

ISSN 2786-5460 (Print)
ISSN 2786-5479 (Online)

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT



ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

Випуск 4 (19), 2025
Issue 4 (19), 2025



Видавничий дім
«Гельветика»
2025

*Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 11 від 10 грудня 2025 року)*

Інформаційні технології та суспільство / [головний редактор І. Остроумов]. – Київ : Міжрегіональна Академія управління персоналом, 2025. – Випуск 4 (19). – 222 с.

Журнал «Інформаційні технології та суспільство» є науковим рецензованим виданням, в якому здійснюється публікація матеріалів науковців різних рівнів у вигляді наукових статей з метою їх поширення як серед вітчизняних дослідників, так і за кордоном.

Редакційна колегія не обов'язково поділяє позицію, висловлену авторами у статтях, та не несе відповідальності за достовірність наведених даних і посилань.

Головний редактор: Остроумов І. В. – д-р техн. наук, професор, професор кафедри комп'ютерних інформаційних систем і технологій, Міжрегіональна Академія управління персоналом

Редакційна колегія:

Василенко М. Д. – д-р фіз.-мат. наук, проф., професор кафедри кібербезпеки, Національний університет «Одеська юридична академія»; **Горбов І. В.** – канд. техн. наук, с.н.с., старший науковий співробітник, Інститут проблем реєстрації інформації НАН України; **Дуднік А. С.** – д-р техн. наук, доц., доцент кафедри мережних та інтернет технологій, Київський національний університет імені Тараса Шевченка; **Євсєєв С. П.** – д-р техн. наук, лауреат національної премії імені Патона 2024 р., професор кафедри кібербезпеки, Національний технічний університет «ХПІ»; **Зибін С. В.** – д-р техн. наук, доц., завідувач кафедри інженерії програмного забезпечення, Національний авіаційний університет; **Кавун С. В.** – д-р екон. наук, канд. техн. наук, проф., завідувач кафедри комп'ютерних інформаційних систем та технологій, Міжрегіональна Академія управління персоналом; **Комарова Л. О.** – д-р техн. наук, с.н.с., директор Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; **Охріменко Т. О.** – канд. техн. наук, старший науковий співробітник науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі, Національний авіаційний університет; **Попов О. О.** – член-кор. НАН України, д-р техн. наук, професор, в.о. директора Центру інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України; **Рудніченко М. Д.** – канд. техн. наук, доц., доцент кафедри інформаційних технологій, Державний університет «Одеська політехніка»; **Скуратовський Р. В.** – канд. фіз.-мат. наук, доц., доцент кафедри обчислювальної математики та комп'ютерного моделювання, Міжрегіональна Академія управління персоналом; **Супрун О. М.** – канд. фіз.-мат. наук, доц., доцент кафедри програмних систем і технологій, Київський національний університет імені Тараса Шевченка; **Табунщик Г. В.** – канд. техн. наук, проф., професор кафедри програмних засобів, Національний університет «Запорізька політехніка»; **Фомін О. О.** – д-р техн. наук, доц., професор кафедри комп'ютеризованих систем управління, професор кафедри прикладної математики та інформаційних технологій, Державний університет «Одеська політехніка»; **Хохлячова Ю. Є.** – канд. техн. наук, доц., доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет; **Чолишкіна О. Г.** – канд. техн. наук, доц., доцент кафедри Інтелектуальних технологій, Київський національний університет імені Тараса Шевченка; **Чорний О. П.** – доктор технічних наук, професор, директор Навчально-наукового інституту електричної інженерії та інформаційних технологій, Кременчуцький національний університет імені Михайла Остроградського; **Юдін О. К.** – д-р техн. наук, проф., директор центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; **Гопеснко Віктор** – dr. sc. ing., проф., проректор з наукової роботи, директор навчальної програми магістратури «Комп'ютерні системи», Університет прикладних наук ISMA (Латвійська Республіка); **Leszczyna Rafal** – dr hab. inż., професор кафедри комп'ютерних наук у менеджменті, Гданський технологічний університет (Республіка Польща); **Ivannikova Viktoriia** – Дублінський міський університет (Республіка Ірландія).

Реєстрація суб'єкта у сфері друкованих медіа:

Рішення Національної ради України з питань телебачення і радіомовлення № 1173 від 11.04.2024 року.
Ідентифікатор медіа: R30-03890

Суб'єкт у сфері друкованих медіа – Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» (вул. Фрометівська, буд. 2, м. Київ, 03039, iart@iart.edu.ua, тел. (044) 490-95-00).

Мова видання: українська, англійська, німецька, французька та польська.
Періодичність видання: 4 рази на рік.

Відповідно до Наказу МОН України № 1290 від 30 листопада 2021 року (додаток 3) журнал включено до Переліку наукових фахових видань України (категорія Б) зі спеціальностей F2 – Інженерія програмного забезпечення; F3 – Комп'ютерні науки; F4 – Системний аналіз та наука про дані; F5 – Кібербезпека та захист інформації; F6 – Інформаційні системи і технології; F7 – Комп'ютерна інженерія.

Усі електронні версії статей журналу оприлюднюються на офіційній сторінці видання
<http://journals.maup.com.ua/index.php/it>

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення
StrikePlagiarism.com від польської компанії Plagiat.pl.

*Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 11 dated 10 December 2025)*

Information Technology and Society / [chief editor Ivan Ostroumov]. – Kyiv : Interregional Academy of Personnel Management, 2025. – Issue 4 (19). – 222 p.

