reproduces the qualitative phenomena expected in a small warehouse cell. As order intensity increases, AMR trajectories become denser and longer, congestion near racks and packing stations rises, and the frequency of near-collision and deadlock events increases correspondingly. The combination of NavMesh-based planning and local priority rules successfully prevented complex deadlocks in nearly all cases, while also exposing the limitations of Blueprint-based planning. Complex path recomputation and repeated collision checks in Blueprint significantly contribute to CPU overhead. They can cause RTF to drop below 1.0 when the environment is heavily cluttered or additional agents are introduced.

Qualitative development experience in UE5 revealed several strengths and weaknesses that are not captured by scalar metrics alone. On the positive side, Datasmith import and the integrated editor significantly reduced the effort required to build a visually consistent and operator-friendly digital twin; UMG-based dashboards and 3D overlays could be iterated rapidly, and Chaos Visual Debugger traces were invaluable for diagnosing intermittent penetration and collision issues. On the negative side, implementing path planning and orchestration logic primarily in Blueprints proved convenient

for prototyping but suboptimal for scaling; offloading planning to C++ modules or external services is clearly advisable for larger fleets. In addition, continuous Chaos Visual Debugger recording over full one-hour episodes was impractical due to storage requirements, suggesting that targeted capture windows are a better strategy for production-like setups.

Overall, the UE5 warehouse case study demonstrates that a game-engine-based stack can function as a complete digital twin platform – handling physics, control logic, DT communication, and rich HMIs—rather than acting solely as a visualisation front-end. At the same time, the quantitative results and observed bottlenecks underscore necessary trade-offs: while UE5 delivers strong rendering quality and interaction capabilities, careful engineering is required to manage CPU/GPU budgets, structure control logic, and design the telemetry pipeline so that real-time factor and latency remain within acceptable bounds as the scale and complexity of the logistics scenario grow. Figure 1 shows the framework of Simulation comparison and evaluation.

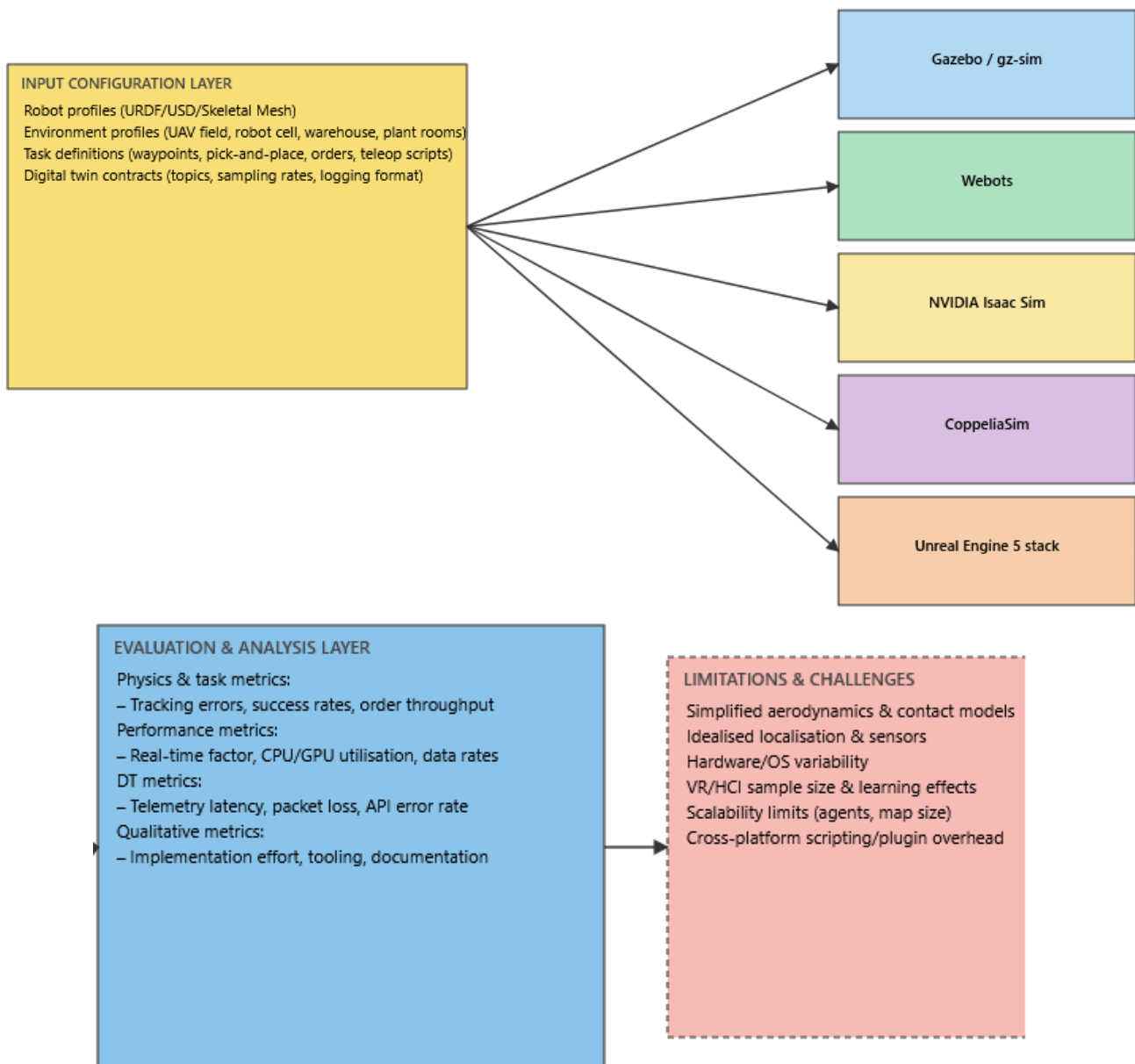


Figure 1 – Simulation comparison and evaluation framework

**Discussion.** Existing comparative works on robotics simulators typically focus on a single robot type and task and evaluate a limited set of platforms. Farley et al. quantitatively compare

CoppeliaSim, Gazebo, MORSE, and Webots for a single mobile robot (Husky A200) navigating to a goal, focusing on motion accuracy and resource usage rather than multi-domain digital-twin aspects. Humanoid-oriented comparisons similarly evaluate a few simulators (Gazebo, Webots, V-REP) on NAO navigation and balance, using metrics such as CPU, memory, and disk access, but without explicit modelling of DT data flows, VR/AR interaction, or cloud connectivity. In contrast, our study spans five heterogeneous use cases (UAV, industrial arm, warehouse logistics, HCI/VR, general patrol) and explicitly couples simulation metrics with digital-twin performance indicators (telemetry data rate, end-to-end latency, DT error rates), making the evaluation directly relevant to integrated cyber-physical systems rather than simulator choice in isolation.

Recent digital-twin papers comparing Unity and Gazebo focus on one or two application scenarios, such as a robotic arm workcell or a tomato greenhouse robot, and emphasize visual fidelity, ROS/ROS 2 integration effort, and development productivity. These studies provide detailed qualitative feedback and some timing measurements but treat the DT layer primarily as a synchronised 3D replica. Our results partially agree with their findings; for example, game engines and high-end visual stacks indeed excel in rendering, UI, and VR integration. Yet we extend the analysis by: (i) quantifying task-level performance (throughput, success rates) across warehouse and UAV scenarios, (ii) normalising metrics by control steps and episode structure, and (iii) systematically measuring the DT data pipeline (Mbit/s, HTTP error rate, UI-to-actuation latency). This reveals trade-offs that are less apparent in prior Unity–Gazebo comparisons, such as how path-planning load and telemetry volume jointly impact real-time factor and DT responsiveness in dense logistics scenes. Figure 2 illustrates the UE5 warehouse logistics digital twin, including the scenario flow and key metrics.

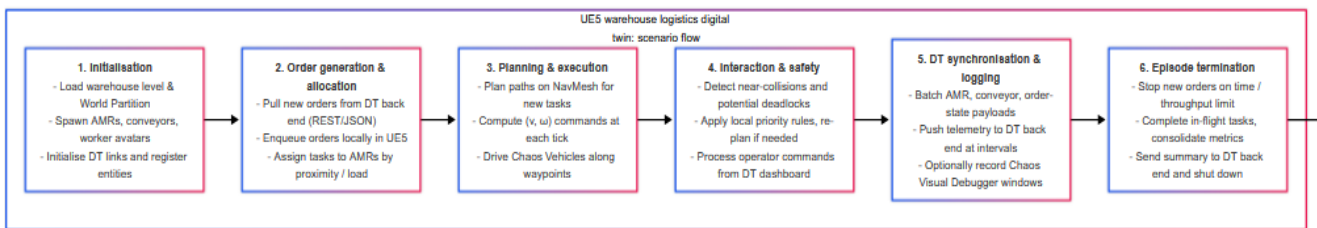


Figure 2 – UE5 warehouse logistics digital twin: scenario flow and key metrics

Benchmarking frameworks like RoboEval, “robot-simulator comparison” testbeds, and recent sim-to-real evaluation schemes focus primarily on policy evaluation and reality gap metrics (task success, fine-grained manipulation scores, sim-to-real correlation coefficients). Our framework is complementary: it does not directly address sim-to-real transfer in this article, but instead treats simulators and digital twin stacks as first-class objects of evaluation. We introduce explicit decomposition into inputs (robot models, environments, controllers, and DT contracts), outputs (physics, performance, and DT metrics), and task complexity descriptors (the number of structured phases and control steps). This leads to a more engineering-oriented selection matrix: rather than asking “which simulator maximises policy success?”, we ask “which stack offers acceptable fidelity and DT latency for a given class of UAV, manipulation, logistics, or HCI tasks under specific computational constraints?”

Finally, compared to existing digital-twin case studies in aviation and extensive infrastructure, where Unity or Unreal-based twins are often reported qualitatively as enablers of operational awareness and predictive maintenance at airports and terminals, our Unreal Engine 5 warehouse case study provides quantitative, reproducible measurements at the simulation level. The UE5 results explicitly report order throughput, near-collision rates, real-time factor, frame times, and DT round-trip latency within a controlled warehouse scenario, rather than focusing solely on visualisation benefits. Together with the multi-platform comparisons, this positions our work as a bridge between DT success stories and low-level simulator benchmarks, highlighting not only where game-engine-based twins outperform classical robotics simulators (e.g., VR/HCI, UI richness), but also where they

encounter scalability and CPU/Blueprint bottlenecks when used as full-stack robotics and logistics simulators.

Despite these benefits, practical implementation challenges remain. Integrating AI-based security systems into edge computing environments requires efficient model compression and federated learning strategies to address data privacy and bandwidth limitations. Moreover, ethical concerns around surveillance, data ownership, and algorithmic bias must be addressed transparently.

**Conclusions.** From an applied perspective, the proposed framework and UE5 warehouse case study can also serve as a design checklist for practitioners planning or refactoring digital twin stacks in robotics and automation. By forcing a clear separation between input configurations, platform-specific implementations, and evaluation/analysis outputs, the framework makes it easier to reason about where complexity and risk are concentrated—whether in physics fidelity, in multi-robot coordination logic, or in the DT data pipeline and HMI. The concrete metrics we report (e.g., throughput, real-time factor, telemetry bandwidth, UI-to-actuation latency) provide realistic target ranges and stress points that can guide early architecture choices, hardware provisioning, and performance budgeting. In this sense, the work not only benchmarks simulators and DT platforms but also offers a reusable blueprint for structuring future comparative studies and for building robust, scalable digital twins in UAV, industrial, logistics, and HCI-centric domains.

A key limitation of this research is that, despite covering five heterogeneous use cases and several major platforms (including UE5), the evaluation remains constrained by specific hardware, software versions, and scenario parameterizations. Real-world deployments may use different robot models, controllers, network conditions, and DT architectures, which can shift performance rankings and expose additional bottlenecks. The study also relies on simplified physics and sensor models (e.g., approximate aerodynamics, contact and friction models, idealized localization), which restrict the extent to which absolute values of tracking error or throughput can be interpreted as proxies for real-world behaviour. Human-in-the-loop results (especially those involving VR/HCI) are further limited by small sample sizes and operator learning effects, making the usability findings indicative rather than statistically conclusive. Finally, we have not yet conducted a systematic sim-to-real transfer analysis, so the link between simulator/DT metrics and real-world deployment quality remains indirect.

Future work will therefore focus on three directions: (i) extending the benchmark suite with larger and more diverse use cases (e.g., outdoor mobile manipulation, multi-floor logistics, human-robot collaboration cells) and additional platforms, including cloud-native DT stacks; (ii) tightening the connection to sim-to-real studies, by running paired experiments on simulated and physical systems and correlating framework metrics (e.g., task complexity-normalised errors, DT latency) with real-world performance and safety indicators; and (iii) developing automated configuration and profiling tools that can generate, run, and analyse benchmark scenarios across platforms with minimal manual intervention. This should enable broader community adoption of the framework, more reproducible cross-platform comparisons, and the progressive refinement of best-practice guidelines for selecting and composing robotics and digital twin simulation stacks.

