Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УДК 004.8
DOI: https://doi.org/10.30837/2522-9818.2025.2.033

Б. КОСАРЕВСЬКИЙ, А. ТЕЦЬКИЙ

СУЧАСНІ ПІДХОДИ ДО РОЗГОРТАННЯ ІНФРАСТРУКТУРИ МОБІЛЬНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ

Предмет дослідження – інфраструктура мобільних інтелектуальних систем (МІС) для моніторингу критичних об’єктів із застосуванням груп безпілотних літальних апаратів (БПЛА), що поєднує крайові та хмарні обчислення, методи балансування навантаження та кібербезпеки. **Мета роботи** – аналіз методів розгортання інфраструктури МІС моніторингу критичних об’єктів, орієнтованих на використання груп БПЛА. Основну увагу зосереджено на підвищенні ефективності, надійності та адаптивності таких систем унаслідок інтеграції хмарних і крайових обчислень, розроблення механізмів автоматизованого керування ресурсами, кіберзахисту та адаптації до умов експлуатації. **Завдання:** розробити архітектуру МІС з гібридним розподілом обчислень між *Edge*- та *Cloud*-компонентами; дослідити вплив механізмів балансування ресурсів на продуктивність за умови змінного навантаження; оцінити ефективність мультиканальних технологій зв’язку в разі втрати основного каналу; впровадити методи кіберзахисту для забезпечення безперебійної роботи системи. **Методи:** теоретичний аналіз наявних підходів, моделювання та симуляція для оцінювання їх продуктивності й надійності. Дослідження передбачає використання генетичних алгоритмів, ройових алгоритмів і штучних потенційних полів для управління траєкторіями ботів. **Результати дослідження.** Експериментальні випробування в середовищах *Microsoft Azure* та *CoppeliaSim EDU* підтвердили ефективність запропонованих підходів. Досягнуто зменшення середньої затримки на 35%, покращено енергоспоживання, забезпечено безперервність передачі даних у 92% сценаріїв втрати зв’язку. Аналіз надійності показав доцільність резервування компонентів і впровадження методів прогнозування, що дало змогу знизити ймовірність критичних відмов на 22% та скоротити середній час відновлення на 42%. **Висновки.** Використання автоматизованого управління ресурсами в МІС забезпечує стабільність і безперервність роботи груп БПЛА навіть у змінних умовах експлуатації. Оптимізація обчислень і адаптивне масштабування сприяють підвищенню продуктивності системи, зменшенню затримки передачі інформації та покращенню енергоспоживання. Розроблені підходи до кібербезпеки гарантують захист даних і надійність функціювання інфраструктури в разі зовнішніх загроз та мережевих атак.

Ключові слова: точкова хмара; глибинне навчання; графова нейронна мережа; автоматичне доповнення точкових хмар; кодування графів; 3D-реконструкція графових моделей.

Вступ

Сучасні технології відіграють ключову роль у забезпеченні моніторингу критичних об’єктів, що вимагає впровадження мобільних інтелектуальних систем (МІС), зокрема безпілотних літальних апаратів (БПЛА), наземних роботизованих платформ і хмарних обчислювальних технологій. Використання таких систем дає змогу значно підвищити ефективність контролю за станом стратегічно важливих інфраструктурних об’єктів, транспортних мереж і екологічно небезпечних зон, що потребують постійного спостереження та аналізу.

Розгортання інфраструктури таких систем передбачає інтеграцію передових технологій оброблення інформації, децентралізованих мереж, машинного навчання та механізмів кіберзахисту. Зокрема актуальним є впровадження *Mobile Edge Computing* (MEC) для оброблення даних безпосередньо в місці їх збору, що дає змогу мінімізувати затримки та зменшити навантаження на центральні сервери [1]. У цьому разі важливу роль відіграє ієрархічна архітектура периферійних обчислень, яка сприяє оптимізації процесів прийняття рішень та покращенню масштабованості систем.

Використання БПЛА для моніторингу критичних об’єктів допомагає підвищити автономність систем спостереження, забезпечуючи швидке розгортання мережі сенсорів і збирання інформації в режимі реального часу. Однак зростання складності таких систем спричиняє низку викликів, пов’язаних із забезпеченням надійного зв’язку, з енергоспоживанням, управлінням роєм БПЛА та протидією потенційним кібератакам [2].

Окремої уваги заслуговує безпека, оскільки системи моніторингу, що базуються на БПЛА, можуть стати об’єктами кібератак, спрямованих на злам каналів зв’язку та компрометацію переданих даних. Запропоновані в останніх дослідженнях методи захисту інформаційних потоків, зокрема комбіновані підходи, що поєднують сигнатурний аналіз та виявлення аномалій, є важливим напрямом у забезпеченні безпечного функціювання таких систем.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Крім того, автоматизація розгортання інфраструктури МІС та керування нею є ключовим чинником підвищення ефективності їх застосування в умовах мінливого середовища. Використання алгоритмів оптимізації та нейронних мереж дає змогу значно покращити точність прийняття рішень, мінімізувати вплив людського фактора та скоротити час реакції на позаштатні ситуації [3].

Отже, розгортання інфраструктури мобільних інтелектуальних систем моніторингу критичних об'єктів є складним процесом, що вимагає поєднання різних технологій і уваги до низки чинників, таких як надійність, масштабованість, безпека й ефективність управління. З огляду на сучасні виклики та тенденції подальші дослідження в цьому напрямі мають бути спрямовані на розроблення нових підходів до інтеграції МЕС, оптимізацію алгоритмів керування групами БПЛА та впровадження вдосконалених механізмів кіберзахисту [4].