Journal «Information Technology and Society» is a peer-reviewed scientific edition, which publishes materials of scientists of various levels in the form of scientific articles for the purpose of their dissemination both among domestic researchers and abroad.

Editorial board do not necessarily reflect the position expressed by the authors of articles, and are not responsible for the accuracy of the data and references.

Chief editor: Ivan Ostroumov – Doctor of Technical Sciences, Professor, Professor at the Department of Computer Information Systems and Technologies, Interregional Academy of Personnel Management

Editorial Board:

Mykola Vasylenko – Doctor of Physics and Mathematics, Professor, Professor at the Department of Cybersecurity, National University «Odesa Law Academy»; **Ivan Horbov** – PhD in Engineering, Senior Research Associate, Senior Research Fellow, Institute for Information Recording of NAS of Ukraine; **Andrii Dudnik** – Doctor of Engineering, Associate Professor, Senior Lecturer at the Department of Networking and Internet Technologies, Taras Shevchenko National University of Kyiv; **Serhii Yevseiev** – Doctor of Engineering, laureate of the 2024 National Prize of Ukraine named after Borys Paton, Professor at the Department of Cybersecurity, National Technical University “Kharkiv Polytechnic Institute”; **Serhii Zybin** – Doctor of Engineering, Associate Professor, Head of the Department of Software Engineering, National Aviation University; **Serhii Kavun** – Doctor of Economics, PhD in Engineering, Professor, Head of the Department of Computer Information Systems and Technologies Interregional Academy of Personnel Management; **Larysa Komarova** – Doctor of Engineering, Senior Research Scientist, Laureate of State Prize, Director of Educational-Scientific Institute of Information Security and Strategic Communications, National Academy of the Security Service of Ukraine; **Tetiana Okhrimenko** – PhD in Engineering, Senior Research Scientist at the Scientific Research Laboratory for Countering Aviation Cyberthreats, National Aviation University; **Oleksandr Popov** – Corresponding Member of NAS of Ukraine, Doctor of Engineering, Professor, Acting Director of the Center for Information-Analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine; **Mykola Rudnichenko** – PhD in Engineering, Associate Professor, Senior Lecturer at the Department of Information Technologies, Odessa Polytechnic State University; **Ruslan Skuratovskyi** – PhD in Physics and Mathematics, Associate Professor, Senior Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of Personnel Management; **Olha Suprun** – PhD in Physics and Mathematics, Associate Professor, Senior Lecturer at the Department of Software Systems and Technologies, Taras Shevchenko National University of Kyiv; **Halyna Tabunshchik** – PhD in Engineering, Professor, Professor at the Department of Software Tools, “Zaporizhzhia Polytechnic” National university; **Oleksandr Fomin** – Doctor of Engineering, Associate Professor, Professor at the Department of Computerized Control Systems, Professor at the Department of Applied Mathematics and Information Technologies, Odessa Polytechnic State University; **Yuliia Khokhlachova** – PhD in Engineering, Associate Professor, Senior Lecturer at the Department of Information Technology Security, National Aviation University; **Olha Cholyshkina** – PhD in Engineering, Associate Professor, Associate Professor at the Department of Intellectual Technologies, Taras Shevchenko National University of Kyiv; **Oleksii Chorny** – Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Institute of Electrical Engineering and Information Technologies, Kremenchuk National University named after Mykhailo Ostrogradskyi; **Oleksandr Yudin** – Doctor of Engineering, Professor, Director of the Cybersecurity Center of the Educational-Scientific Institute of Information Security and Strategic Communications, National Academy of the Security Service of Ukraine; **Hopeienko Viktor** – dr. sc. ing., Professor, Vice Rector for Research, Director of the study programme “Computer systems”, ISMA University of Applied Sciences (Republic of Latvia); **Leszczyna Rafal** – dr hab. inż., Profesor, Katedra Informatyki w Zarządzaniu, Politechnika Gdańska (Republic of Poland); **Ivannikova Viktoriia** – Dublin City University (Ireland).

Registration of Print media entity:

*Decision of the National Council of Television and Radio Broadcasting of Ukraine: Decision No. 1173 as of 11.04.2024.
Media ID: R30-03890*

Media entity – Private Joint-Stock Company «Higher education institution «Interregional Academy of Personnel Management» (03039, Kyiv, Frometivska str., 2, iapm@iapm.edu.ua, tel. (044) 490-95-00).

*Language of publication: Ukrainian, English, German, French, and Polish.
Periodicity: 4 times a year.*

According to the Decree of MES No. 1290 (Annex 3) dated November 30, 2021, the journal was included in the List of scientific professional publications of Ukraine (category B) in specialties F2 – Software Engineering; F3 – Computer Sciences; F4 – Systems Analysis and Data Science; F5 – Cybersecurity and Data Protection; F6 – Information Systems and Technologies; F7 – Computer Engineering.

All electronic versions of articles in the collection are available on the official website edition
<http://journals.maup.com.ua/index.php/it>

The articles were checked for plagiarism using the software
StrikePlagiarism.com developed by the Polish company Plagiat.pl.