## References

1. Ariesen-Verschuur, N., Verdouw, C., & Tekinerdogan, B. (2022). Digital twins in greenhouse horticulture: A review. *Computers and Electronics in Agriculture*, 199, Article 107183. <https://doi.org/10.1016/j.compag.2022.107183>.
2. Baratta, A., Cimino, A., Longo, F., & Nicoletti, L. (2024). Digital twin for human-robot collaboration enhancement in manufacturing systems: Literature review and direction for future developments. *Computers & Industrial Engineering*, 187, Article 109764. <https://doi.org/10.1016/j.cie.2023.109764>.
3. Davila, M. F., Schwark, F., Dawel, L., & Pehlken, A. (2023). Sustainability digital twin: A tool for the manufacturing industry. *Procedia CIRP*, 116, 143–148. <https://doi.org/10.1016/j.procir.2023.02.025>.

4. Glaessgen, E. H., & Stargel, D. S. (2012, April). The digital twin paradigm for future NASA and U.S. Air Force vehicles. In 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference (Paper 2012-1818). <https://doi.org/10.2514/6.2012-1818>.
5. Grieves, M. (2014). Digital twin: Manufacturing excellence through virtual factory replication [White paper]. Florida Institute of Technology.
6. He, B., & Bai, K.-J. (2021). Digital twin-based sustainable intelligent manufacturing: A review. *Advances in Manufacturing*, 9, 1–21. <https://doi.org/10.1007/s40436-020-00302-5>.
7. Huang, C., Luo, W., Yang, C., & Li, X. (2021). A survey on AI-driven digital twins in Industry 4.0: Smart manufacturing and advanced robotics. *Sensors*, 21(19), Article 6340. <https://doi.org/10.3390/s21196340>.
8. Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, 51(11), 1016–1022. <https://doi.org/10.1016/j.ifacol.2018.08.474>.
9. Lim, K. Y. H., Zheng, P., & Chen, C.-H. (2020). A state-of-the-art survey of digital twin: Techniques, engineering product lifecycle management and business innovation perspectives. *Journal of Intelligent Manufacturing*, 31, 1313–1337. <https://doi.org/10.1007/s10845-019-01512-w>.
10. Lu, Y., Liu, C., Wang, K. I.-K., Huang, H., & Xu, X. (2020). Digital twin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robotics and Computer-Integrated Manufacturing*, 61, Article 101837. <https://doi.org/10.1016/j.rcim.2019.101837>.
11. Pylianidis, C., Osinga, S., & Athanasiadis, I. N. (2021). Introducing digital twins to agriculture. *Computers and Electronics in Agriculture*, 184, Article 105942. <https://doi.org/10.1016/j.compag.2020.105942>.
12. Qi, Q., Tao, F., Hu, T., Anwer, N., Liu, A., Wei, Y., Wang, L., Nee, A. Y. C., & Zhong, R. Y. (2021). Enabling technologies and tools for digital twin. *Journal of Manufacturing Systems*, 58, 3–21. <https://doi.org/10.1016/j.jmsy.2019.10.001>.
13. Alam, K. M., & El Saddik, A. (2017). C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems. *IEEE Access*, 5, 2050–2068. <https://doi.org/10.1109/ACCESS.2017.2657006>.
14. Farley, A., Wang, J., & Marshall, J. A. (2022). How to pick a mobile robot simulator: A quantitative comparison of CoppeliaSim, Gazebo, MORSE and Webots with a focus on accuracy of motion. *Simulation Modelling Practice and Theory*, 120, Article 102629. <https://doi.org/10.1016/j.simpat.2022.102629>.
15. Koenig, N., & Howard, A. (2004). Design and use paradigms for Gazebo, an open-source multi-robot simulator. In *Proceedings of the 2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (pp. 2149–2154). <https://doi.org/10.1109/IROS.2004.1389727>.
16. Freese, M., Singh, S., Ozaki, F., & Matsuhira, N. (2010, November). Virtual robot experimentation platform V-REP: A versatile 3D robot simulator. In *International Conference on Simulation, Modeling, and Programming for Autonomous Robots* (pp. 51–62). Springer. [https://doi.org/10.1007/978-3-642-17319-6\\_5](https://doi.org/10.1007/978-3-642-17319-6_5).
17. Michel, O. (2004). Webots: Professional mobile robot simulation. *International Journal of Advanced Robotic Systems*, 1(1), 39–42. <https://doi.org/10.5772/5618>.
18. Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., Wheeler, R., & Ng, A. Y. (2009). ROS: An open-source robot operating system. In *ICRA Workshop on Open Source Software* (Vol. 3, No. 3.2). <https://www.ros.org>.
19. Microsoft. (2020). AirSim: High-fidelity simulator for autonomous vehicles (Version 1.7) [Computer software]. GitHub. <https://github.com/microsoft/AirSim>.
20. Project AirSim Team. (2023). Project AirSim: Simulation platform for drones, robots, and autonomous systems on Unreal Engine 5 [Computer software]. Microsoft. <https://projectairsim.github.io/ProjectAirSim/>.

21. Epic Games. (2025). Digital twins. Unreal Engine. <https://www.unrealengine.com/en-US/digital-twins>.
22. Implexus Lab. (2024). HMI for an industrial facility digital twin with UE5 [Conference talk and blog post]. Unreal Fest 2024 / Implexus Lab. <https://www.implexuslab.com/post/hmi-for-an-industrial-facility-digital-twin-with-ue5>.
23. Epic Games. (2024). Let's train virtual robots [Lesson plan]. Unreal Engine Learning Portal. <https://www.unrealengine.com/en-US/lesson-plans/let-s-train-virtual-robots>.
24. MathWorks. (2024). Unreal Engine simulation for robots [Documentation]. MathWorks. <https://www.mathworks.com/help/robotics/ug/3d-simulation-for-robots.html>.
25. SAS Institute. (2025). SAS digital twins on Unreal Engine transform manufacturing. Times of India – Business Technology. <https://timesofindia.indiatimes.com/business/india-business/sas-digital-twins-on-unreal-engine-transform-manufacturing/articleshow/>.

### **Назаренко Володимир Анатолійович**

доктор філософії, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,  
Національний університет біоресурсів і природокористування України

ORCID: <https://orcid.org/0000-0002-7433-2484>

E-mail: [volodnz@nubip.edu.ua](mailto:volodnz@nubip.edu.ua)

### **Остроушко Богдан Павлович**

асистент кафедри комп'ютерних систем, мереж та кібербезпеки,  
Національний університет біоресурсів і природокористування України

ORCID: <https://orcid.org/0009-0003-0849-8990>

E-mail: [b.ostroushko@nubip.edu.ua](mailto:b.ostroushko@nubip.edu.ua)

## **ВІРТУАЛЬНА СИСТЕМА МОДЕЛЮВАННЯ ДЛЯ РОБОТОТЕХНІКИ ТА ПЛАТФОРМ СИМУЛЯЦІЇ ЦИФРОВИХ ДВІЙНИКІВ З ПРИКЛАДОМ СКЛАДСЬКОЇ СИСТЕМИ В UNREAL ENGINE 5**

***Анотація.** Цифрові двійники та високоякісні симулятори стають центральними для проектування, тестування та експлуатації сучасних робототехнічних систем у промисловості, логістиці та взаємодії людини з роботами. Однак, існуючі порівняльні дослідження зазвичай зосереджуються на одному типі роботів, однотипних завданнях або симуляторі та рідко враховують специфічні для цифрових двійників аспекти, такі як телеметричні конвеєри, інтерфейси операторів або хмарне підключення. У цій статті пропонується уніфікована система оцінки для цифрових двійників, орієнтованих на робототехніку. Проведене дослідження застосовується до п'яти репрезентативних випадків використання: 1 – малі БПЛА, 2 – промисловий робот маніпулятор, 3 – логістична ячейка складу з автономними мобільними роботами (AMR), 4 – мобільний маніпулятор на основі HSI/VR, і 5 – загальний сценарій патрулювання та стикування у приміщенні.*

*Фреймворк стандартизує вхідні дані (профілі роботів і середовища, визначення завдань, контракти даних цифрових двійників) та вихідні дані (метрики завдань і продуктивності та метрики DT), а також кодує складність завдань через структуровані фази та кроки керування на кожен конкретний епізод. Він реалізований на кількох робототехнічних симуляторах, що на сьогодні широко використовуються, а саме: Gazebo/gz-sim, Webots, NVIDIA Isaac Sim, CoppeliaSim, та на стеку на базі Unreal Engine 5 (UE5), який поєднує імпорт активів Datasmith, Chaos Physics, Blueprints/Control Rig та інтерфейсу UMG/VR.*

*Як детальне кейс-стаді, в роботі автори втілюють логістичний приклад використання складу як цифрового двійника на базі UE5 та демонструють кількісні результати щодо пропускної здатності замовлень, довжини шляхів, коефіцієнта реального часу, часу кадру, пропускної здатності телеметрії та затримки UI до спрацьовування. Також проаналізовано технічні недоліки, такі як накладні витрати процесора Blueprint і уповільнення, викликані візуальним навантаженням. На всіх платформах і кейсах використання результатів дослідження демонструє компроміси між фізичною точністю, масштабованістю, багатогранністю взаємодії та чутливістю DT, а також призводять до практичних рекомендацій щодо вибору та композиції симуляційних і цифрових стеків для БПЛА, маніпуляцій, логістики та HSI-центричних застосувань.*

*Стаття завершується обговоренням обмежень, зокрема спрощення симуляції та апаратної залежності, а також окреслює майбутні кроки до кореляції симулятора до реального та автоматизованого benchmarking.*

***Ключові слова:** цифровий двійник, робототехніка, Unreal Engine 5, Gazebo, Webots, NVIDIA Isaac Sim, CoppeliaSim, автоматизація логістичних задач, симуляція БПЛА, промисловий робот, VR/AR управління, розумна система.*

UDC 004.056.53:510.644

**Лакно Валерій Анатолійович**

*доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки,*

*Національний університет біоресурсів і природокористування України*

ORCID: <http://orcid.org/0000-0001-9695-4543>

E-mail: [lva964@nubip.edu.ua](mailto:lva964@nubip.edu.ua)

**Касаткін Дмитро Юрійович**

*кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,*

*Національний університет біоресурсів і природокористування України*

ORCID: <https://orcid.org/0000-0002-2642-8908>

E-mail: [d.kasatkin@nubip.edu.ua](mailto:d.kasatkin@nubip.edu.ua)

## НЕЧІТКО-ЛОГІЧНА МОДЕЛЬ ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІД ЧАС DDoS-АТАК

***Анотація.** Запропоновано нечітко-логічну модель оцінювання стану інформаційної системи (ІС) під час DDoS-атак. Модель базується на використанні системи лінгвістичних змінних, які описують критичні параметри мережевого трафіку та характеристик функціонування ІС. Для формування оцінки поточного ризику застосовано нечіткий висновок типу Мамдані з подальшою дефазифікацією методом центра ваги. Проведено імітаційний експеримент, який реалізовано у середовищі Python із використанням бібліотеки scikit-fuzzy. Отримані результати підтвердили, що запропонована модель адекватно відображає залежність інтегрального ризику від зміни параметрів навантаження, забезпечує безперервність оцінювання та чутливість до критичних комбінацій факторів трафіку. Отримані результати дають підставу розглядати розроблену модель як базис синтезу модуля моніторингу стану ІС.*

***Ключові слова:** DDoS-атака, нечітка логіка, модель ризику, інформаційна система, нечіткий висновок Мамдані, оцінювання стану, моніторинг безпеки.*

**Вступ.** Під час функціонування корпоративних інформаційних систем (ІС) з високим рівнем інтеграції та навантаженням виникає потреба у безперервному контролі їхнього технічного та інформаційного стану. Також виникає завдання виявлення і оцінювання наслідків DDoS-атак, коли потік запитів формується з великої кількості джерел, а класичні сигнатурні та порогові методи не дають можливостей своєчасно розпізнати перехід системи до критичного стану [1, 2]. У подібних умовах стандартні метрики продуктивності або ізольовані показники безпеки не відображають реального ступеня деградації системи, оскільки мають нечіткі границі між нормальними та атиповими режимами. Практичний досвід експлуатації мережевої інфраструктури показав, що поведінка ІС під навантаженням DDoS-типу описується не лише кількісними параметрами трафіку. Її також описують якісними співвідношеннями між показниками, а саме інтенсивністю запитів, пропускну здатністю каналів, часткою втрат пакетів, затримками обробки транзакцій тощо [3, 4]. Зміна навіть одного з цих факторів може не мати суттєвого впливу на ІС. Проте їх комбінація створить ситуацію, коли система втратить стійкість до подальшого навантаження. Подібні залежності складно формалізувати аналітично. Але вони піддаються опису засобами нечіткої логіки [5]. Використання нечітко-логічного підходу для оцінювання стану ІС під час DDoS-атак дасть змогу інтегрувати різноманітні параметри у єдину узагальнену оцінку ризику. На відміну від детермінованих методів, нечітка модель дозволить врахувати неповноту та неточність вхідних даних, а також суб'єктивні експертні знання, отримані з практики адміністрування систем захисту.

Саме тому, у даній роботі запропоновано нечітко-логічну модель оцінювання стану інформаційної системи під час DDoS-атак. Модель базується на сукупності лінгвістичних

змінних, що відображають параметри мережевого трафіку та внутрішніх процесів обробки даних. Результатом є інтегрована оцінка ризику порушення працездатності ІС.