Аналіз останніх досліджень і публікацій

Робота С. Лютфі та інших [5] демонструє інтеграцію МЕС у 6G-мережі, що дає змогу оптимізувати передачу інформації між мобільними агентами. Т. Хуан [6] досліджує оптимізацію якості обслуговування в МЕС для IoT, що є актуальним для моніторингу критичних об'єктів. А. Рахмані та інші [7] запропонували використання блокчейн-технологій у МЕС, що підвищує безпеку оброблення даних. Крім того, автори статті [8] досліджують флюїдні антени, які покращують адаптивність МЕС-систем.

А. Фірузі [9] розглядає використання штучного інтелекту (AI) та Інтернету речей (IoT) для дистанційного моніторингу критичної інфраструктури. Автор аналізує найкращі практики розгортання та експлуатації таких систем, що має важливе значення для мобільних інтелектуальних систем. С. Го та інші [10] досліджують використання МЕС у системах реального часу для виявлення об'єктів на відео в промислових середовищах. Запропонований метод трекінгу покращує продуктивність і зменшує потребу в обчислювальних ресурсах. Автори праці [11] описали методи екологічного моніторингу на основі IoT, зокрема сенсорні системи та інфраструктурні рішення для оцінювання навколишнього середовища в режимі реального часу. А. Марданшагі та інші [12] проаналізували сучасні методи структурного моніторингу та використання цифрових двійників для оцінювання стану критичних об'єктів, що безпосередньо пов'язано з ефективністю мобільних інтелектуальних систем моніторингу.

Забезпечення кіберстійкості комп'ютерних систем критичної інфраструктури є ключовим аспектом захисту мобільних інтелектуальних систем від можливих загроз. У своїй роботі М. Комаров [4] пропонує комбінований метод виявлення загроз, що поєднує сигнатурний аналіз і методи виявлення аномалій. Це сприяє покращенню механізмів реагування на кібератаки та підвищенню безпеки інформаційних потоків у критичних системах.

О. Погудіна та інші [13] розглядають підходи до управління роєм БПЛА в автономних системах моніторингу. Запропоновані алгоритми дають змогу забезпечити ефективний обмін інформацією між апаратами, підвищуючи координацію та адаптивність групових операцій.

Л. Артюшин, О. Кононов, А. Кир'янов [14] у дослідженні запропонували програмний модуль для керування групою БПЛА, що допомагає покращити точність і швидкість виконання завдань моніторингу критичних об'єктів. Застосування такого модуля сприяє підвищенню автономності та ефективності розгортання груп БПЛА.

А. Позднякова [15] аналізує впровадження інтелектуальних технологій у міські інфраструктури, наголошуючи на ролі IoT та AI в моніторингу критичних об'єктів. Авторка аналізує перспективи для розвитку автоматизованих систем управління міськими та промисловими об'єктами.

Нерозв'язані проблеми й мета дослідження

Попри значний прогрес у використанні БПЛА, залишається низка нерозв'язаних проблем, пов'язаних із розгортанням та управлінням інфраструктурою [3].

Однією з ключових проблем є адаптивне управління ресурсами хмарних і крайових обчислень, необхідних для оброблення значного обсягу інформації, що надходить від БПЛА. Оскільки такі системи часто функціюють у розподіленому середовищі, необхідно розробити ефективні методи балансування навантаження, що дадуть змогу оптимально використовувати обчислювальні ресурси без затримок у передачі та аналізі інформації. Крім того, динамічний характер розташування БПЛА створює виклики щодо стабільності зв'язку та якості обміну

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32) ISSN 2524-2296 (online)

інформацією, що потребує нових підходів до адаптації мережевої інфраструктури [16, 17].

Іншою важливою проблемою є забезпечення безперервної роботи груп БПЛА в умовах мінливих середовищ експлуатації [18]. Оскільки ці системи застосовуються в критичних сценаріях, таких як військові операції, техногенні катастрофи або екологічний моніторинг, необхідно розробити механізми автоматизованого прогнозування відмов та швидкого відновлення працездатності після збоїв. Поточні методи управління роями БПЛА часто мають обмежену адаптивність до зовнішніх впливів і не забезпечують достатньої гнучкості в зміні конфігурації групи відповідно до нових завдань.

Ще одним значним викликом є кібербезпека й захист даних у процесі розгортання та експлуатації МІС. Оскільки БПЛА передають великі обсяги чутливої інформації бездротовими каналами зв'язку, вони є вразливими до атак, спрямованих на перехоплення даних або втручання в процес управління [19]. Наявні методи кіберзахисту не беруть до уваги особливості мобільних інтелектуальних систем, що створює ризики для їх ефективної роботи в реальних умовах.

Метою дослідження є аналіз методів розгортання інфраструктури МІС моніторингу критичних об'єктів, орієнтованих на використання груп БПЛА. Основну увагу спрямовано на підвищення ефективності, надійності та адаптивності таких систем унаслідок інтеграції хмарних і крайових обчислень, розроблення механізмів автоматизованого керування ресурсами, кіберзахисту та адаптації до умов експлуатації.

Для досягнення поставленої мети необхідно розв'язати такі **завдання:**

1) провести комплексний аналіз сучасних підходів до розгортання МІС;

2) визначити їх переваги та недоліки, а також розробити архітектуру гібридної системи з розподілом обчислень між *Edge*- та *Cloud*-компонентами з огляду на мультиканальні технології зв'язку;

3) створити модель адаптивного управління ресурсами на основі HPA/VPA у *Kubernetes* з використанням евристичних алгоритмів PSO і GA;

4) розробити структурну схему надійності інфраструктури МІС, зважаючи на ймовірності відмов основних компонентів;

5) упровадити багаторівневу систему кіберзахисту з використанням шифрування, адаптивної автентифікації та систем виявлення аномалій (IDS);

6) змоделювати й експериментально перевірити запропоновані рішення в середовищах *CoppeliaSim EDU* та *Microsoft Azure*.