ЗМІСТ

Павло БАЛИЧ

МЕТОДОЛОГІЧНІ ОСНОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДТРИМКИ
ТА ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ ЛОГІСТИКИ ПОСТАЧАВАННЯ.....8

Володимир БРОДКЕВИЧ, Олександр ЧЕРНІЧЕНКО

РОЗРОБКА ВЕБ-ДОДАТКУ ДЛЯ УПРАВЛІННЯ ЗАДАЧАМИ
З РЕАЛІЗАЦІЄЮ АЛГОРИТМІВ ПРІОРИТИЗАЦІЇ ТА СОРТУВАННЯ.....13

Тетяна ВАКАЛЮК, Микола ФАНТ, Денис ФУРІХАТА, Олег ВЛАСЕНКО, Вадим КОЛОМІЄЦЬ

ОГЛЯД НАЯВНИХ МЕТОДІВ АНАЛІЗУ ДАНИХ
ДЛЯ РОЗРОБКИ СИСТЕМИ ВСТАНОВЛЕННЯ ПОПИТУ ТОВАРІВ23

Анастасія ВОЗНИЦЯ

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ AGILE-МЕНЕДЖМЕНТУ ЗА ДОПОМОГОЮ N8N:
СТВОРЕННЯ ІНТЕЛЕКТУАЛЬНОЇ ЕКОСИСТЕМИ УПРАВЛІННЯ ПРОЄКТАМИ29

Владислав ГОЛЕЦЬ, Ганна САРИБОГА

ПРОГРАМНИЙ КОМПЛЕКС ДЛЯ ПРОГНОЗУВАННЯ ЕНЕРГОСПОЖИВАННЯ ТА МОНІТОРИНГУ
СТАНУ ВИРОБНИЧОГО ОБЛАДНАННЯ НА ОСНОВІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ.....33

Галина ГРИГОРЧУК, Любомир ГРИГОРЧУК, Оксана ГРИГОРЧУК

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СУШІННЯ УТФЕЛЮ В БАРАБАННІЙ СУШАРЦІ39

Наталія ДОЦЕНКО, Ярослав ЛУЦІВ

РОЗРОБКА МОДЕЛІ ІНСТРУМЕНТАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ТРАНСФОРМАЦІЇ
ПРОЦЕСІВ УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ В МУЛЬТИПРОЄКТНОМУ СЕРЕДОВИЩІ45

Віталій ЖЕПЛІНСЬКИЙ, Михайло ЛУЧКЕВИЧ

ГІБРИДНА МОДЕЛЬ ГЕНЕРАЦІЇ ТЕСТОВИХ СЦЕНАРІЇВ НА ОСНОВІ LLM ТА АНАЛІЗУ ІСТОРІЇ ДЕФЕКТІВ.....50

Ганна ЗАВГОРОДНЯ, Валерій ЗАВГОРОДНІЙ

МОДЕЛЬ ПРОГНОЗУВАННЯ ПОВЕДІНКИ ГРАВЦІВ У МОБІЛЬНИХ ІГРАХ
НА ОСНОВІ МАШИННОГО НАВЧАННЯ55

Вадим ЗЮЗЮН, Анастасія АВРАМЕЦЬ

МОДЕЛЬ ТА КРИТЕРІЙ ОЦІНКИ ЕФЕКТИВНОСТІ ІНТЕЛЕКТУАЛЬНОЇ ФІЛЬТРАЦІЇ СПОВІЩЕНЬ
ДЛЯ ІТ-ФАХІВЦІВ.....61

Юлія КАМЕНЕЦЬКА, Роман АРТЕМЕНКО, Аліна КОВАЛЬ

AI-РЕФЕРЕНСИ ЯК ІНСТРУМЕНТ ФОРМУВАННЯ ВІЗУАЛЬНОГО СТИЛЮ У ЦИФРОВОМУ ДИЗАЙНІ.....68

Alia KARITON, Tamara FRANCHUK, Dmytro TYSHCHENKO, Alona DESIATKO, Maksym SVYSTUN

ADVANTAGES AND DISADVANTAGES OF IOS 2674

Світлана КАШКЕВИЧ, Олена НЕЧИПОРУК, Наталія АПЕНЬКО, Ірина БРАНОВИЦЬКА

МЕТОД ОПТИМІЗАЦІЇ МАРШРУТІВ НА ОСНОВІ ПОВЕДІНКИ ЗМІЙ В СИСТЕМАХ ОБМІНУ ДАНИМИ БПЛА.....78

Наталія КІЦЕЛЬ, Євген ВОЛКАНІН, Оксана БОРИСЕНКО, Валерій МАТВЄЄВ, Володимир МАЛЬОВАНІЙ

КОМПЛЕКСНИЙ АНАЛІЗ ШКІДЛИВИХ ПРОГРАМ: ПІДХОДИ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ83

Олександр КОРНІЙЧУК, Марина ГРАФ

МЕТОД ОПТИМІЗАЦІЇ ПРОЦЕДУРИ ВИБОРУ ПЕРЕМОЖЦЯ В СИСТЕМАХ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ
ШЛЯХОМ ІНТЕГРАЦІЇ ПАРАМЕТРІВ РИЗИКУ88

Олександр ЛАСТІВКА

МЕТОД ОБРОБКИ РІЗНОТИПНИХ ДАНИХ В КАНАЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ БПЛА94

Дмитро МАРЧУК

АНАЛІЗ МЕТОДІВ СТИСНЕННЯ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ
ДЛЯ ЕФЕКТИВНОГО РОЗГОРТАННЯ У СЕРЕДОВИЩІ EDGE AI98