**Постановка проблеми.** Інформаційні системи (ІС) постійно стикаються із ситуацією, коли мережеві потоки та інтенсивність запитів постійно змінюється. А під час DDoS-атак ІС опиняються в умовах перевантаження. Проблема полягає у відсутності інтегрованих моделей, здатних оцінювати поточний стан ІС за множиною взаємопов'язаних параметрів трафіку та внутрішніх характеристик системи з урахуванням нечітких меж між нормальним і критичним станом ІС. Отже виникає потреба синтезу моделі оцінювання поточного стану ІС на основі системи нечітких правил.

**Аналіз актуальних досліджень.** Аналіз наукових джерел засвідчив зростання інтересу до використання методів нечіткої логіки для виявлення та нейтралізації DDoS-атак. Зокрема у статтях [1, 2] систематизовано методи виявлення DDoS-атак у високошвидкісних мережах. Автори наголосили, що сигнатурні та статистичні підходи поступаються за ефективністю інтелектуальним методам аналізу, зокрема заснованим на нечітких моделях прийняття рішень.

Перші практичні підходи до застосування нечіткої логіки у задачі виявлення DDoS-атак розглянуто у дослідженні Shiaeles S. N. та ін. [3]. Автори реалізували систему на основі нечітких оцінювачів трафіку й довели придатність нечітких правил для ідентифікації відхилень у мережевих потоках. Подальший розвиток цього напрямку представлено у роботі [4]. Автори розробили метод виявлення та відновлення роботи бездротових сенсорних мереж із використанням нечітких параметрів, які характеризували інтенсивність DDoS атак.

Вагомий внесок у систематизацію методів нечіткої логіки при виявленні DDoS атак зробили Javaheri D. зі співавторами у [5]. В цих роботах автори виконали порівняльний аналіз сучасних моделей виявлення аномалій трафіку та класифікацію підходів на основі типу нечіткого висновку. Автори підкреслили, що, нечіткі системи демонстрували під час досліджень стійкість до змін характеристик мережевого середовища та забезпечували гнучке налаштування параметрів оцінювання працездатності мережі. У [6] Almseidin M. та інші співавтори колеги запропонували нечітку систему висновку для виявлення DDoS-атак. Система базувалася на інтеграції вхідних метрик трафіку, а отримані результати підтвердили ефективність нечіткого висновку для підвищення точності детекції при низькому рівні хибнопозитивних спрацьовувань системи нечіткого висновку.

У [7] Petković M. та інші співавтори досліджували ефективність нечіткого методу Такегі–Сугено–Канг (TSK) у поєднанні з моделлю оцінювання ентропії трафіку. Автори довели, що запропонований у статті метод забезпечив високу чутливість до низько інтенсивних DDoS атак порівняно з традиційними статистичними методами.

Lin H., Wu C., та Masdari M. у [8] узагальнили релевантні схеми виявлення аномалій. Автори наголосили на доцільності застосування гібридних методів виявлення DDoS атак. Зокрема методів та моделей, у яких нечітка логіка поєднувалася з машинним навчанням для зменшення похибки класифікації.

Інтеграційні рішення для виявлення DDoS атак розглянуті у роботах [9, 10]. У статтях автори використовували апарат нечіткої логіки як керуючий модуль для системи класифікаторів у середовищі Apache Spark. Додатково у [9] Almotiri S. H. представив нечітку модель кількісного оцінювання стійкості мережі до DDoS-атак на основі методу TOPSIS.

Загалом проведений аналіз засвідчує, що використання нечіткої логіки у завданнях виявлення та оцінювання стану інформаційних систем під час DDoS-атак забезпечує підвищення точності та стійкості механізмів захисту. Проте, більшість проаналізованих досліджень зосереджена на задачах детекції, тоді як питання формалізації нечітко-логічних моделей оцінювання поточного стану інформаційних систем під час DDoS атак залишилися недостатньо розробленими, що визначило актуальність подальших досліджень у цьому напрямі.

**Метою статті** є розробка та апробація нечітко-логічної моделі оцінювання стану ІС під час DDoS-атак, яка забезпечує інтегроване відображення впливу основних параметрів мережевого трафіку та характеристик продуктивності системи на її поточний рівень ризику.

**Матеріали і методи дослідження.** Метою побудови моделі є формування інтегрованої оцінки поточного стану ІС під час дії DDoS-атак з урахуванням параметрів трафіку, характеристик мережевого середовища та показників деградації продуктивності. Для цього запропоновано використати нечітко-логічний підхід, який дозволить формалізувати експертні знання про залежності між множиною факторів та якісною оцінкою стану ІС.

Як вхідні дані моделі використовуємо часткові параметри стану ІС, які характеризують потік запитів, поведінку мережевих протоколів, пропускну здатність каналів ІС, затримки обробки та інші індикатори, які реагують на DDoS-навантаження. Для кожного параметра визначено універсум значень та відповідні лінгвістичні терми, наведені у табл. 1.

Таблиця 1 – База нечітких правил типу Мамдані для оцінювання поточного стану ІС під час дії DDoS-атак з урахуванням параметрів трафіку

Позначення	Опис параметра	Універсум	Лінгвістичні терми
$y_1$	Показник поточних ризиків	[0,1]	некритична (нкр), критична (кр)
$y_2$	Прийнятний рівень інформаційного ризику	[0,1]	прийнятний (пр), неприйнятний (нп)
$y_3$	Інтенсивність потоку кадрів (запитів)	[10,6000] кадр/с	немає (н), незначна (нк), середня (ск), велика (вк)
$y_4$	Пропускна спроможність каналу	[10,100] Мбіт/с	низька (нпс), середня (спс), висока (впс)
$y_5$	Кількість спроб доступу до середовища	[0,1]	зафіксовані (зф), незафіксовані (нф)
$y_6$	Час очікування обслуговування транзакції	[0.001, 0.01] с	неприйнятний (нп), середній (сп), нормальний (н)
$y_7$	Довжина IP-паketу	[1,65529] байт	низька (н), нижче критичної (нкр), критична (кр), вище критичної (вкр)
$y_8$	Кількість великих IP-паketів (Ping of Death)	[0,1]	мала (м), середня (с), велика (в)
$y_9$	Кількість HTTP-запитів	[0,1]	мала (м), середня (с), велика (в)
$y_{10}$	Частка TCP-паketів	[0,1]	мала (м), середня (с), велика (в)
$y_{11}$	Частка UDP-паketів	[0,1]	мала (м), середня (с), велика (в)
$y_{12}$	Частка ICMP-паketів	[0,1]	мала (м), середня (с), велика (в)
$y_{13}$	Ознаки SQL-ін'єкції	[0,1]	виявлені (в), частково виявлені (чв), невиявлені (нв)
$y_{14}$	Міжкадровий інтервал	[10,100] біт	малий (м), середній (с), великий (в)

Для кожного терма  $T_i$  визначаємо функцію належності  $\mu_{T_i}(y_i)$ , яка відобразить ступінь, з яким значення параметра ( $y_i$ ) відповідатиме відповідному лінгвістичному опису. Як

базові типи функцій належності використовуємо трикутні та трапецієподібні функції, що забезпечать інтерпретованість та простоту обчислень.

Нечітко-логічна модель сформує оцінку ( $Y^*$ ) поточного стану ІС на основі системи правил виду:

$R_k$ : якщо  $y_3$  є велика та  $y_6$  є неприйнятний, то  $Y^*$  є критичний.

Загальну систему нечітких рівнянь, що відповідають дереву висновку, подамо у вигляді:

$$\mu_{Y^*}(x) = \max_k \min_i \mu_{T_i}(y_i),$$

де  $\mu_{T_i}(y_i)$  – функції належності вхідних змінних до відповідних термів;

операції ( $\max_k$ ) та ( $\min_i$ ) відповідають логічним операціям **АБО** та **І** у системі нечіткого висновку типу Мамдані [11].

У процесі дефазифікації для отримання числової оцінки рівня ризику застосовувався метод центра ваги [8]:

$$Y^* = \frac{\int x \cdot \mu_{Y^*}(x) dx}{\int \mu_{Y^*}(x) dx}.$$

Результат ( $Y^*$ ) інтерпретуємо як ступінь критичності стану ІС у діапазоні [0,1]. Значення, близькі до 0, відповідають нормальному режиму. Значення, близькі до 1, відповідно, критичному стану внаслідок DDoS-навантаження.

Базу правил сформовано експертним шляхом на основі практичних спостережень поведінки ІС під час атак. Типові приклади правил:

- якщо інтенсивність запитів велика і час обслуговування неприйнятний – то стан системи критичний;
- якщо пропускна спроможність висока і інтенсивність кадрів середня – то стан системи нормальний;
- якщо кількість ICMP-пакетів велика і міжкадровий інтервал малий – то система перебуває у потенційно небезпечному стані.

Отже, модель надала змогу об'єднати різномірні показники в єдину метрику ризику, яка характеризувала реальний стан ІС у момент часу ( $t$ ).

**Результати дослідження та їх обговорення.** Для оцінювання працездатності запропонованої нечітко-логічної моделі проведено імітаційний експеримент (рис. 1 і рис. 2), спрямований на дослідження поведінки оцінки стану ІС під час зміни основних параметрів DDoS-навантаження. Експеримент реалізовано у середовищі Python (Google Colab) з використанням бібліотеки scikit-fuzzy, яка забезпечила реалізацію бази правил типу Мамдані та процедуру дефазифікації методом центру ваги.

У моделі використовувались дві вхідні змінні – інтенсивність запитів ( $y_3$ ) та затримка обслуговування транзакцій ( $y_6$ ), а також одна вихідна змінна – інтегральний рівень ризику ( $Y^*$ ), який відображав узагальнений стан ІС у діапазоні [0,1]. Вибір саме цих параметрів зумовлений тим, що в реальних умовах саме вони мають найбільший вплив на деградацію продуктивності ІС.

Для кожної змінної побудовано набір функцій належності трикутного або трапецієподібного типу. Це забезпечило просту інтерпретацію експертних знань. Зокрема, інтенсивність трафіку описано трьома термами – «низька», «середня» і «висока»; затримка – «нормальна», «середня», «критична»; рівень ризику – «нормальний», «підвищений», «критичний». Базу правил сформовано таким чином, щоб відобразити типові залежності між параметрами мережевого навантаження та станом системи.

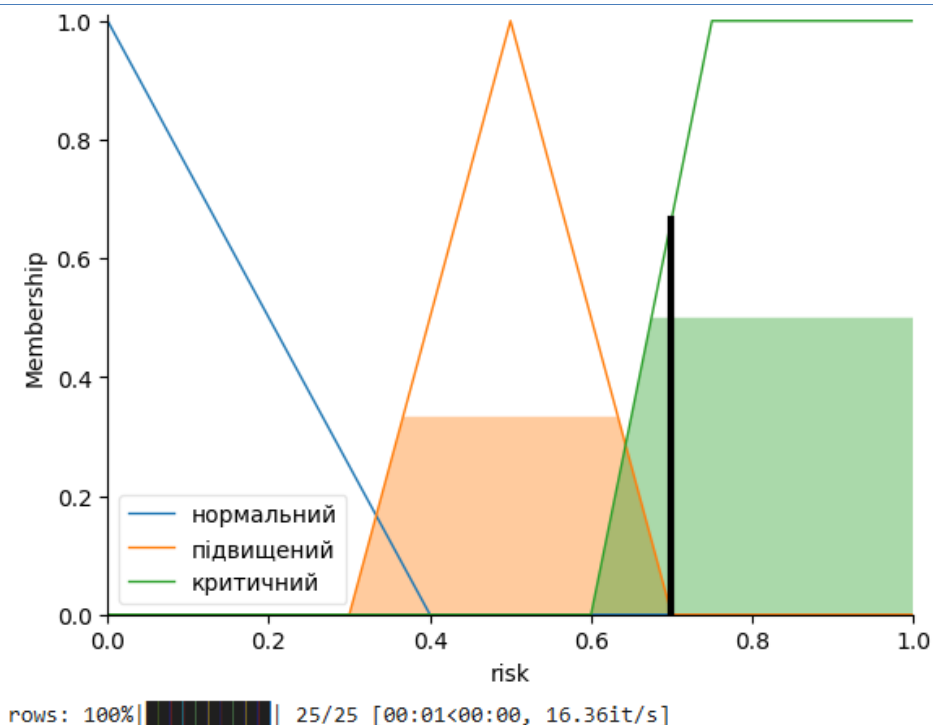


Рисунок 1 – Оцінка стану ризику

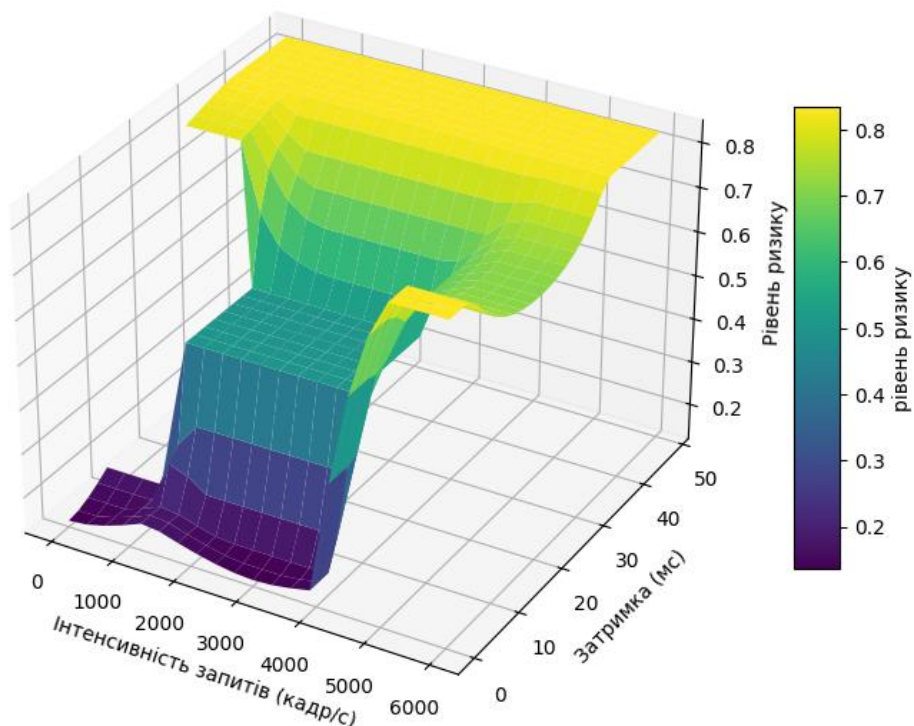


Рисунок 2 – Оцінка стану ризику у вигляді поверхні

Під час моделювання проведено дискретне сканування простору вхідних параметрів у діапазонах [0, 6000] кадр/с для трафіку та [0, 50] мс для затримки. Для кожної комбінації значень обчислювалась відповідна величина ризику ( $Y^*$ ). Отримані результати подано у вигляді поверхні нечіткого висновку, яка характеризує залежність рівня ризику від обох вхідних параметрів. Аналіз поверхні показав, що модель демонструє плавну зміну

інтегральної оцінки при зростанні навантаження та затримки, без різких стрибків, що свідчить про коректну роботу процедури нечіткого висновку.