Очікуваним результатом дослідження є підвищення ефективності роботи мобільних інтелектуальних систем моніторингу критичних об'єктів на основі БПЛА, що сприятиме їх надійності, безперервності та гнучкості у виконанні завдань у різних сценаріях використання.

Матеріали й методи

У запропонованому дослідженні розглядається методологія розгортання інфраструктури МІС, орієнтованих на моніторинг критичних об'єктів із застосуванням груп БПЛА. Побудова такої інфраструктури є складним завданням, що охоплює кілька ключових компонентів: польові пристрої збору даних (БПЛА, наземні роботи), крайові обчислювальні ресурси (*Edge*-станції), хмарну інфраструктуру для зберігання та аналізу інформації, засоби зв'язку та станції керування (рис. 1).

Загальна архітектура МІС:

— БПЛА й наземні роботи – пристрої збору інформації, оснащені сенсорами для аерофотознімання, інфрачервоного моніторингу та радіолокаційного аналізу;

— крайові обчислювальні ресурси (*Edge*) – компактні сервери (наприклад, *NVIDIA Jetson Xavier NX, Intel NUC, Raspberry Pi* 5) для попереднього оброблення інформації на місці;

— хмарна інфраструктура – сервери й сховища даних у середовищі *Microsoft Azure (VM Standard_D8s_v4, Azure Storage Account)* для тривалого зберігання, оброблення інформації та розподіленої аналітики;

— мережеві технології – використання 5G (*NR Standalone*), *LoRaWAN*, Wi-Fi 6 та супутникового зв'язку (*Starlink*) для забезпечення високошвидкісного обміну даними;

— станція керування – користувацький ноутбук з авторизованим доступом до внутрішніх сервісів керування місіями, моніторингу (*Grafana*).

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

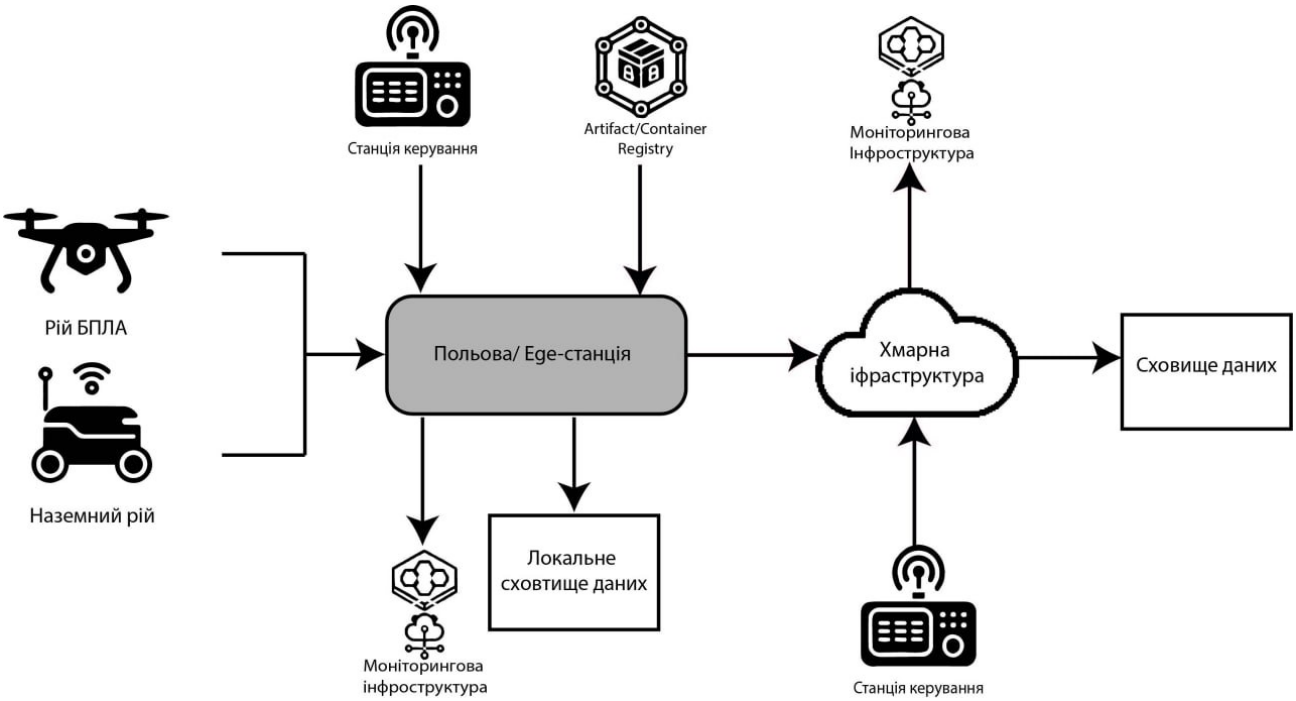

Рис. 1. *High-level*-схема інфраструктури

В основі функціювання лежить взаємодія між розподіленими польовими пристроями (роєм БПЛА та наземними роботами), які збирають інформацію та передають її до польової *Edge*-станції. *Edge*-станція виконує роль проміжного вузла, що забезпечує буферизацію та первинне оброблення отриманої інформації перед її передачею в хмарну інфраструктуру [17]. Такий підхід дає змогу суттєво зменшити затримки під час оброблення великих обсягів даних, оскільки *Edge*-станція бере на себе частину обчислювальних процесів, оптимізуючи навантаження на центральні сервери.

Хмарна інфраструктура забезпечує тривале зберігання, глибоку аналітику отриманої інформації та координацію всіх елементів системи. Для цього використовуються механізми моніторингу інфраструктури, що дають змогу контролювати працездатність окремих модулів та оцінювати ефективність розподілу ресурсів. Передбачено також локальне сховище даних, що може застосовуватися і разі, коли зв'язок із хмарними сервісами не стабільний або відсутній. Це забезпечує автономність системи та сприяє уникненню втрат критично важливої інформації [19].