Юрій МАСЛОВ, Юрій БОРЗУНОВ АВТОМАТИЗАЦІЯ ПРОЦЕСІВ У ТРАНСПОРТНИХ ЕЛЕКТРОМЕХАНІЧНИХ СИСТЕМАХ НА БАЗІ ІОТ-ТЕХНОЛОГІЙ	106
Valerii MYKHAILOV AN OVERVIEW OF THE CURRENT STATE AND FUTURE PROSPECTS OF RESPIRATORY GAS SUPPLY MANAGEMENT SYSTEMS	113
Руслан МОРОЗОВ, Володимир ДОНЕЦЬ РОЗРОБКА МЕТОДУ RAG ДЛЯ НАДАННЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ КОРИСТУВАЧАМ	121
Євген ПАТЛАНЬ, Ірина БІЛОУС МЕТОД АВТОМАТИЗОВАНОЇ МІГРАЦІЇ ДАНИХ МІЖ ВАРІАНТАМИ СХОВИЩ У СИСТЕМАХ З БАГАТОВАРІАНТНОЮ ПЕРСИСТЕНТНІСТЮ	129
Дмитро ПЕРСУНОВ ТЕХНОЛОГІЯ КОНТРОЛЮ ТА ВІДНОВЛЕННЯ ЦІЛІСНОСТІ ДАНИХ У РОЗПОДІЛЕНИХ СХОВИЩАХ.....	140
Сергій РЕВА, Денис ЦИБЛІЄВ РОЗРОБКА МЕТОДУ КОМП'ЮТЕРНОГО АНАЛІЗУ ПАРАМЕТРІВ СПЕКТРОМЕТРИЧНИХ СИГНАЛІВ З ВИКОРИСТАННЯМ ДИСКРЕТНИХ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ	144
Микита СМОЛЕНСЬКИЙ, Євген СІДЕНКО ФОРМАЛІЗАЦІЯ ТЕХНІЧНИХ ВИМОГ ДО ЗАСОБІВ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЯ В КОНТЕКСТІ ПОКРАЩЕННЯ ПРОЦЕСУ НАДАННЯ МЕДИЧНИХ ПОСЛУГ	154
Андрій СУДИН, Лукаш СЦІСЛО, Андрій ПЕРЕКРЕСТ, Юрій ОНИЩЕНКО ГІБРИДНА НЕЙРОМЕРЕЖЕВА МОДЕЛЬ ВИЯВЛЕННЯ ТА КІЛЬКІСНОЇ ОЦІНКИ РИЗИКУ ТАРГЕТОВАНИХ АТАК НА SCADA/ICS СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	162
Ольга СУПРУН, Мар'яна МУСІЙОВСЬКА, Тетяна ЛАВРИК ВИКОРИСТАННЯ СТЕГANOГРАФІЧНИХ ПРОТОКОЛІВ У ЗАХИСТІ ВІДЕОДАНИХ В УМОВАХ ІНФОРМАЦІЙНИХ АТАК.....	170
Олег ТИЩЕНКО РЕГУЛЯТОРНІ ПІДХОДИ ДО ВИКОРИСТАННЯ БПЛА: МОДЕЛІ ЗОНУВАННЯ ПОВІТРЯНОГО ПРОСТОРУ ..	177
Олександр ХОМЕНКО, Олександр КОВАЛЬ АНАЛІЗ СЦЕНАРІЇВ КАСКАДНИХ ЕФЕКТІВ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ НА ОСНОВІ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ	182
Євгеній ЧИЧИКАЛО, Віра ШЕНДРИК ПРОГРАМНИЙ МОДУЛЬ МОНІТОРИНГУ АКУМУЛЯТОРНИХ БАТАРЕЙ ДЛЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ З ВИКОРИСТАННЯМ ЦИФРОВОГО ДВІЙНИКА	191
Ірина ЧУБ, Катерина ДЕМЧЕНКО, Сергій ТИМЧУК АВТОМАТИЗОВАНА ІДЕНТИФІКАЦІЯ БІОЕСТИМАТОРІВ АКТИВНОГО МУЛУ НА ОСНОВІ МЕРЕЖЕВОЇ МОДЕЛІ YOLOV8	199
Лідія ШТАЄР, Наталія ВОЗНА, Володимир ГРИГА, Леся МИЧУДА, Оксана БЕЛЕЙ ПІДВИЩЕННЯ СТІЙКОСТІ АКУСТИЧНОГО МЕТОДУ КОНТРОЛЮ ВИТОКІВ ШЛЯХОМ ЗАСТОСУВАННЯ ЕНТРОПІЙНИХ ТА РЕЛЯЦІЙНИХ ОЗНАК	206
Ігор КОЛІСНИК, Андрій ДУДНІК, Дарина ЯРЕМЕНКО, Владислав ФЕСЕНКО МЕТОДИ РОЗПІЗНАВАННЯ ТА СЕГМЕНТАЦІЇ АЕРОФОТО ДЛЯ ЦИФРОВИХ КАРТ	214

УДК 004.72:531.7.08

DOI <https://doi.org/10.32689/maup.it.2025.4.27>**Олег ТИЩЕНКО**

аспірант кафедри комп'ютерно-інформаційних систем і технологій,

ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», 0987651234um@gmail.com

ORCID: 0009-0001-2763-579X

**РЕГУЛЯТОРНІ ПІДХОДИ ДО ВИКОРИСТАННЯ БПЛА:
МОДЕЛІ ЗОНУВАННЯ ПОВІТРЯНОГО ПРОСТОРУ**

Анотація. Стаття систематизує підходи до інтеграції безпілотних повітряних апаратів у публічний простір із фокусом на моделях зонування повітряного простору та суміжних правових і технічних режимах. Роз'яснено, як поєднуються категорії експлуатації, цифрові служби керування польотами, віддалена ідентифікація апаратів, відкритість і формат даних про обмеження. Порівняно європейську модель із практиками США та окреслено український контекст воєнного і післявоєнного періодів. Доведено, що саме зонування створює керовану рамку: юридично визначені географічні зони, вимоги до ідентифікації та ризик-орієнтована авторизація операцій поєднуються з цифровими сервісами взаємодії між провайдерами послуг, органами обслуговування повітряного руху та операторами. Запропоновано для громад трирівневу модель впровадження (правовий, технологічний і процедурний шари) та послідовну дорожню карту гармонізації, де ключем є публікація геозон у спільному машиночитному форматі, дослідні сектори цифрових сервісів і впровадження віддаленої ідентифікації. Практична цінність полягає в наданні зрозумілих критеріїв оцінювання, прикладах міських сценаріїв і типових адміністративних рішень, що зменшують витрати для держави та операторів і водночас підвищують безпеку, прозорість та повагу до приватності громадян.