Типова точка експерименту, що відповідає інтенсивності запитів 4200 кадр/с і затримці 30 мс, дала значення інтегрального ризику ( $Y^* = 0,76$ ). Це відповідало критичному стану системи, коли ресурси серверів близькі до вичерпання, а затримка обробки транзакцій перевищує прийнятні межі. У діапазоні середніх навантажень (2000–3000 кадр/с) ризик залишається у межах 0,4–0,55. При низьких інтенсивностях і коротких затримках (до 1000 кадр/с, <10 мс) оцінка ризику стабільно не перевищує 0,2. А отже ІС система функціонує у нормальному режимі. Результати імітаційного експерименту підтверджують, що запропонована нечітко-логічна модель адекватно відображає залежність інтегрального ризику від мережеских параметрів, забезпечує безперервність оцінювання та стійкість до варіацій вхідних даних. Це дозволяє розглядати її як основу для побудови модуля моніторингу стану ІС у режимі реального часу.

Вважаємо, що подальші дослідження доцільно спрямувати на розширення бази правил з урахуванням характеристик різних типів атак (UDP flood, HTTP flood, ICMP flood), а також на інтеграцію нечітко-логічного ядра з алгоритмами машинного навчання для автоматичного коригування функцій належності залежно від поточних даних моніторингу ІС.

**Висновки.** Запропоновано нечітко-логічну модель оцінювання стану інформаційної системи під час DDoS-атак, що дозволило формалізувати залежність між параметрами мережевого трафіку, затримками обслуговування транзакцій та інтегральним рівнем ризику. Основні результати дослідження можна узагальнити так. Розроблено систему лінгвістичних змінних, що описують критичні характеристики ІС під час DDoS-навантаження, зокрема інтенсивність запитів, пропускну здатність каналів, затримку обслуговування, частку протокольних пакетів та інші індикатори аномалій. Сформовано базу нечітких правил типу Мамдані, що відображає експертні знання про вплив комбінацій параметрів на стан ІС. Проведено імітаційний експеримент, який підтвердив адекватність запропонованої моделі. Продемонстровано плавний характер зміни інтегрального ризику залежно від інтенсивності навантаження та затримки обробки, без різких стрибків і розривів у результатах. Встановлено критичні області функціонування ІС, у яких поєднання високої інтенсивності запитів і збільшення затримки призводило до переходу системи у нестійкий стан. Отримані значення ризику добре узгоджуються з реальною поведінкою корпоративних ІС під час DDoS-інцидентів. Практична значущість моделі полягає у потенціалі її інтеграції до систем моніторингу безпеки як модуля оцінювання стану ІС у реальному часі.

### Список використаних джерел

1. Savchenko, V., Ponochovnyi, P., & Averichev, I. (2024). Vyivlennia DDoS-atomy na vysokoshvydkisnu merezhu: Opytuvannia [Detection of a DDoS attack on a high-speed network: A survey]. *Prykladni Problemy Kompiuternykh Nauk, Bezpeky ta Matematyky* [Applied Problems of Computer Science, Security and Mathematics], 3, 71–81.
2. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., & Petrenko, T. (2024). Nechitki kohnityvni karty yak instrument vizualizatsii stsenariiiv reahuvannia na intsydenty v systemakh bezpeky [Fuzzy cognitive maps as a tool for visualizing incident response scenarios in security systems]. *Kiberbezpeka: Osvita, Nauka, Tekhnika* [Cybersecurity: Education, Science, Technique], 2(26), 417–429. <https://doi.org/10.28925/2663-4023.2024.26.707>.
3. Shiaeles, S. N., Katos, V., Karakos, A. S., & Papadopoulos, B. K. (2012). Real time DDoS detection using fuzzy estimators. *Computers & Security*, 31(6), 782–790. <https://doi.org/10.1016/j.cose.2012.06.002>.
4. Pajila, P. B., Julie, E. G., & Robinson, Y. H. (2022). FBDR-fuzzy based DDoS attack detection and recovery mechanism for wireless sensor networks. *Wireless Personal Communications*, 122(4), 3053–3083. <https://doi.org/10.21203/rs.3.rs-217674/v1>.

5. Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*, 626, 315–338. <https://doi.org/10.1016/j.ins.2023.01.067>.
6. Almseidin, M., Al-Sawwa, J., Alkasassbeh, M., & Alweshah, M. (2023). On detecting distributed denial of service attacks using fuzzy inference system. *Cluster Computing*, 26(2), 1337–1351. <https://doi.org/10.1007/s10586-022-03657-5>.
7. Petković, M., Bašičević, I., Kukulj, D., & Popović, M. (2018). Evaluation of Takagi-Sugeno-Kang fuzzy method in entropy-based detection of DDoS attacks. *Computer Science and Information Systems*, 15(1), 139–162. <https://doi.org/10.2298/CSIS160905039P>.
8. Lin, H., Wu, C., & Masdari, M. (2022). A comprehensive survey of network traffic anomalies and DDoS attacks detection schemes using fuzzy techniques. *Computers and Electrical Engineering*, 104, 108466. <https://doi.org/10.1016/j.compeleceng.2022.108466>.
9. Almotiri, S. H. (2024). Improving network resilience against DDoS attacks: A fuzzy TOPSIS-based quantitative assessment approach. *Heliyon*, 10(22), Article e40018. <https://doi.org/10.1016/j.heliyon.2024.e40413>.
10. Alsirhani, A., Sampalli, S., & Bodorik, P. (2019). DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in Apache Spark. *IEEE Transactions on Network and Service Management*, 16(3), 936–949. <https://doi.org/10.1109/TNSM.2019.2929425>.
11. Imamguluyev, R. (2025). Detection and prevention of cyber attacks based on fuzzy logic and deep learning. In *International Conference on Intelligent and Fuzzy Systems* (pp. 402–409). Springer. [https://doi.org/10.1007/978-3-031-97992-7\\_45](https://doi.org/10.1007/978-3-031-97992-7_45).

### **Lakhno Valerii**

*Doctor of Technical Sciences, Professor, Professor of the Department of Computer Systems, Networks and Cybersecurity, National University of Life and Environmental Sciences of Ukraine*  
ORCID: <http://orcid.org/0000-0001-9695-4543>  
E-mail: [lva964@nubip.edu.ua](mailto:lva964@nubip.edu.ua)

### **Kasatkin Dmytro**

*PhD of Pedagogical Sciences, Associate Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National University of Life and Environmental Sciences of Ukraine*  
ORCID: <https://orcid.org/0000-0002-2642-8908>  
E-mail: [d.kasatkin@nubip.edu.ua](mailto:d.kasatkin@nubip.edu.ua)

## **A FUZZY-LOGICAL MODEL FOR ASSESSING THE STATUS OF AN INFORMATION SYSTEM DURING DDOS ATTACKS**

**Abstract.** A fuzzy-logical model for assessing the state of an information system (IS) during DDoS attacks is proposed. The model is based on the use of a system of linguistic variables that describe critical parameters of network traffic and the operational characteristics of the IS. To form an assessment of the current risk, Mamdani-type fuzzy inference was applied, followed by defuzzification using the centre-of-gravity method. A simulation experiment was conducted, implemented in the Python environment using the scikit-fuzzy library. The results obtained confirmed that the proposed model adequately reflects the dependence of the integral risk on changes in load parameters, ensures continuity of assessment and sensitivity to critical combinations of traffic factors. The results obtained provide grounds for considering the developed model as a basis for the synthesis of an IS status monitoring module.

**Keyword:** DDoS Attack, Fuzzy Logic, Risk Model, Information System, Mamdani Fuzzy Inference, State Assessment, Security Monitoring.

UDC 629.3.017:004.318

**Nikitenko Yevheniy**

*PhD in Physical and Mathematical Sciences, Associate Professor of the Department of Computer Systems, Networks and Cybersecurity,*

*National University of Life and Environmental Sciences of Ukraine*

ORCID: <http://orcid.org/0000-0002-9222-644X>

E-mail: [ev.nikitenko@nubip.edu.ua](mailto:ev.nikitenko@nubip.edu.ua)

**Gladkij Anatolij**

*PhD in Physical and Mathematical Sciences, Associate Professor of the Department of Computer Systems, Networks and Cybersecurity,*

*National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0000-0001-8852-0884>

E-mail: [amglad@nubip.edu.ua](mailto:amglad@nubip.edu.ua)

**SPECIALIZED MODULE BASED ON ARDUINO FOR A CAR SECURITY SYSTEM**

***Abstract.** The high rate of car theft has led to an increased demand for efficient and reliable security systems capable of providing continuous monitoring of a vehicle's condition and promptly responding to attempts of unauthorized access. A significant portion of existing commercial solutions is characterized by high cost, closed architecture, and insufficient adaptability to the specific requirements of car owners. The use of open hardware platforms such as Arduino makes it possible to develop cost-effective, flexible, and specialized security modules that can be integrated into any vehicle model while maintaining a high level of safety.*

*The Arduino platform, due to its open hardware architecture and wide selection of compatible modules, is one of the most common foundations for building automotive security systems. Among the main advantages of Arduino are its low cost, support for standard interfaces (UART, I2C, SPI), compatibility with numerous digital and analog sensors, availability of libraries, and ease of debugging. These factors make Arduino a convenient tool for implementing fully functional security modules.*

***Keywords:** Automotive Security System, Specialized Module, Arduino Platform, Sensors.*

**Introduction.** The purpose of this work is to develop a specialized hardware and software module based on the Arduino platform, designed for automated monitoring and signaling of unauthorized interference or attempted vehicle theft.

To achieve this goal, the following tasks have been defined:

1. Analyze similar automotive security systems, identifying their advantages and disadvantages.
2. Develop a structural model of the specialized security system module.
3. Select the optimal hardware configuration of the Arduino platform for solving the stated tasks.
4. Develop software for controlling the module and implementing the main monitoring and signaling functions.

The practical significance of the work lies in the development of an accessible and effective solution for vehicle security systems, which can be used in the real business sector.

The growing level of vehicle automation, the introduction of intelligent functions into onboard electronic systems, and the expansion of wireless communication have significantly increased the vulnerability of cars to external cyber and physical threats. At the same time, the widespread use of keyless access, telematics modules, and CAN buses in standard security systems has revealed numerous shortcomings of existing security architectures, including:

- weak user authentication and the absence of multi-factor access verification
- the technical possibility of conducting relay attacks, breaches via OBD-II, and spoofing identifiers in CAN packets
- insufficient control by the end user over updating or expanding security functions

- lack of support for flexible integration of new sensor, cryptographic, or tracking modules.

In addition, most OEM systems are closed both in software and hardware, which makes it impossible to promptly update or adapt such systems to new requirements or real threat scenarios.

Under such conditions, the development of an autonomous, modular security solution becomes especially relevant—one that not only performs basic functions of intrusion detection or blocking but also provides:

- independence from the manufacturer's central ECUs or CAN bus
- support for adaptive real-time threat response
- the ability for remote event indication and object tracking
- an open structure for integration with additional protective modules.

Using the Arduino platform as the basis for implementing such a module is considered appropriate.

The engineering task includes forming the logical structure of the system, synthesizing the hardware configuration based on available modules, developing program code using Arduino IDE libraries, and conducting simulations and real-world testing. Special attention is given to modularity, structural autonomy of each component, and the compliance of event-processing logic with the requirements for time sensitivity, minimization of false alarms, and safe handling of input signals.

Within the defined purpose and considering the specifics of embedded security systems, particular attention must be paid to the technical requirements of the security module, which must operate under conditions of limited computational and energy resources. These requirements are formed taking into account the principles of energy efficiency, response time, event detection accuracy, resistance to external interference, and the ability to integrate additional modules. These characteristics must be incorporated at the system design stage, including the architectural model, choice of hardware platform, software configuration, and the logic of input signal processing.