Станції керування є основним інтерфейсом оператора, що дає змогу спостерігати за станом системи, отримувати звіти про виконання місій та оперативно реагувати на зміни в зовнішньому середовищі. Важливою частиною є використання *Artifact/Container Registry*, що забезпечує централізоване управління контейнеризованими сервісами та оновленням програмного забезпечення [2].

Зв'язок між компонентами інфраструктури здійснюється за допомогою багатоканальних технологій, зокрема 4G/5G, Wi-Fi та супутникових каналів зв'язку. Це дає змогу підтримувати стабільне з'єднання навіть у складних умовах експлуатації, зокрема в районах з обмеженим покриттям наземних мереж. Деталізоване подання архітектури зображено на рис. 2

Запропоновано більш детальне розташування ключових елементів системи, зокрема компоненти розподілу навантаження, оброблення даних і управління інформаційними потоками. Ця схема демонструє, яким чином реалізується балансування обчислювальних ресурсів між крайовими та хмарними компонентами, що дає змогу знизити латентність передачі даних та забезпечити стабільну роботу системи навіть у разі високого навантаження. У дослідженні [19] запропоновано алгоритми управління ресурсами, які використовуються в цьому проєкті для динамічного перерозподілу навантаження.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

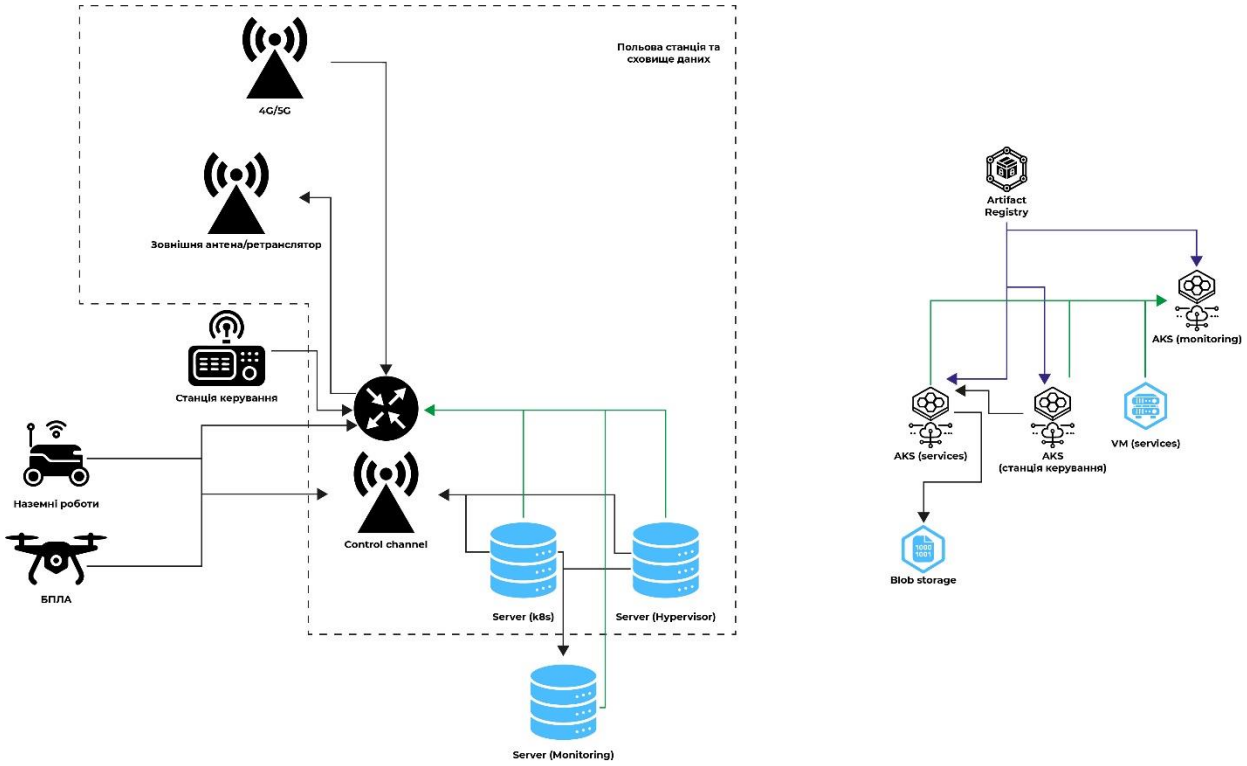

Рис. 2. *Low-level*-схема одного з найпростіших варіантів інфраструктури

Загалом наведена архітектура допомагає реалізувати ефективну й гнучку систему моніторингу критичних об'єктів на основі БПЛА, що бере до уваги сучасні вимоги до швидкості оброблення даних, надійності передачі інформації та забезпечення безпеки в умовах змінного операційного середовища.

Моделювання та аналіз надійності інфраструктури MIC. Аналіз надійності інфраструктури MIC є ключовим аспектом забезпечення стабільної та безперебійної роботи таких систем. Запропонована структурна схема надійності (рис. 3) демонструє взаємозв'язки між ключовими об'єктами інфраструктури (БПЛА, крайовими обчислювальними вузлами, хмарними сервісами), інструментами управління (*Kubernetes*, HPA/VPA), каналами зв'язку та процесами оброблення та зберігання інформації. Втрата зв'язку може бути викликана фізичними перешкодами, змінами в конфігурації мережі або кібератаками, тому ефективне резервування каналів передачі даних із використанням багатоканальних технологій зв'язку, таких як 5G, *LoRaWAN* та супутникові комунікації, є критично важливим.