Ключові слова: географічні зони безпілотників, цифрові служби керування польотами, віддалена ідентифікація, оцінювання ризиків, місцеве регулювання, приватність, міське зонування.

**Oleg TYSHCHENKO. REGULATORY APPROACHES TO THE USE OF UAS IN PUBLIC SPACE:
AIRSPACE ZONING MODELS**

Abstract. The article systematizes approaches to integrating unmanned aircraft into the public space, focusing on airspace zoning models and related legal and technical regimes. It explains how operational categories, digital flight management services, remote identification of aircraft, and the openness and formats of restriction data fit together. The European model is compared with U.S. practices, and the Ukrainian wartime and post-war context is outlined. It is demonstrated that zoning creates a governable framework: legally defined geographical zones, identification requirements, and risk-oriented authorization of operations are combined with digital services enabling interaction among service providers, air traffic services, and operators. For municipalities, a three-tier implementation model (legal, technological, and procedural layers) and a phased harmonization roadmap are proposed, with key elements being the publication of geozones in a shared machine-readable format, pilot sectors for digital services, and the deployment of remote identification. The practical value lies in providing clear evaluation criteria, examples of urban scenarios, and typical administrative decisions that reduce costs for the state and operators while increasing safety, transparency, and respect for citizens' privacy.

Key words: geographical zones for unmanned aircraft, digital flight management services, remote identification, risk assessment, local regulation, privacy, urban zoning.

Вступ. Швидке поширення безпілотників у містах, над об'єктами критичної інфраструктури та під час публічних заходів створює одразу кілька викликів. Потрібно водночас забезпечити безпеку людей і польотів, захист приватності, передбачуваність для бізнесу та доступність інноваційних послуг. Підхід, що базується лише на заборонах, не працює в реальному житті: міське середовище змінне, а потреби – різноманітні. Відтак потрібен порядок, у якому правила не тільки забороняють, а й дозволяють безпечні дії за зрозумілих умов. Таку логіку задає зонування повітряного простору та супутні цифрові сервіси.

Огляд досліджень і практик. Європейська модель надає державам право визначати географічні зони для безпілотників і зобов'язує публікувати їх у спільному машиночитному форматі. Такі зони описують, де саме і за яких умов можливі польоти: наприклад, із обмеженням висоти, з потребою попереднього дозволу, у визначені години, із застереженнями щодо приватності або довкілля. Окрема частина правил присвячена вимогам до самих апаратів: класам, маркуванню та засобам віддаленої ідентифікації, які дають змогу встановити, що саме летить, ким керується і чи дотримується меж дозволеної зони. Для масштабних операцій запроваджено набір цифрових сервісів, які забезпечують

інформаційну підтримку польотів: повідомляють про зони, допомагають планувати маршрути, попереджають про конфлікти та підтверджують дозвіл.

США демонструють іншу траєкторію, однак із близькою метою. Там діє система швидких дозволів поблизу аеропортів, яка спирається на публічні сітки висот і дає можливість отримати погодження практично в режимі реального часу. Віддалена ідентифікація оголошена обов'язковою, але передбачені винятки для спеціально визначених майданчиків, що підтримують аматорську діяльність. Обидві моделі, попри відмінності, сходяться в одному: без відкритих даних про зони та без надійної ідентифікації говорити про масове безпечне використання безпілотників неможливо.

Україна до повномасштабної війни використовувала загальні авіаційні правила з базовими обмеженнями. Після 2022 року діють особливі режими повітряного простору: пріоритет безпеки та централізоване дозвілля польотів. У 2025 році частину вимог спрощено, але стратегічне завдання лишається незмінним – поступова гармонізація з європейською моделлю після зняття надзвичайних обмежень і створення зрозумілих міських рішень для повсякденних потреб.

Мета дослідження. Мета статті – запропонувати цілісну модель зонування простору для безпілотників, зрозумілу органам місцевого самоврядування, операторам і громадянам. Ідеться про поєднання правових рішень, відкритих даних і прозорих адміністративних процедур так, щоб місто могло безпечно дозволяти корисні польоти, а не тільки щось забороняти.

Виклад основного матеріалу. Насамперед зауважимо, що дослідження спирається на аналіз європейських регламентів щодо експлуатації безпілотних повітряних апаратів, вимог до виробів і комплексу цифрових служб підтримки польотів, а також на огляд методик оцінювання ризиків і практик країн, де такі рішення уже працюють. До цього блоку входять базові акти Європейського Союзу про порядок виконання польотів безпілотниками, вимоги до продукції та набір цифрових сервісів керування рухом у спеціально визначених секторах повітряного простору [1–4]. Для зіставлення використано американський досвід швидких дозволів поблизу аеропортів і віддаленої ідентифікації апаратів [11–12; 27–29]. Окрему увагу приділено українським документам, що визначають особливий порядок польотів у період воєнного стану і містять орієнтири для подальшої гармонізації з правом ЄС [13–16; 18–20]. Для практичних висновків розглянуто відкриті портали з даними про зони та офіційні набори даних, які застосовуються для надання дозволів, зокрема поблизу аеропортів [6–7; 29].