**Literature Review.** Vehicle security systems are an integral part of the overall concept of automotive safety and serve the function of preventing unauthorized access, theft, and damage to the vehicle or its individual components. Due to the increasing information and physical threats in the automotive sector, security systems are continuously evolving in both technical and software aspects. Their functional complexity is constantly growing, which necessitates precise classification to analyze the advantages, limitations, and application areas of each type.

In [1], the authors describe automated systems that activate without user intervention after a certain period of inactivity. They usually block engine start, starter operation, or fuel supply. A typical example of such systems is the immobilizer, which does not require additional actions for activation but has limited functionality.

Active systems require explicit user action to turn the system on or off (pressing a button, entering a code, using a key fob). They provide extended configuration options, allowing the activation of various sensors (impact, volume, tilt) and alarm modes [2].

The systems proposed in [3], integrated into the vehicle's electronic architecture (OEM), allow synchronization with control units via the CAN bus, ensuring deep interaction with other electronic systems of the vehicle. They may include telematic functions and interact with mobile applications or cloud platforms.

Physical vehicle protection means include mechanical blockers of the steering wheel, gearbox, hood, and pedals. These devices provide a direct physical barrier but do not offer remote control or notification capabilities [4].

Smart key and GSM alarm systems incorporate authentication algorithms, encryption, dynamic signal coding (rolling code), and intrusion detection [4].

In [5], a comparison is presented between the traditional electronic device communication architecture in vehicles and a CAN-bus-based architecture. In the non-CAN variant, each device has a separate connection to the electronic control unit (ECU), creating a complex network of wired channels. In the CAN-based variant, all devices are connected to a common two-wire bus, through which data exchange occurs, providing a more efficient and scalable network topology.

Security systems also actively use sensor modules, among which the most common are ultrasonic, infrared, gyroscopic, and magnetoresistive sensors. They enable the detection of movements inside the cabin, vehicle body tilt, impacts, attempts to break locks, or hood opening. Due to low power consumption and compactness, these sensors are widely used in embedded solutions based on microcontrollers such as Arduino, STM32, or ESP32 [6].

Analyzing the results of recent studies, it is advisable to focus on the development of flexible, autonomous, and adaptive security modules with built-in self-diagnostic capabilities, cryptographic protection, and integration with mobile services, which constitutes the goal of further system design based on the Arduino platform.

**Purpose.** The purpose of this article is to develop and study a specialized hardware-software module based on the Arduino platform for an automotive security system, designed to automatically monitor the vehicle’s condition, detect unauthorized access attempts, and promptly generate alarms and lock critical vehicle components.

**Results and Discussion.**

*Architecture of the security module*

The design of an effective automotive security module is based on the principles of modularity, autonomy, and adaptability to external threats, which is especially relevant given the continuous increase in both cyber and physical attacks on vehicles. The architecture of the system must ensure not only the detection of and response to unauthorized access attempts, but also support the scalability of functionality, integration of new components, and flexible configuration of operating logic according to specific usage conditions.

The central element of the developed security module is the Arduino UNO microcontroller, based on the ATmega328P, which performs the functions of controlling all subsystems, processing input data from sensors, and generating control signals for actuators. The choice of this platform is determined by its open architecture, low power consumption, compatibility with numerous peripheral modules, and extensive library support for implementing monitoring and signaling algorithms [7].

The structural diagram of the security module architecture is shown in Figure 1. This UML diagram reflects the main hardware components of the system, their functional interconnections, and the directions of data transmission between the modules.

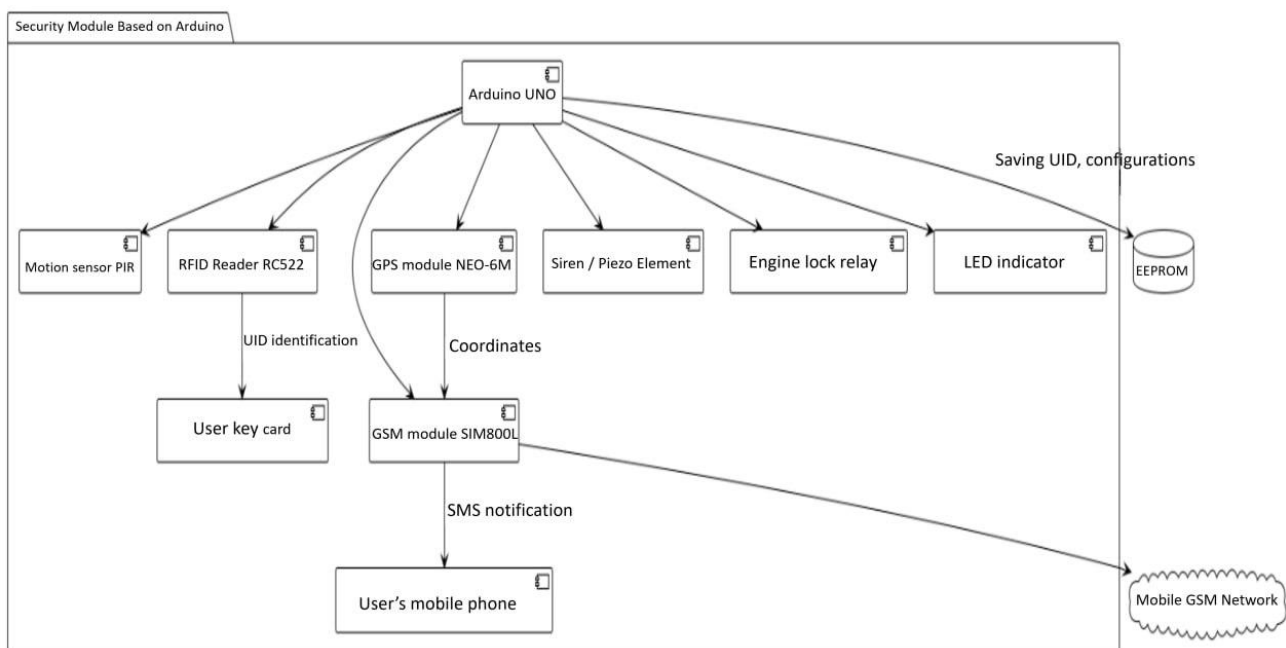


Figure 1 – Architecture of the Arduino-based security module

As shown in Figure 1, the Arduino UNO serves as the central node that coordinates the operation of all peripheral devices. Sensors and actuators are directly connected to the microcontroller, ensuring a rapid response to events. The transmission of alarm signals and coordinates is carried out via the GSM module, which interacts with the mobile network to notify the user.

An important feature of the architecture is its modularity, which enables easy integration of additional functional blocks, such as Wi-Fi modules, tilt sensors, or biometric authentication units. The open Arduino IDE software environment provides flexibility in configuring event-processing logic and adapting the system to specific usage scenarios [8].

#### *Design of the structural and schematic diagrams*

The development of a vehicle security module involves constructing both a structural and a schematic electrical diagram. The structural diagram allows the main functional blocks of the system and their interactions to be represented at a conceptual level, while the schematic diagram details the electrical connections between components, defining the connection logic and the nature of the signals.

The structural diagram of the security module is built taking into account the functional distribution of subsystems into threat-detection blocks, indication blocks, and active countermeasure blocks. The central link of the system is the Arduino UNO microcontroller, which processes signals from sensors, generates control signals for actuators, and provides interaction with the user. Inputs to the Arduino UNO include signals from a PIR sensor for motion detection, an ultrasonic distance sensor for proximity monitoring, and an SW-200D tilt sensor for registering changes in the vehicle's position. Control signals are generated for a relay module that blocks the vehicle's critical systems, for LED indication, and for an audible alarm. Interaction with a mode-selection button and a potentiometer for adjusting parameters is also provided (Figure 2).

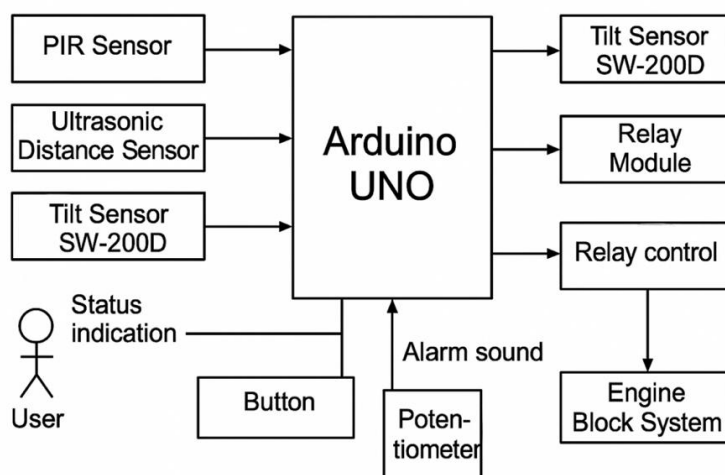


Figure 2 – Structural diagram of the security module

The schematic diagram details the connections between the system components, taking into account power supply, signal connections, and control circuits. Power is provided by a 9V battery, which, through a voltage regulator, supplies the Arduino and peripheral devices. Sensors (ultrasonic, PIR, and tilt) are connected to the microcontroller's digital inputs. LEDs for status indication are connected through 220  $\Omega$  current-limiting resistors. The audible alarm is implemented using a piezo element, controlled by a separate digital output. Additionally, a button and a potentiometer are connected, serving for manual control and parameter adjustment, respectively (Figure 3).

The constructed circuit implements basic security logic: when any of the sensors is triggered, the system activates both visual and audible alarms while simultaneously opening the relay to block the engine start system. This approach provides comprehensive, multi-level vehicle protection, combining threat detection, signaling, and physical countermeasures against theft attempts.

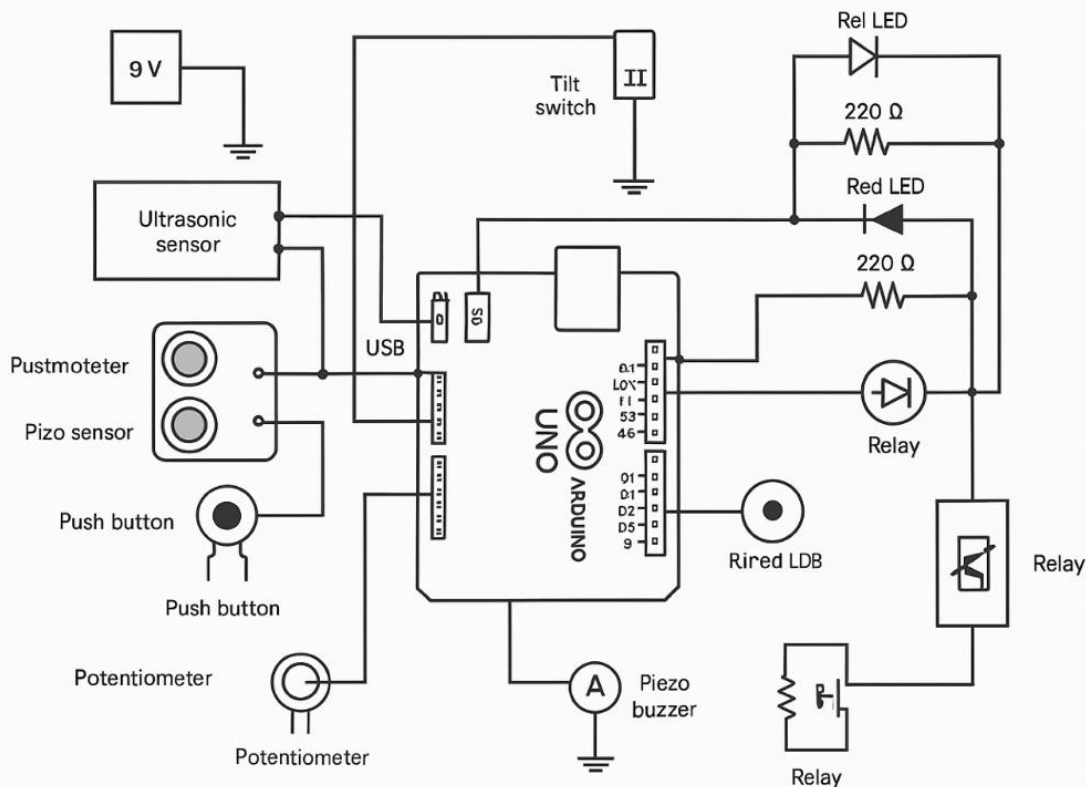


Figure 3 – Schematic diagram of the security module

*Development of the system operation algorithm*

To ensure the correct functioning of the Arduino-based security module, a system operation algorithm was developed that implements the logic for responding to threats detected by various sensors and activates the corresponding actuators. The main requirements for the algorithm are: continuous monitoring of sensor status, minimization of false alarms, the ability for the user to reset the alarm, and restoration of the system’s initial state.

The operation of the module begins with the initialization of all components. The system then checks for the presence of power. If power is absent, a standby mode is activated. Upon detecting a stable power source, the system switches to security mode.

During the monitoring phase, the system reads data from the following sensors:

- **PIR sensor**, which reacts to motion within the monitored area.
- **SW-200D tilt sensor**, which detects changes in the vehicle’s position (e.g., during a towing attempt).
- Ultrasonic distance sensor, which allows detection of an object approaching the vehicle.

If any sensor is triggered, the system enters an alarm mode. Specifically, the audible alarm (piezo element) is activated, the visual indicator (red LED) is turned on, and critically, the relay blocks the engine start system, preventing unauthorized vehicle movement.