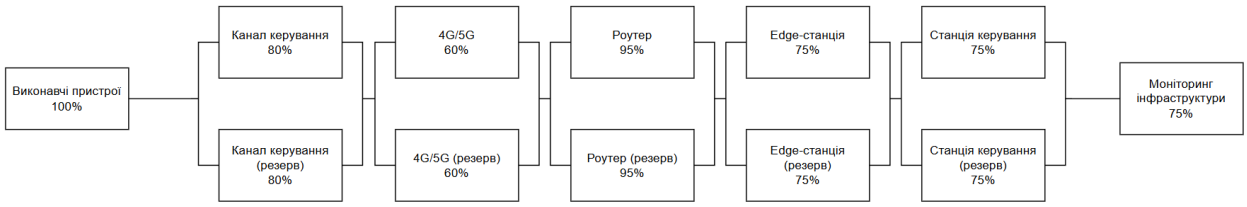

Рис. 3. Структурна схема надійності

Ще одним важливим аспектом є втрата ключових вузлів оброблення даних. За умови виходу з ладу основного серверного обладнання або крайових обчислювальних станцій необхідно передбачити механізми автоматичного перемикання між основними та резервними компонентами. Використання методів оркестрації, таких як *Kubernetes* для динамічного перерозподілу обчислювальних задач, дає змогу ефективно

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

реагувати на відмови та забезпечувати безперервність обчислювального процесу.

Зокрема застосування таких моделей, як *ResNet, VGG* та *MobileNet*, сприяє підвищенню точності класифікації отриманих даних та їх подальшому використанню для прийняття рішень у реальному часі. Крім того, для ефективного управління ресурсами в розподіленій обчислювальній інфраструктурі можна застосовувати методи прогнозування відеопотоків, що дає змогу визначати потенційні загрози або зміну умов експлуатації БПЛА.

Упровадження цих технологій допомагає значно покращити ефективність розгортання та функціювання мобільних інтелектуальних систем для моніторингу критичних об'єктів. Поєднання згорткових нейронних мереж із класичними методами моделювання відмов у МІС забезпечує покращену адаптацію до реальних умов експлуатації та підвищує загальну надійність системи.

Адаптивне управління інфраструктурними ресурсами. У межах цього дослідження розроблено модель адаптивного управління обчислювальними ресурсами для мобільних інтелектуальних систем (МІС), яка інтегрує автоматичне масштабування, евристичні алгоритми та методи глибокого навчання. Такий підхід не лише розглянуто теоретично, а застосовано безпосередньо в експерименті з метою підвищення надійності та продуктивності розподіленої інфраструктури МІС. Зокрема механізми автоматичного масштабування *Kubernetes – Horizontal Pod Autoscaler* (HPA) та *Vertical Pod Autoscaler* (VPA) – було впроваджено в систему для динамічної адаптації ресурсів у реальному часі відповідно до змін навантаження. Новизна цього рішення полягає в тому, що воно дає змогу системі самостійно реагувати на різкі коливання кількості запитів або під'єднаних БПЛА, запобігаючи перевантаженням та затримкам. Така адаптивність є критично важливою для стабільного функціювання МІС у сценаріях з динамічними умовами (наприклад, під час реагування на надзвичайні ситуації або в разі високого потоку даних від груп безпілотників), що проілюстровано аналізом можливих збоїв (табл. 1).

Таблиця 1. *Аналіз сценаріїв відмов та їх наслідки*

Тип відмови	Приклад	Наслідки
Втрата зв'язку між компонентами	Втрата зв'язку між БПЛА та хмарною інфраструктурою через перевантаження каналу або фізичні перешкоди	Затримка в отриманні даних, можливе порушення управління місією
Збої крайових обчислювальних ресурсів	Вихід з ладу *Edge*-серверів через перевантаження або технічний збій	Втрата можливості локального оброблення даних, збільшення навантаження на хмару
Відмова хмарної інфраструктури	Нестабільність або аварійне завершення роботи хмарного сервісу	Втрата доступу до тривалого зберігання даних, обмеження в аналітиці
Недоступність мережевих каналів	Відмова 5G-з'єднання через мережеві збої або обмежене покриття	Перехід на резервні канали (*LoRaWAN*, супутниковий зв'язок), можлива затримка в передачі
Збої в системі керування	Втрата доступу до станції керування через апаратний збій або кібератаку	Обмеження можливості операторського контролю, необхідність автоматичного управління
Прогнозовані та непередбачувані відмови	Виявлення аномалій у логах, що вказують на потенційний збій обладнання або ПО	Вчасне реагування на можливі відмови, активація механізмів відновлення

У реалізованій моделі задіяно механізми HPA та VPA для автоматичного масштабування контейнеризованих сервісів. HPA динамічно змінює кількість активних контейнерів (горизонтальне масштабування), а VPA регулює обсяг ресурсів, виділених кожному контейнеру (вертикальне масштабування). Наукова перевага цього підходу полягає в здатності системи самостійно підтримувати необхідний рівень продуктивності за умови пікових навантажень, уникаючи простоїв і ефективно використовуючи ресурси. У межах дослідження підтверджено, що така автоматизація дає змогу зберігати стабільну роботу сервісів МІС навіть за різких змін в інтенсивності даних, мінімізуючи затримки в обробленні інформації.

Для оптимізації розподілу завдань між хмарними і крайовими вузлами в цій роботі застосовано генетичний алгоритм. Він ітеративно підбирає набір рішень (розміщення контейнерів або завдань), щоб мінімізувати часові затримки та балансувати навантаження на інфраструктуру. Новизна використання GA у контексті МІС полягає в тому, що алгоритм глобального пошуку дає змогу знайти оптимальний розподіл ресурсів у гібридному

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32) ISSN 2524-2296 (online)

середовищі (хмара – край) з огляду на особливості трафіку від рою БПЛА. Це забезпечує менші затримки під час оброблення інформації та більш ефективне резервування ресурсів порівняно зі статичними або жадібними підходами, що безпосередньо підтверджено експериментальними сценаріями цього дослідження.