По суті, логіка зонування повітряного простору у Європі полягає в тому, що держава визначає географічні зони різних типів і зобов'язана оприлюднювати їх у спільному машиночитному форматі. Найжорсткіший тип – повна заборона польотів над місцями підвищеної небезпеки або чутливими об'єктами. Поширенішим є підхід «дозволено з умовами»: польоти допускаються лише до певної висоти, у встановлений час, після попереднього дозволу або за умови, що апарат передає свою ідентифікацію та параметри польоту. Вимога публікувати зони у структурованому форматі означає не просто наявність статичної карти на сайті, а доступність даних, які автоматично зчитують наземні картографічні програми та бортові системи безпілотників. Це передбачено в керівних матеріалах Європейського агентства з авіаційної безпеки, де докладно описано структуру даних і приклади національних впроваджень такого формату [5–7; 30].

З іншого боку, вимоги до самих апаратів доповнюють цю систему. Регламент щодо продукції запроваджує класифікацію виробів і визначає засоби віддаленої ідентифікації, які дозволяють встановити, який саме апарат перебуває у повітрі, хто відповідає за політ і чи виконує він умови конкретної зони. Завдяки цьому органи безпеки та, за визначених обставин, громадськість отримують можливість контролю та реагування. Там, де відбувається значна кількість польотів, до роботи залучається комплекс цифрових служб: вони надають операторові актуальні дані про зони, допомагають планувати маршрут, попереджають про можливі конфлікти та підтверджують дозвіл. Такий підхід перетворює розпорошену активність на керований процес із прозорими правилами та відповідальністю сторін [2–4; 8].

Американський досвід, розглянутий крізь призму потреб міст, демонструє, як поєднання публічних даних і простих процедур різко скорочує час очікування дозволу. Навколо аеропортів опубліковано сітки максимально допустимих висот, і якщо параметри польоту узгоджуються із сіткою, цифрові застосунки видають погодження практично миттєво. Паралельно діє загальна вимога віддаленої ідентифікації апаратів, а для визначених майданчиків, що підтримують аматорську діяльність, існують винятки з цієї вимоги. Така комбінація – відкриті дані про обмеження плюс оперативні дозволи – є показовою для міських умов, де важливі і швидкість ухвалення рішень, і безпека [11–12; 27–29].

Український контекст суттєво відрізняється через війну: у період надзвичайних обставин пріоритет надано безпеці, діє особливий порядок польотів із централізованими дозволами та розширеними обмеженнями. Разом із тим завдання повоєнної відбудови вже зараз вимагає підготовки до керованої інтеграції безпілотників у повсякденне міське життя. Доцільним є опис місцевих зон

у машиночитному форматі, визначення типових сценаріїв, які після скасування надзвичайних обмежень можна буде дозволяти автоматично або за спрощеною процедурою, а також пілотування виділених сегментів міського повітряного простору, де цифрові служби підтримують безпечні інспекції, фотозйомку муніципальних подій та логістичні перевезення [13–16; 18–20; 30–31].

Оскільки повітряна зйомка торкається приватного життя людей, будь-яке місцеве рішення має спиратися на принципи необхідності та пропорційності. Якщо зйомка проводиться, громадяни повинні бути завчасно поінформовані; зібрані матеріали слід обробляти з мінімальним обсягом персональних даних, а також забезпечити зрозумілий механізм подання скарг і видалення матеріалів у разі порушень. У зонах із підвищеною чутливістю, наприклад біля лікарень, навчальних закладів або місць скупчення людей, варто встановлювати обмежувальні зони з чітким правовим обґрунтуванням і прозорим описом умов, за яких можливі винятки. Ці підходи ґрунтуються на висновках європейських органів із захисту даних і відповідають сучасній практиці міст, що використовують безпілотики в інтересах громади, але з повагою до приватності [21].

Практична архітектура місцевої політики доцільно вибудовується у три шари. Перший – правовий – визначає сталий перелік постійних і тимчасових географічних зон, порядок зйомки публічних заходів, обов'язок використовувати засоби віддаленої ідентифікації, а також відповідальність за порушення. Тут важливо узгодити місцеві рішення з національними документами з авіаційної інформації, щоб уникнути суперечностей та подвійних тлумачень [1; 13–14; 26]. Другий – технологічний – забезпечує дані: місто публікує зони у спільному машиночитному форматі, надає стабільні програмні інтерфейси доступу, поєднує на одній карті місцеві обмеження та тимчасові повідомлення. До цієї ж площини належить технічна сумісність із механізмами міждержавного обміну реєстраційними даними в Європейському Союзі, аби національні служби могли коректно підтверджувати відомості про операторів і апарати [5–7; 29–31]. Третій – процедурний – організовує сервіси для людей і операторів: зрозумілі електронні форми заяв на типові дії (інспекція даху, обстеження споруди, зйомка заходу), чітко прописані умови виконання, скорочені строки розгляду для низькоризикових сценаріїв, а також публічні журнали виданих дозволів для прозорості процесів [3; 9–12].