To prevent false triggers of the ultrasonic sensor, a mechanism for confirming object proximity is implemented, taking into account the signal duration exceeding a predefined threshold. This avoids alarm activation due to short-term movements or minor obstacles.

The alarm state can be reset by pressing a user button. In this case, the siren is turned off, the relay is unlocked, and the visual indicator returns to its initial state. Thus, the algorithm maintains a closed loop — after the alarm condition ends, the system returns to the monitoring phase.

The logic of the algorithm is visualized in a UML activity diagram shown in Figure 4. The diagram illustrates the sequence of events, logical branches, user actions, and transitions between different system states.

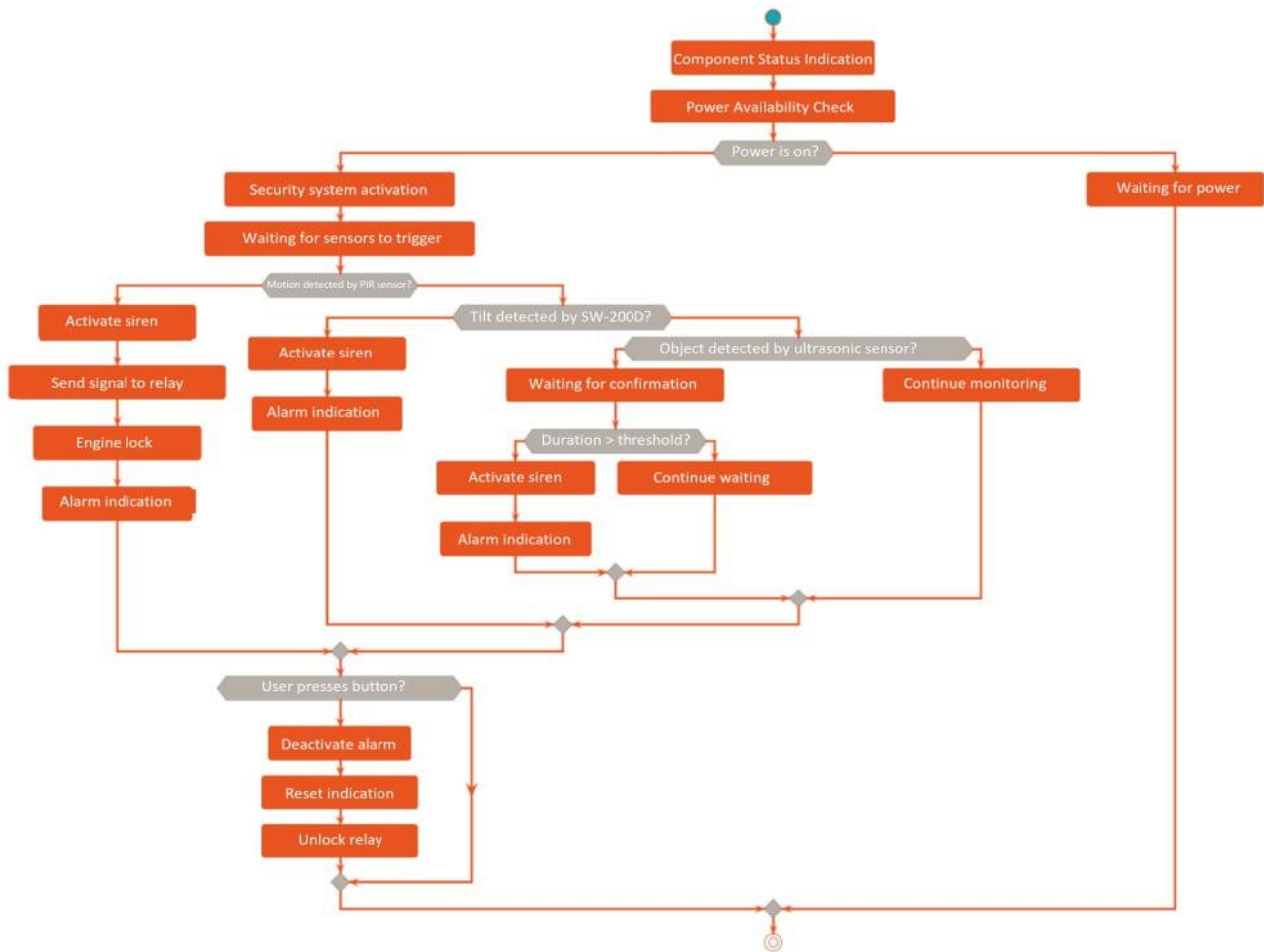


Figure 4 – Operation algorithm of the security module (UML activity diagram)

The implementation of such an algorithm enables a comprehensive system response to potential threats and enhances the vehicle’s security level. The presence of multi-level control logic, verification mechanisms, and user intervention makes the system reliable, adaptive, and convenient to use.

#### Description of the module software

The security module software is implemented in C++ within the Arduino IDE environment, using a procedural model for event and signal management. The main functionality of the module includes monitoring input signals from sensors, processing breach logic, generating the corresponding alarm response, and controlling actuators.

The software architecture employs a modular approach to handling data from heterogeneous sensors: passive infrared (PIR), ultrasonic (HC-SR04), tilt sensor (Tilt), analog sound sensor, potentiometer, and button. Each sensor is connected to a separate digital or analog input of the Arduino UNO R3 microcontroller. Signal processing is performed in the main program loop (loop()), where each sensor is checked according to its threshold values or activation conditions.

During initialization (setup()), ports are configured, pin modes (input/output) are set, the serial monitor is activated, and libraries for external components are loaded. For digital inputs such as PIR, Tilt, and Button, the signal level is read directly using the digitalRead() function. Analog sensors (Potentiometer, Sound Sensor) are processed using analogRead(), with subsequent comparison of values against predefined sensitivity thresholds.

Figure 5 presents the UML component diagram of the developed system, illustrating the logical connections between the central controller (Arduino UNO R3), the sensor subsystem, actuators, and

auxiliary infrastructure elements. The diagram indicates connection types (digital input/output, analog input, I2C interface), corresponding to the program code structure and port configuration.

The implementation logic also takes into account optimization of event response time, achieved by avoiding blocking functions such as delay() in critical sections of the code. Instead, time control is implemented using the millis() function, allowing for pseudo-parallel operation.

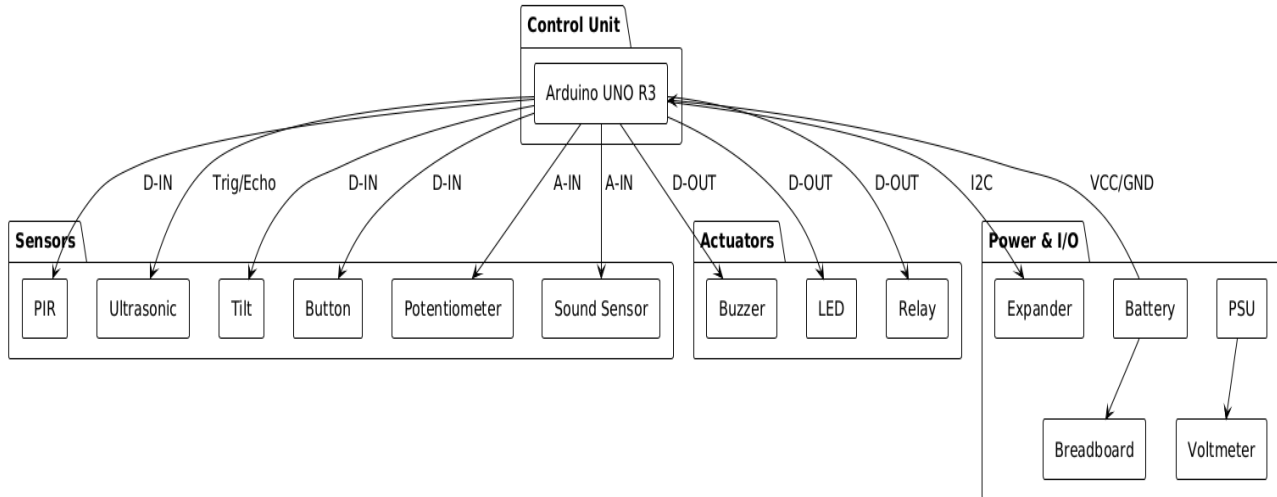


Figure 5 – UML component diagram of the Arduino UNO-based security module

The developed software ensures full integration of all physical components of the security system, guarantees real-time event response, and provides a foundation for further functionality expansion within secure embedded solutions.

*Implementation of control and signaling functions*

The control and signaling system of the security module is built around the Arduino UNO R3 microcontroller, which interacts with motion, tilt, and sound sensors and controls actuators — an LED, a relay, and a buzzer. The response logic architecture ensures the detection of unauthorized actions and the immediate activation of the alarm system.

Figure 6 shows a fragment of the system’s initial setup, where digital input and output ports are configured for operation with sensors and signaling devices. Specifically, ports D2 and D3 are configured to receive data from the motion (PIR) and tilt sensors, while ports D4–D6 are used to activate the LED, relay, and buzzer, respectively.

```
void setup() {
    pinMode(2, INPUT); // PIR sensor
    pinMode(3, INPUT); // Tilt sensor
    pinMode(4, OUTPUT); // LED
    pinMode(5, OUTPUT); // Relay
    pinMode(6, OUTPUT); // Buzzer
    Serial.begin(9600);
}
```

Figure 6 – Fragment of digital port initialization in the security module

The module’s operation logic involves continuous monitoring of sensor states. When an active signal is detected from any sensor (motion or tilt), the microcontroller immediately sends control signals to the actuators, triggering the alarm. Figure 7 shows the implementation of the main loop() cycle, which is responsible for event analysis and the corresponding response.

The module also implements a function for monitoring acoustic changes in the environment using an analog microphone sensor. Noise level readings are taken through port A0, and alarm

activation is triggered when the predefined threshold is exceeded. A fragment of the corresponding code listing is shown in Figure 8.

```
void loop() {  
  int motion = digitalRead(2);  
  int tilt = digitalRead(3);  
  
  if (motion == HIGH || tilt == HIGH) {  
    digitalWrite(4, HIGH); // LED ON  
    digitalWrite(5, HIGH); // Relay ON  
    tone(6, 1000); // Buzzer ON  
    Serial.println("Alert: Motion or Tilt Detected!");  
  } else {  
    digitalWrite(4, LOW);  
    digitalWrite(5, LOW);  
    noTone(6); // Buzzer OFF  
  }  
  
  delay(200);  
}
```

*Figure 7 – Implementation of the main loop() cycle*

```
int soundLevel = analogRead(A0);  
int threshold = 500;  
  
if (soundLevel > threshold) {  
  digitalWrite(4, HIGH); // LED ON  
  tone(6, 1500); // Buzzer high tone  
  Serial.println("Sound alert triggered");  
}
```

*Figure 8 – Code fragment for acoustic change monitoring*

This implementation allows for multiple threat detection channels, thereby increasing the overall reliability of the module.

**Conclusions.** During the course of this work, the stated goal was fully achieved – a specialized automotive security system module based on the Arduino platform was developed, providing a basic level of protection against unauthorized access and mechanical tampering.

It was determined that modules based on Arduino microcontrollers with open architecture demonstrate high adaptability to specific user requirements. The main advantages of such systems were identified: low cost, ease of implementation, and customization possibilities. Among the disadvantages are the need for configuration, lack of protection against scanners, and limited energy efficiency in the basic implementation.

Functional and structural models of the specialized security module were developed. The model provides multi-channel monitoring: door status, nearby motion detection, and vehicle body tilt. All events are processed centrally by the microcontroller, after which the response is initiated – activation of visual and audible alarms, engine start system blocking, and signal transmission to an external module.

The developed software ensures continuous scanning of sensor states, event processing, and execution of responses according to predefined scenarios.

Results of modular and system testing confirmed the functionality of all components – sensors, logic, and actuators. The system responded to threats within an average of 140–200 ms, which is

acceptable for this class of devices. Stability of event handling was verified under simultaneous signals from multiple sensors.

Thus, the developed security module demonstrated effective operation, high stability in monitoring and signaling modes, and flexibility for future expansion. The obtained results allow the recommended solution to be used for educational, research, and practical purposes, as well as serving as a foundation for building full-featured automotive or stationary security systems with additional functionalities.

### References

1. Tverdokhlebov, V. I. (2018). Vehicle security systems. National Aviation University.
2. Mikhieiev, A. V., & Demchenko, S. O. (2020). Microcontrollers for embedded systems: Arduino and its applications. Kharkiv National University of Radio Electronics.
3. Struk, A. O., & Yavorskyi, I. P. (2021). Fundamentals of digital electronics and microprocessor technology. Lviv National University Publishing House.
4. Sharma, K., & Patel, D. (2021). Vehicle security system using GSM and GPS: A review. International Journal of Engineering Research and Applications, 11(4), 11–15.
5. Martin, J. (2019). Arduino for automotive projects. Packt Publishing.
6. Volodin, S. V. (2017). Automatic control and vehicle security systems [Methodical guidelines]. Kyiv National University of Construction and Architecture.
7. Maksimović, D., & Erickson, R. (2020). Fundamentals of power electronics. Springer. <https://doi.org/10.1007/978-3-030-43881-4>.
8. Zozulia, S. M. (2022). Working with sensors in Arduino IDE. Vinnytsia National Technical University.