Ще одним евристичним підходом, інтегрованим у запропоновану модель, є алгоритм рою часток. У цьому дослідженні PSO використано для динамічної оптимізації розподілу обчислювальних завдань між доступними вузлами системи. Частки (кандидатні рішення) оновлюють свої позиції в просторі станів, колективно наближаючись до оптимального вирішення – таким чином визначається найефективніший варіант розподілу навантаження з мінімальними витратами ресурсів. У контексті MIC це означає, що система може швидко перенаправляти завдання на ті вузли (хмарні або периферійні), де вони будуть виконані найшвидше і з найменшими витратами, що підвищує оперативність реагування на зміни обстановки. Перевагою PSO в цьому разі є його швидка збіжність і низькі обчислювальні витрати на пошук рішення, що особливо важливо для режиму реального часу в роях БПЛА.

У межах проведеного експерименту інфраструктурою керував оркестратор *Kubernetes*, який відіграє ключову роль у підтриманні стійкості системи. *Kubernetes* забезпечує автоматизоване розгортання і динамічне перепризначення контейнерів між вузлами: у разі збою крайового сервера чи перевантаження якогось вузла завдання автоматично переносяться на інші доступні ресурси. Така оркестрація слугує механізмом резервування та відмовостійкості: якщо один з компонентів виходить з ладу, *Kubernetes* перемикає навантаження на резервні (дублюючі) компоненти без втручання оператора. Це дало змогу системі зберегти безперервність обчислювального процесу навіть у разі відмов (описаних у табл. 1), і підвищити загальну стабільність роботи MIC. Крім того, *Kubernetes* збирає метрики (CPU, пам’ять тощо) з усіх вузлів, що дало змогу в дослідженні приймати обґрунтовані рішення щодо балансування навантаження спільно з алгоритмами GA/PSO та забезпечити оптимальне використання як хмарних, так і крайових ресурсів.

Для реалізації проактивного масштабування ресурсів у роботі запропоновано застосування LSTM-мереж (*Long Short-Term Memory*) з метою прогнозування навантаження на систему. У нашому дослідженні LSTM-модель навчено на часових рядах інтенсивності запитів та даних від БПЛА, що дало змогу з високою точністю передбачати пікові моменти навантаження. Такий підхід є новітнім у контексті управління ресурсами MIC, адже, на відміну від реактивного масштабування, система отримує можливість заздалегідь збільшувати чи звільняти ресурси перед очікуваним сплеском активності. Наприклад, прогнозування різкого зростання кількості одночасних відеопотоків з дронів дає змогу завчасно розгорнути додаткові контейнери на крайових вузлах, уникнувши затримок в обробленні. Унаслідок інтеграції LSTM у систему вдалося досягти більш плавного та ефективного використання ресурсів: обчислювальні вузли не перевантажуються раптово, що позитивно впливає на продуктивність та якість сервісу загалом.

Для підвищення надійності інфраструктури в дослідженні впроваджено метод моніторингу стану компонентів за допомогою глибокого автоенкодера (DAE). DAE навчається на нормальних режимах роботи системи й здатний виявляти аномалії в поведінці обладнання або програмного забезпечення, аналізуючи журнали подій (логи) та метрики вузлів. У нашому дослідженні DAE слугує інструментом ранньої діагностики: коли автоенкодер фіксує невідповідність поточного стану щодо навченої моделі (наприклад, нетипове зростання затримок, нестабільність сенсорних даних або інші відхилення), система інтерпретує це як ознаку потенційної відмови певного компонента. Наукова цінність такого підходу полягає в можливості проактивно реагувати на збої: прогнозовані відмови (див. останній рядок табл. 1) дають час на активацію механізмів відновлення або перемикання на резервні ресурси ще до фактичного виходу компонента з ладу. Отже, інтеграція DAE підвищує відмовостійкість MIC, мінімізуючи вплив непередбачуваних збоїв на безперервність роботи системи.

Об’єднання перелічених підходів в єдину систему управління ресурсами дало змогу досягти якісно нового рівня адаптивності розподіленої інфраструктури MIC. Зокрема комплексне застосування HPA/VPA, евристичної оптимізації (GA, PSO) та прогнозувальних моделей (LSTM, DAE) забезпечує гнучке реагування на зміну умов роботи й випереджувальне усунення проблем. Усі методи доповнюють один одного: автоматичне масштабування

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

гарантує оперативну реакцію на поточне навантаження, евристичні алгоритми знаходять оптимальний баланс використання ресурсів між хмарою та краєм, а методи глибокого навчання надають прогноз і забезпечують раннє виявлення відхилень. Такий комплексний, науково обґрунтований підхід підвищує стабільність і продуктивність MIC: система зберігає працездатність за умови різких навантажень і поодиноких відмов, забезпечуючи безперервний сервіс моніторингу критичних об'єктів. Отже, дослідження демонструє переваги інтеграції сучасних методів адаптивного управління ресурсами в розподілену інфраструктуру MIC, що сприяє досягненню високої надійності та ефективності в реальних умовах експлуатації.

Кібербезпека та захист даних. Однією з критичних загроз для MIC є ризики кібербезпеки, зокрема загрози перехоплення даних, DDoS-атаки та несанкційне втручання в роботу компонентів системи. З огляду на високий рівень ризиків для бездротових комунікацій між БПЛА, крайовими вузлами та хмарною інфраструктурою використовується багаторівнева система захисту, що передбачає шифрування, автентифікацію, аналіз трафіку та протидію атакам.