Щоби оцінювати дієвість політики, пропонується набір простих і водночас показових індикаторів. Ключовим є відсоток місцевих зон, оприлюднених у машиночитному форматі, адже без якісних даних автоматизація неможлива. Не менш важливий середній час розгляду заяв для низького ризику: зменшення цього показника свідчить про налаштовані процеси й зрозумілі вимоги. Вартими уваги є частка польотів із активною віддаленою ідентифікацією, кількість інцидентів на тисячу польотів та результати опитувань мешканців і операторів щодо зручності карт і сервісів. Такі метрики узгоджуються з європейськими підходами до цифровізації даних про зони, американською практикою оперативних дозволів і методиками ризик-орієнтованого регулювання [5; 12; 21; 29–30].

Технічні засоби підтримки є необхідною умовою успіху. Віддалена ідентифікація фактично виконує роль «цифрового номерного знака» у небі: апарат періодично передає свій ідентифікатор і основні параметри польоту, що дає змогу контролювати дотримання правил, пришвидшувати реагування служб і розв'язувати спірні ситуації. Паралельно міські зони мають публікуватися у форматі, який безпосередньо сприймають програмні засоби – і наземні, і бортові. Тільки тоді карти міста, застосунки операторів і обладнання виробників працюватимуть узгоджено. Для транскордонної сумісності важливо врахувати механізми обміну реєстраційними даними, які впроваджує Європейський Союз, і забезпечити можливість перевірок на національному рівні [2; 5–7; 22–24; 31].

Разом із тим слід бачити ризики та заздалегідь пропрацьовувати запобіжники. Фрагментація даних – коли різні підрозділи публікують зони у різних форматах або з різною якістю – долається запровадженням єдиного міського порталу з чіткими правилами публікації та відповідальною службою за дані. Ризик надмірних обмежень для зйомки й збору інформації зменшується через попередні оцінки впливу на приватність, мінімізацію персональних даних і прозорі повідомлення громадянам. Перевантаження дозвільних каналів контролюється завдяки типізації сценаріїв і наданню спрощених дозволів для низького ризику. Проблеми з нелегальними або немаркованими апаратами зменшуються завдяки системним перевіркам віддаленої ідентифікації в полі та інформаційним кампаніям для користувачів [11; 21; 22–24; 27–30].

У міських умовах уже зараз можна виокремити кілька показових сценаріїв. Інспекція фасадів і дахів у щільній забудові досягає прийняттого рівня безпеки за умови дотримання обмежень висоти, витримування буферів над місцями пересування пішоходів і постійної віддаленої ідентифікації апарата. Обстеження мостів та інших інженерних споруд потребує погоджених маршрутів і часових «вікон», аби уникнути конфліктів із рухом транспорту та людьми. Зйомка публічних заходів можлива в межах тимчасової зони, заздалегідь позначеної на міській карті, з чіткими умовами і зрозумілими

оголошеннями для мешканців. Логістичні польоти у промислових та малозаселених районах доцільно виконувати у виділених сегментах повітряного простору, де працюють цифрові служби попередження зіткнень і підтвердження дозволів [1–4; 8–12].

Послідовність упровадження для громад має бути поетапною. Спочатку впорядковується правова база: ухвалюється локальне положення про зони, описуються типові сценарії та їхні умови, визначаються відповідальні органи. Далі формується набір відкритих даних: постійні й тимчасові зони публікуються у машиночитному форматі з описом структури та регламентом оновлення. Наступним кроком стають пілотні проекти – тимчасові зони для заходів або інспекцій, навчання адміністраторів і користувачів, канали зворотного зв'язку. На етапі масштабування визначаються ділянки повітряного простору, де потрібні цифрові служби підтримки польотів, укладаються угоди щодо рівня якості цих сервісів, забезпечується сумісність із національними системами. На зрілому етапі частина дозволів для низького ризику надається автоматично, регулярно проводяться перевірки впливу на приватність і публікуються квартальні звіти з ключовими показниками ефективності [3; 5–7; 12; 21; 31].

Узагальнюючи, викладений матеріал показує, що керована інтеграція безпілотників у міський простір спирається на три стовпи: зони, які зрозуміло описані та визначені; ідентифікація апаратів, яка забезпечує прозорість і відповідальність; цифрові служби, які перетворюють окремі польоти на безпечну та передбачувану систему. Європейські правила, американські рішення щодо оперативних дозволів і українські реалії воєнного часу вказують на спільний знаменник: без якісних даних, прозорих процедур і продуманої взаємодії з громадянами досягти балансу між безпекою, правами людини та інноваціями неможливо [1–4; 11–12; 13–16; 21; 29–31].

Висновки. Зонування повітряного простору у поєднанні з віддаленою ідентифікацією та цифровими сервісами – найкоротший шлях до безпечної і прогнозованої інтеграції безпілотників у міста. Успіх залежить від якості даних, узгоджених місцевих правил і простих процедур для людей та операторів. Україні доцільно готуватися до гармонізації з європейською моделлю вже зараз: описувати зони в машиночитному форматі, запускати пілотні сегменти міського простору та робити правила прозорими і зручними. Подальші дослідження варто спрямувати на створення репозиторію міських пілотів, оцінювання впливу на безпеку й приватність та вироблення справедливих моделей оплати послуг для підтримки польотів.