### Нікітенко Євгеній Васильович

кандидат фізико-математичних наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,

Національний університет біоресурсів і природокористування України

ORCID: <http://orcid.org/0000-0002-9222-644X>

E-mail: [ev.nikitenko@nubip.edu.ua](mailto:ev.nikitenko@nubip.edu.ua)

### Гладкий Анатолій Михайлович

кандидат фізико-математичних наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,

Національний університет біоресурсів і природокористування України

ORCID: <https://orcid.org/0000-0001-8852-0884>

E-mail: [amglad@nubip.edu.ua](mailto:amglad@nubip.edu.ua)

## СПЕЦІАЛІЗОВАНИЙ МОДУЛЬ НА БАЗІ ARDUINO ДЛЯ АВТОМОБІЛЬНОЇ СИСТЕМИ БЕЗПЕКИ

**Анотація.** Високий рівень викрадень автомобілів призвів до зростання попиту на ефективні та надійні системи безпеки, здатні забезпечувати постійний моніторинг стану транспортного засобу та оперативно реагувати на спроби несанкціонованого доступу. Значна частина існуючих комерційних рішень характеризується високою вартістю, закритою архітектурою та недостатньою адаптованістю до конкретних вимог власників автомобілів. Використання відкритих апаратних платформ, таких як Arduino, дозволяє розробляти економічно ефективні, гнучкі та спеціалізовані модулі безпеки, які можна інтегрувати в будь-яку модель автомобіля, зберігаючи при цьому високий рівень безпеки.

Платформа Arduino, завдяки своїй відкритій апаратній архітектурі та широкому вибору сумісних модулів, є однією з найпоширеніших основ для побудови автомобільних систем безпеки. Серед основних переваг Arduino — низька вартість, підтримка стандартних інтерфейсів (UART, I2C, SPI), сумісність з численними цифровими та аналоговими датчиками, наявність бібліотек та простота налагодження. Ці фактори роблять Arduino зручним інструментом для реалізації повнофункціональних модулів безпеки.

**Ключові слова:** система безпеки для автомобілів, спеціалізований модуль, платформа Arduino, датчики

UDC 004.056.55:004.421.2

### Sahun Andrii

*PhD, Associated Professor of the Department of Computer Systems, Networks and Cybersecurity, National University of Life and Environmental Sciences of Ukraine*

ORCID: <https://orcid.org/0000-0002-5151-9203>

E-mail: [a.sagun@nubip.edu.ua](mailto:a.sagun@nubip.edu.ua)

### Panasko Olena

*PhD, Associated Professor of the Department of Telecommunication and Robotics Systems and Cybersecurity,*

*Cherkasy State Technological University*

ORCID: <https://orcid.org/0000-0002-0510-7742>

E-mail: [lena.pa@ukr.net](mailto:lena.pa@ukr.net)

## TRENDS IN INCREASING THE CRYPTO-STRENGTH OF SYMMETRIC BLOCK CIPHERS IN THE CONTEXT OF THE MODERN CRYPTOSYSTEMS DEVELOPMENT

**Abstract.** *The article examines the combination of analytical and applied approaches to improving symmetric block ciphers in light of current trends in the development of cryptographic systems. The study analyzes the current SOG-IS standards and recommendations that define the basic directions of symmetric algorithm evolution, such as the transition from outdated Feistel-based schemes to optimized structures (AES, lightweight block ciphers for IoT). Using a modified version of the Simple-DES (S-DES) cipher, the paper proposes a method for enhancing cryptographic strength without changing the key or block length. The main improvements involve an enhanced design of S-boxes and their dynamic selection based on a key graph. The results of the comparative analysis demonstrate a significant increase in resistance to brute-force and differential cryptanalysis compared to the standard S-DES, while maintaining low computational complexity. The conducted research confirms the relevance of using educational and experimental models such as S-DES to explore modern methods for improving the security of symmetric ciphers, which is of practical importance for prototyping and lightweight implementations in Internet of Things systems.*

**Keywords:** *Symmetric Encryption, Block Ciphers, Feistel Network, S-DES, S-Boxes, Cryptographic Strength, AES, Lightweight Ciphers, IoT, SOG-IS.*

**Introduction.** Symmetric block cryptosystems are a fundamental component of modern information protection methods that ensure data confidentiality and integrity in both networked and autonomous environments. The rapid development of asymmetric algorithms has had little effect on the evolution of symmetric ciphers, since symmetric encryption remains crucial due to its combination of high performance, implementation simplicity, and low computational cost.

Recently, there has been a growing interest in lightweight block ciphers designed for Internet of Things (IoT) and mobile systems, as well as in improving the components of block algorithms—namely, S-boxes, key generation mechanisms, and round functions. However, the study of trends in the evolution of well-known and thoroughly analyzed symmetric cryptosystems, particularly those based on classical Feistel networks, remains relevant. For this reason, in many studies, the S-DES cipher is considered primarily as an educational symmetric block cryptosystem with research potential.

**Literature Review.** The principles of constructing symmetric block ciphers, particularly Feistel networks, are presented in the classical works of W. Stallings [1] and B. Schneier [2-4]. A generalization of approaches to the development of modern cryptographic algorithms is provided in the works of AES standard developers – J. Daemen and V. Rijmen [5].

The current trends in the evolution of block ciphers, described in [6-13], indicate a gradual transition from complex and cumbersome algorithms to energy-efficient and secure implementations, such as those used in the PRESENT, GIFT, and SPECK ciphers, among others.

As shown in several studies [2, 8-10], the modernization of a basic Feistel-based cipher solely through an increased number of rounds leads to a noticeable improvement in cryptographic strength. At the same time, enhancing resistance by increasing key length results in significant complications

in cryptographic transformations and increases the computational load. Therefore, in practice, the only feasible way to improve the cryptographic strength when modifying the S-DES cipher is by refining the design of its S-boxes. Some possible improvements are described in [14, 15]. Although for 4-bit S-boxes used in the S-DES cipher there are no ideal variants with perfect cryptographic properties, it is possible to select tables with similar properties among  $4 \rightarrow 4$  or  $6 \rightarrow 4$  mappings, or even use S-boxes from the DES cipher.

Ukrainian studies [10, 11] and national standards [16, 17] emphasize the importance of adapting international cryptographic solutions to national security requirements and educational applications.

Among many works devoted to an in-depth analysis of modern trends in symmetric cryptosystem development, sources [7-10] deserves particular attention. It explores the prospects for improving S-boxes, key-schedule methods, and integrating post-quantum principles into classical symmetric encryption structures.

A review of block cipher development reveals the dominance of AES (Advanced Encryption Standard). Numerous sources note that AES is currently the most widely used block cipher, particularly in the context of NIST certification [18]. In most cases, practical data protection mechanisms are implemented using AES-based systems, which firmly establishes it as the “standard block cipher.” However, there is also a growing interest in lightweight block ciphers.

Recent research (2025) covering 58 lightweight block ciphers – spanning the period between 2018 and 2025 — highlights this trend [6, 7, 11, 12]. The emergence of lightweight block ciphers suitable for microcontroller implementations is directly linked to the rapid growth of the IoT market (52 such ciphers introduced in the current year) [7, 11].

Thus, while major computer systems primarily rely on AES-based cryptosystems, the increasing demand for specialized encryption solutions in resource- or energy-constrained environments drives the development of new lightweight block ciphers. Numerous studies note that algorithms such as DES or 3-DES are recommended exclusively as “legacy” solutions rather than viable options for new computer systems.

The recommendations of the European organization SOG-IS (Senior Officers Group – Information Systems Security Mutual Recognition Agreement, Crypto Working Group) describe current and legacy symmetric algorithms for data protection and specify their permitted usage periods. For instance, the 3-DES algorithm with two effective keys (effective key length  $\approx 112$  bits) is officially considered obsolete and permitted for practical use only until 2024, after which its use is discouraged due to insufficient cryptographic strength. The 3-DES algorithm with three independent keys (effective key length  $\approx 168$  bits) is permitted only until 2027.

According to the SOG-IS Crypto Working Group documents (2023, v1.3), AES is recognized as the only symmetric cipher recommended for new applications in Europe. The 3-DES cipher may be allowed only for compatibility with existing systems but should be gradually phased out of use [19].

Objectively, there is a lack of comprehensive statistical data on the practical use of most existing symmetric block ciphers; however, some sources provide sufficient information to assess the overall trends in this field [1, 9, 10].

**Purpose.** The main point of research is to develop and substantiate an integrated approach to enhancing the cryptographic strength of symmetric block ciphers, which combines the modification of internal structural components of the cipher, the use of multilevel encryption schemes, and the application of modern methods for assessing resistance to differential and linear cryptanalysis, taking into account current trends and the potential for the development of cryptographic systems.

**Results and Discussion.** In the context of modern trends, the focus is not merely on the choice of the encryption algorithm itself but on its implementation and the optimization of security.

The dynamics of the development trends of symmetric block ciphers from 2001 to 2025, shown in Figure 1, demonstrate a steady increase in the number of various AES system implementations and an intensive growth in the number of new “lightweight” block ciphers within the IoT segment.

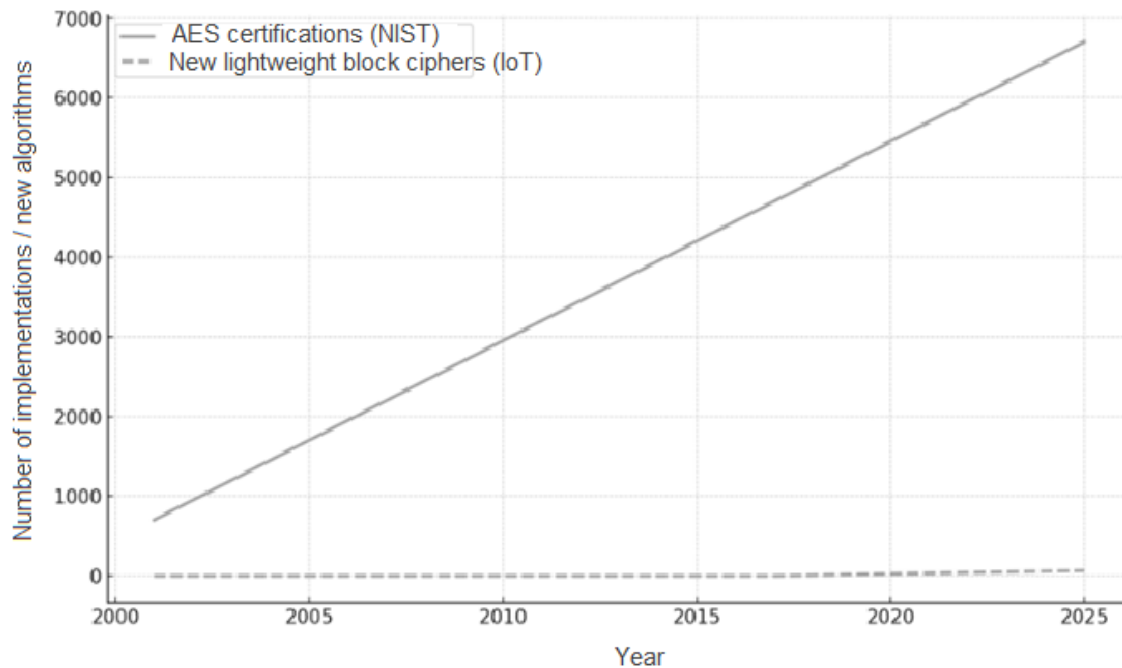


Figure 1 – Dynamics of the symmetric block ciphers development from 2001 to 2025

Existing statistics and assessments of the use of symmetric block ciphers for the period from 2018 to 2025 show that NIST certifications of symmetric block cipher variants indicate a continuous increase in various implementations of the AES cipher (over the reviewed period, the number of implementations has grown more than 7,000 times compared to 2001) [7, 8, 10]. In the IoT segment, according to research data for 2025, 58 new “lightweight” block ciphers have emerged during the period from 2018 to 2025.

To enhance the encryption quality of the Feistel-based block cipher Simple-DES (S-DES), a specific set of S-boxes was generated (a pool derived from the PRESENT cipher S-box), and a modified version of S-DES was implemented. The modified cipher uses 12 rounds ( $R = 12$ ), incorporating an improved key-schedule transformation and dynamic S-box selection. It was compared to the original S-DES (2 rounds) using two metrics:

- average avalanche effect — the mean number of ciphertext bits that change when a single plaintext bit is inverted (averaged over 500 cases). In the original S-DES, this value was approximately 3.94 bits, while in the modified S-DES ( $R = 12$ ) it increased to about 3.99 bits;
- maximum differential probability (DDT probability) — the worst-case value from the differential distribution table of the S-boxes. For the original S-DES ( $S_0/S_1$  mapped as a  $4 \rightarrow 2$  equivalent), this probability was approximately 0.75, whereas for the modified PRESENT-based S-DES it decreased to about 0.44;
- both variants were compared according to the criterion of resistance to differential cryptanalysis (Fig. 2).

As shown in Figure 2, the implemented modification significantly reduced the maximum differential probability of the S-boxes, which directly complicates differential cryptanalysis. Moreover, the avalanche effect in the original cipher was already very close to the ideal ( $\sim 4$  bits out of 8), and the modification slightly improved this parameter.