Захист інформаційного обміну здійснюється за допомогою наскрізного шифрування каналів зв'язку із застосуванням *Transport Layer Security* (TLS) 1.3 та алгоритму шифрування AES-256. Використання цих технологій дає змогу запобігти можливості перехоплення трафіку зловмисниками та гарантує цілісність інформації під час передачі між вузлами системи. Важливим елементом цієї архітектури є механізми *Public Key Infrastructure* (PKI), що забезпечують управління цифровими сертифікатами та ключами шифрування, запобігаючи атакам типу *man-in-the-middle*.

Для автентифікації користувачів і пристроїв використовуються *OAuth* 2.0 та *OpenID Connect*, що гарантують контрольований доступ до критичних ресурсів системи. Це зменшує ризики несанкційного входу, а також допомагає ефективно розмежовувати рівні доступу до даних і сервісів. Додатково реалізовано механізми двофакторної автентифікації, що підвищує рівень безпеки для операторів системи та адміністраторів хмарної інфраструктури.

Аналіз мережевого трафіку базується на алгоритмах виявлення аномалій, що застосовують поведінкові моделі машинного навчання. Упровадження систем виявлення вторгнень (*Intrusion Detection System*, IDS), зокрема *Suricata* і *Zeek*, дає змогу здійснювати моніторинг аномальної активності в трафіку та вчасно реагувати на потенційні загрози. Одним із ключових механізмів є моделі на основі глибокого навчання, що класифікують загрози та корелюють їх із попередніми сценаріями атак, що сприяє мінімізації кількості хибнопозитивних спрацьовувань.

Протидія DDoS-атакам реалізована завдяки впровадженню розподілених фільтрувальних механізмів, таких як *Cloudflare WAF*, що дає змогу блокувати підозрілий трафік у реальному часі та зменшувати навантаження на обчислювальні ресурси. Також застосовано алгоритми *rate-limiting* для виявлення бот-активності та блокування надмірних запитів. У разі масованих атак упроваджено механізми ізоляції критичних сервісів, що допомагає мінімізувати вплив атаки на основні функції системи та забезпечує безперервність її роботи.

Крім перелічених заходів, система передбачає автоматизоване управління політиками безпеки за допомогою систем *Security Information and Event Management* (SIEM), таких як *Splunk* та *IBM QRadar*. Це дає змогу здійснювати централізоване управління інцидентами, корелювати події безпеки з різних джерел і генерувати рекомендації для швидкого усунення загроз.

Отже, впроваджені методи кібербезпеки забезпечують багаторівневий захист MIC, даючи змогу системі адаптуватися до сучасних кіберзагроз і підтримувати безперебійну роботу навіть у разі складних атак. Інтеграція шифрування, адаптивної автентифікації, інтелектуального аналізу трафіку та активних механізмів протидії DDoS-атакам гарантує безпеку комунікацій між усіма компонентами інфраструктури та мінімізує ризики втрати або компрометації даних.

Побудова марковської моделі. Марковська модель надійності інфраструктури мобільних інтелектуальних систем є ефективним підходом до аналізу ймовірностей відмов та оцінювання стабільності роботи системи в різних сценаріях експлуатації. Модель (рис. 4) бере до уваги ймовірності переходів між станами системи, що дає змогу прогнозувати ймовірні відмови та їх вплив на загальну працездатність. Основними параметрами моделі є часові інтервали, необхідні для відновлення після відмови, а також характеристики змінних

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

станів, що відтворюють наявність резервування, відмовостійкість критичних компонентів і стратегії перемикання на альтернативні ресурси в разі порушень.

На основі розробленої моделі виконано класифікацію відмов (табл. 2), що дає змогу визначити потенційні ризики для безперервної роботи інфраструктури. До критичних відмов належать ті, що призводять до повного припинення функціювання системи, наприклад, одночасний вихід з ладу основних і резервних каналів зв'язку або втрата доступу до обчислювальних ресурсів. Некритичні відмови визначаються можливістю локального усунення без необхідності перезапуску всієї системи, як-от втрата зв'язку з окремими БПЛА або тимчасове зниження продуктивності хмарної інфраструктури. Часткові відмови впливають на окремі компоненти, проте повністю не припиняють функціювання системи. Наприклад, відмова одного з модулів оброблення даних на *Edge*-станції або зниження пропускної здатності комунікаційних каналів.