Список використаних джерел:

1. Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32019R0947>
2. Commission Delegated Regulation (EU) 2019/945 (consolidated 01.05.2025) on unmanned aircraft systems. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A02019R0945-20250501>
3. Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32021R0664>
4. EASA. Easy Access Rules for U-space (EU) 2021/664. URL: <https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-u-space-regulation-eu-2021664>
5. EASA. Easy Access Rules for UAS: AMC/GM to Article 15 (digital format for zones, ED-269). URL: <https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems>
6. EASA. Geo-Zones – know where to fly your drone. URL: <https://www.easa.europa.eu/en/light/topics/geo-zones-know-where-fly-your-drone>
7. Irish Aviation Authority. UAS Geographical Zones (example of ED-269/GeoJSON publication). URL: <https://www.iaa.ie/general-aviation/drones/uas-geographic-zones>
8. SESAR JU. Implementation of U-space airspace in a restricted area. URL: <https://www.sesarju.eu/sesar-solutions/implementation-u-space-airspace-restricted-area-uncontrolled-airspace>
9. JARUS. SORA v2.5 (2024): Main Body. URL: https://jarus-rpas.org/wp-content/uploads/2024/06/SORA-v2.5-Main-Body-Release-JAR_doc_25.pdf
10. EASA. Specific Operations Risk Assessment (SORA) – overview. URL: <https://www.easa.europa.eu/en/domains/drones-air-mobility/operating-drone/specific-category-civil-drones/specific-operations-risk-assessment-sora>
11. Federal Register. Remote Identification of Unmanned Aircraft (Final Rule; Part 89). URL: <https://www.federalregister.gov/documents/2021/01/15/2020-28948/remote-identification-of-unmanned-aircraft>
12. UAS Facility Maps (LAANC). URL: https://www.faa.gov/uas/commercial_operators/uas_facility_maps
13. Державіаслужба України. Безпілотні повітряні судна (довідкова сторінка). URL: <https://avia.gov.ua/bezpilotni-povitryani-sudna-2/>
14. Авіаційні правила України «Загальні правила польотів у повітряному просторі України». URL: <https://zakon.rada.gov.ua/go/z0654-17>
15. Міністерство оборони України. Спрощення правил використання БПЛА під час воєнного стану (17.07.2025). URL: <https://mod.gov.ua/en/news/ministry-of-defence-simplifies-regulations-for-using-ua-vs>
16. Інститут масової інформації. Зйомки з використанням дронів: воєнний стан та зміни до законодавства (аналітика). URL: <https://imi.org.ua/monitorings/zjomky-z-vykorystanniam-droniv-voyennyj-stand-ta-zminy-do-zakonodavstva-i54375>

17. Liability for Violating the Procedure for Airspace Usage by Unmanned Aircraft in Ukraine (огляд). URL: https://www.researchgate.net/publication/357743848_Liability_for_Violating_the_Procedure_for_Airspace_Usage_by_Unmanned_Aircraft_in_Ukraine/fulltext/61dda03a5c0a257a6fdf3ab8/Liability-for-Violating-the-Procedure-for-Airspace-Usage-by-Unmanned-Aircraft-in-Ukraine.pdf
18. Наказ Міністерства інфраструктури №478 від 28.10.2011 «Правила польотів цивільних повітряних суден України». URL: <https://zakon.rada.gov.ua/laws/show/z1327-11>
19. Міністерство розвитку громад. Порядок дозволів на польоти державних повітряних суден за дозволом Генштабу (28.05.2025). URL: <https://mindev.gov.ua/storage/app/sites/1/uploaded-files/poriadok-15676476.pdf>
20. State Aviation Administration of Ukraine (EN). Notices on airspace closure for civil flights (war). URL: <https://avia.gov.ua/en/page/4/?s=i>
21. Article 29 Working Party / EDPB. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. URL: <https://ec.europa.eu/newsroom/article29/redirection/item/640602>
22. European Commission Implementing Decision (EU) 2024/2103 on harmonised standard for direct remote identification. Overview. URL: <https://www.unmannedairspace.info/uncategorized/european-commission-publishes-decision-on-remote-id-harmonised-standards/>
23. Irish Aviation Authority. Guidance on Direct Remote ID (UAM-014). URL: <https://www.iaa.ie/docs/default-source/publications/advisory-memoranda/uas-advisory-memoranda-%28uam%29/uam-014---guidance-on-direct-remote-id-issue-1.pdf>
24. Dronetag. Remote ID explained (overview of technical options). URL: <https://help.dronetag.cz/knowledge-base/remote-id-explained>
25. Dronewatch.eu. 11 Critical Flaws in EU-wide Drone Geo-Awareness. URL: <https://www.dronewatch.eu/elevating-concerns-11-critical-flaws-in-the-current-drone-geo-awareness-system/>
26. UK CAA. Article 15 – operational conditions for UAS geographical zones (guidance). URL: https://regulatorylibrary.caa.co.uk/2019-947/Content/map/00185_art_15_Operational_conditions_for_UAS_geographical_zones.htm
27. Remote Identification – information page. URL: https://www.faa.gov/uas/getting_started/remote_id
28. FAA. FRIA Program Environmental Assessment (06.2023). URL: https://www.faa.gov/uas/advanced_operations/nepa_and_drones/FRIA-PEA-and-FONSI-ROD_Final_2023-06-29-signed.pdf
29. UAS Data Delivery System / LAANC grids. URL: <https://udds-faa.opendata.arcgis.com/>
30. EUROCONTROL. Notes on 2019/947 (requirement to publish zones in a digital format). URL: https://www.eurocontrol.int/archive_download/all/node/14966
31. EASA / Drones.gov.cy. “Broker” – EU-wide sharing of drone registration data. URL: <https://drones.gov.cy/easa-delivers-broker-solution-to-enable-european-wide-sharing-of-drone-registration-data/>

Дата надходження статті: 20.11.2025

Дата прийняття статті: 10.12.2025

Опубліковано: 30.12.2025