Despite the unchanged key space (10 bits), the proposed enhancement has effectively increased the cipher’s resistance to analytical attacks, particularly differential and linear cryptanalysis. During testing of the developed S-DES cipher modification, it was also found, that even a very significant modification is unable to somehow increase the theoretical cryptographic strength of this cipher. This can be attributed to the fact that both of its variants (S-DES with two rounds of iterations and with 12 rounds of crypto transformation iterations) use a similar length of the common key – 10 bits. That’s

why the estimate of the complexity of the full enumeration for both variants of the cipher is the same and is the number of:  $\log_{10}(2^{10}) = 10 * \log_{10}(2) \approx 3,0103$ .

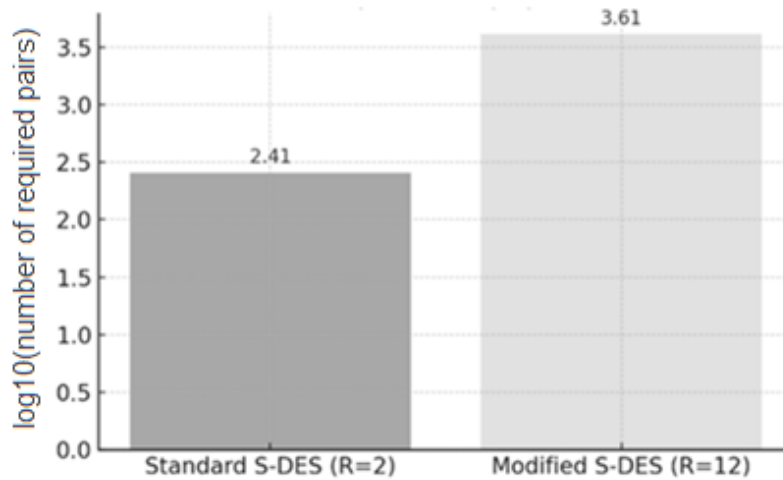


Figure 2 – Indicator of equivalent resistance against differential cryptanalysis (logarithmic scale)

At the same time, the equivalent resistance against differential cryptanalysis for the modified version of the cipher has improved significantly, which can be seen in the graph (Figure 3).

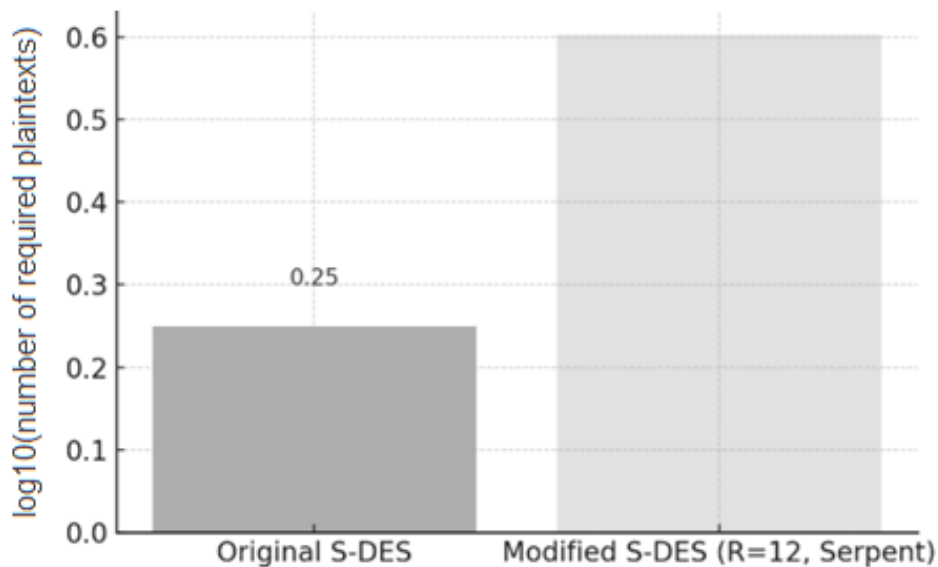


Figure 3 – Comparison of resistance to linear cryptanalysis for the modified and unmodified version of the S-DES cipher (logarithmic scale)

It is known that the standard S-DES cipher with the number of encryption rounds R=2 requires approximately  $10^{2,4} \approx 251,84$  pairs of plaintext and ciphertext for key computation. While the modified S-DES cipher with the number of rounds R=12, in one of its modifications, the PRESENT-based S-box pool modification, requires already  $10^{3,6} \approx 3981$  pairs, i.e., approximately 16 times more.

The obtained data indicate a real increase in the cryptoresistance of the cipher to known types of cryptanalysis, achieved only by optimizing the structure of S-boxes and increasing the number of rounds. Moreover, such changes in the design of the S-DES cipher were not accompanied by a change in the length of the key.

**Conclusions.** Improving the design of S-boxes is the most effective way to improve S-DES stability without increasing the key size or block size. Using a pool of S-boxes based on proven schemes (example, Serpent cipher, PRESENT, etc.) allows to significantly reduce the number of linear and differential dependencies in the output sequences. To complicate the construction of analytical attacks, it is effective to use dynamic selection of S-boxes, which depends on the current round key (key-dependent S-box selection).

It is expected that increasing the number of rounds of the S-DES training cipher from 2 to 12 in the modified version of this cipher performs an avalanche effect and allows to ensure a more uniform distribution (dispersion) of the ciphertext bits. Although legacy algorithms like DES or 3-DES are increasingly used in new systems, their role is still important because it allows for the exploration of the design of S-boxes, which are part of modern encryption algorithms.

As can be seen from the conducted research, improving the quality of the design of S-boxes of symmetric block ciphers, even without increasing the key length, allows in practice to increase their resistance to differential cryptanalysis by approximately 16 times, and to linear cryptanalysis by approximately 2–3 times, which is confirmed by Linear Approximation Table type cryptanalysis.

As a result of the analysis of modern trends in the development of symmetric cryptographic systems, it should be noted that the AES cipher today remains the main practical cipher for use in large information and communication systems.

**Prospects for improvement.** Given the current trend towards smaller systems with limited resources, as well as the development of Internet of Things or Smart Home technologies, the current trend is to use lightweight block ciphers. Today, the key parameters in choosing a block cipher are not only the algorithm itself, but also its implementation (hardware/software), resistance to side-channel attacks, and adaptability to new threats (such as post-quantum ones). This indicates that one of the directions for improving symmetric block ciphers may involve changes to the key space and enhancements to the design of S- and P-boxes. Increasing the key space of such a “lightweight” IoT cipher can significantly improve its practical cryptographic strength. A similar effect can be achieved by refining the structure of the round functions.

## References

1. Stallings, W. (2014). *Cryptography and network security: Principles and practice* (6th ed.). Pearson Education. URL: [https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive\\_exam/Cryptography\\_and\\_Network\\_Security.pdf](https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf).
2. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., & Hall, C. (1998). On the Twofish key schedule. In *Selected Areas in Cryptography* (pp. 27–42). Springer. [https://doi.org/10.1007/3-540-48892-8\\_3](https://doi.org/10.1007/3-540-48892-8_3).
3. Schneier, B. (1998). Cryptographic design vulnerabilities. *Computer*, 31(9), 29–33. <https://doi.org/10.1109/2.708447>.
4. Blaze, M., & Schneier, B. (1995). The MacGuffin block cipher algorithm. In B. Preneel (Ed.), *Fast Software Encryption: FSE '94* (pp. 97–110). Springer. [https://doi.org/10.1007/3-540-60590-8\\_8](https://doi.org/10.1007/3-540-60590-8_8).
5. Daemen, J., & Rijmen, V. (2020). *The design of Rijndael: The Advanced Encryption Standard (AES)* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-662-60769-5>.
6. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Mori, K. (2015). Midori: A block cipher for low energy. In *Advances in Cryptology – ASIACRYPT 2015* (pp. 411–436). Springer. [https://doi.org/10.1007/978-3-662-48800-3\\_17](https://doi.org/10.1007/978-3-662-48800-3_17).
7. Al-Nofaie, S. M., Sharaf, S., & Molla, R. (2025). Design trends and comparative analysis of lightweight block ciphers for IoTs. *Applied Sciences*, 15(14), 7740. <https://doi.org/10.3390/app15147740>.
8. Knudsen, L. R. (1994). *Block ciphers: Analysis, design and applications* (DAIMI Report Series No. 23/485). University of Aarhus. <https://doi.org/10.7146/dpb.v23i485.6978>.
9. Luzhetskyi, V. A., & Ostapenko, A. V. (2013). Analiz alhorytmiv symetrychnoho blokovocho shyfruvannia [Analysis of symmetric block cipher algorithms]. *ITKI*, 25(3).

10. Kuznetsov, O. O., Oliinykov, R. V., Horbenko, Yu. I., Pushkarov, A. I., Dyrda, O. V., & Horbenko, I. D. (2014). Obgruntuvannya vymoh, pobuduvannya ta analiz perspektyvnykh symetrychnykh kryptoperetvoren na osnovi blochnykh shyfriv [Substantiation of requirements, construction and analysis of перспективних symmetric cryptographic transformations based on block ciphers]. *Visnyk Natsionalnoho universytetu "Lvivska politehnika"*, 124–141. <https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6634/21-124-141.pdf>.
11. Hryshchuk, R., & Hryshchuk, O. (2025). Otsiniuvannya kryptostiikosti kryptosystemy Fredholma: metodolohiia ta analiz rezultativ [Evaluation of the cryptographic strength of the Fredholm cryptosystem: Methodology and analysis of results]. *Kiberbezpeka: osvita, nauka, tekhnika*, 1(29), 748–761. <https://doi.org/10.28925/2663-4023.2025.29.935>.
12. Jiang, X., Lakhno, V., Sahun, A., & Mamchenko, S. (2024). Development of a symmetric cryptographic differential distinguisher based on deep learning. *Cybersecurity: Education, Science, Technique*, 2(26), 123–139. <https://doi.org/10.28925/2663-4023.2024.26.674>.
13. Gargiulo, J. (2002, July 25). S-Box modifications and their effect in DES-like encryption systems (GSEC v1.4, Option 1). GIAC. <https://www.giac.org/paper/gsec/2048/s-box-modifications-effect-des-like-encryption-systems/103534>.
14. Shawky, N., Ahmed, I., & Ibrahim, A. (2023). S-box modification for the block cipher algorithms. *Przegląd Elektrotechniczny*, 99(4), 47–50. <https://doi.org/10.15199/48.2023.04.48>.
15. Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy. (2009). DSTU GOST 28147:2009. Systema obrobky informatsii. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (GOST 28147-89). Kyiv: DP «UkrNDNTs». [https://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=55943](https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=55943).
16. Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy. (2014). DSTU 7624:2014. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm symetrychnoho blokovooho peretvorennia. Kyiv: DP «UkrNDNTs», 2014. [https://online.budstandart.com/ua/catalog/doc-page?id\\_doc=65314](https://online.budstandart.com/ua/catalog/doc-page?id_doc=65314).
17. National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES) (NIST FIPS 197). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.FIPS.197>. [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=901427](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901427) (Accessed December 4, 2025).
18. SOG-IS Crypto Working Group. (2023). SOGIS agreed cryptographic mechanisms (Version 1.3). SOG-IS. <https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>.

### Сагун Андрій Вікторович

*кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,*

*Національний університет біоресурсів і природокористування України*

ORCID: <https://orcid.org/0000-0002-5151-9203>

E-mail: [a.sagun@nubip.edu.ua](mailto:a.sagun@nubip.edu.ua)

### Панаско Олена Миколаївна

*кандидат технічних наук, доцент, доцент кафедри робототехнічних і телекомунікаційних систем та кібербезпеки,*

*Черкаський державний технологічний університет, м. Черкаси*

ORCID: <https://orcid.org/0000-0002-0510-7742>

E-mail: [lena.pa@ukr.net](mailto:lena.pa@ukr.net)

## ТЕНДЕНЦІЇ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ МІЦНОСТІ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ У КОНТЕКСТІ СУЧАСНОГО РОЗВИТКУ КРИПТОСИСТЕМ

*Анотація.* У статті розглядається поєднання аналітичних та прикладних підходів до вдосконалення симетричних блокових шифрів у світлі сучасних тенденцій розвитку криптографічних систем. У дослідженні аналізуються сучасні стандарти та рекомендації SOG-IS, що визначають основні напрямки еволюції

симетричних алгоритмів, такі як перехід від застарілих схем на основі алгоритму Файстеля до оптимізованих структур (AES, полегшені блокові шифри для Інтернету речей). Використовуючи модифіковану версію шифру Simple-DES (S-DES), у статті пропонується метод підвищення криптографічної стійкості без зміни довжини ключа або блоку. Основні вдосконалення полягають у вдосконаленій конструкції S-боксів та їх динамічному виборі на основі графа ключів. Результати порівняльного аналізу демонструють значне підвищення стійкості до брут-форс-аналізу та диференціального криптоаналізу порівняно зі стандартним S-DES, зберігаючи при цьому низьку обчислювальну складність. Проведене дослідження підтверджує актуальність використання навчальних та експериментальних моделей, таких як S-DES, для вивчення сучасних методів підвищення безпеки симетричних шифрів, що має практичне значення для прототипування та легких реалізацій у системах Інтернету речей.

**Ключові слова:** симетричне шифрування, блокові шифри, мережа Файстеля, S-DES, S-бокси, криптографічна стійкість, AES, полегшені шифри, Інтернет речей, SOG-IS.