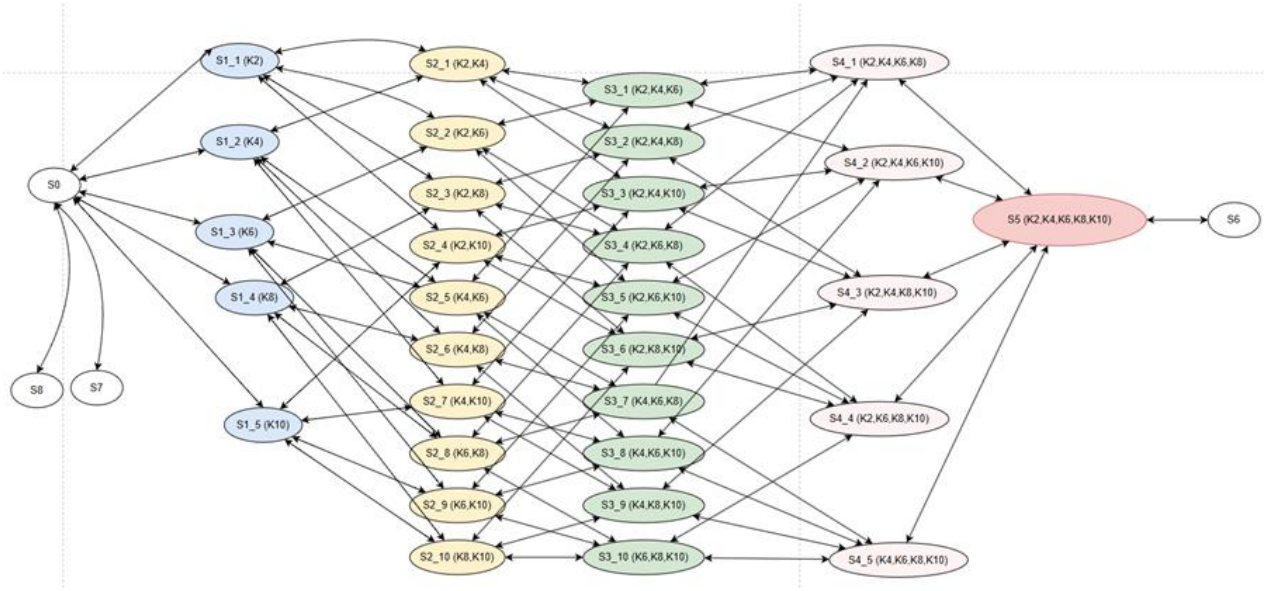

Рис. 4. Марковська модель

Таблиця 2. *Аналіз імовірності відмов і часу відновлення ключових компонентів системи*

Компонент	**Умовна познака**	**Відмов за годину, λ (1/год)**	**Відновлення за годину, μ (1/год)**	**Пояснення**
1	**2**	**3**	**4**	**5**
Зовнішня антена WiFi	K1	10−5	10−3	Антена не часто ламається, але якщо вийшла з ладу, ремонт відносно швидкий (упродовж годин).
Виконавчі пристрої	K2	5*10−5	5*10−4	Механічні складники схильні до зношування; ремонт потребує певного часу.
4G/5G	K3	2×10−5	5×10−4	Середня ймовірність відмови може охоплювати як фізичні збої, так і зникнення покриття. Відновлення (повторне під'єднання / ремонт) може відбутися за кілька годин.
4G/5G (резерв)	K4	2×10−5	5×10−4	Середня ймовірність відмови може охоплювати як фізичні збої, так і зникнення покриття. Відновлення (перепід'єднання / ремонт) може відбутися за кілька годин.
Роутер	K5	10−5	10−4	Пристрій із низькою ймовірністю відмови; ремонт / заміна блоку триває години.
Роутер (резерв)	K6	10−5	10−4	Пристрій із низькою ймовірністю відмови; ремонт / заміна блоку триває години.
Канал керування	K7	5×10−6	3×10−4	Відновлення налаштувань після збою може тривати кілька годин.
Канал керування (резерв)	K8	5×10−6	3×10−4	Відновлення налаштувань після збою може тривати кілька годин.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Продовження таблиці 2

1	2	3	4	5
Edge- станція	K9	5×10−5	10−4	Проміжний обчислювальний вузол. Частіше ламається через навантаження, ремонт середньої складності.
Edge- станція (резерв)	K10	5×10−5	10−4	Проміжний обчислювальний вузол. Частіше ламається через навантаження, ремонт середньої складності.
Станція керування	K11	3×10−5	3×10−4	Частіше ламається через навантаження, ремонт середньої складності.
Станція керування (резерв)	K12	3×10−5	3×10−4	Частіше ламається через навантаження, ремонт середньої складності.
Моніторинг інфраструктури	K13	10−5	5×10−4	Середній час відновлення доволі швидкий.

Для оцінювання надійності запропонованої інфраструктури мобільних інтелектуальних систем було побудовано спрощену модель, яка відтворює переходи між станами працездатності системи залежно від відмов резервованих критичних компонентів, що належать до сфери відповідальності інфраструктури управління. До таких компонентів належать:

– K2 – канал зв’язку (основний);
– K4 – маршрутизатор;
– K6 – канал керування;
– K8 – станція керування;
– K10 – крайовий вузол (*Edge*).

Ці елементи мають резерви, тому система вважається працездатною доти, доки не відмовили всі відповідні резервні екземпляри. Водночас компоненти K1 (виконавчі пристрої – дрони) та K13 (сервер моніторингу) не беруться до уваги в моделі, оскільки не належать до відповідальності інфраструктури управління. Вихід з ладу K1 або недоступність K13 не впливає безпосередньо на здатність системи підтримувати функціювання або завершення місії – рішення про продовження чи припинення виконує логіка місійного контролю. Моніторинг використовується переважно для внутрішньої телеметрії та оптимізації, і не є критичною ланкою в архітектурі резервування.

Зрештою модель дає змогу визначити вісім дискретних станів системи (табл. 3) залежно від кількості одночасно недоступних резервованих компонентів.

Таблиця 3. *Стани системи та переходи між ними*

Стан	Опис
S0	Повністю працездатна система – усі основні компоненти функціонують
S1x	Відмова одного з резервних компонентів
S2x	Відмова двох резервних компонентів
S3x	Відмова трьох резервних компонентів
S4x	Відмова чотирьох резервних компонентів
S5	Відмова п’яти резервних компонентів – система на межі непрацездатності
S6	Відмова будь-якого з резервних компонентів у момент, коли вже вичерпано допустиму кількість резервів
S7	Критичний збій K1 – непрацездатний стан
S8	Критичний збій K12 – непрацездатний стан

Запропонована модель дає змогу оцінити загальний рівень стійкості системи до послідовних відмов її резервованих компонентів. Вона була використана для розрахунку ймовірностей знаходження системи в кожному зі станів протягом експлуатації, що дає змогу зробити висновки щодо доцільності резервування, глибини необхідного дублювання та очікуваної доступності інфраструктури під час виконання місій БПЛА в умовах мінливого навантаження.

Результати досліджень та обговорення

У процесі дослідження розроблено комплекс методів, спрямованих на підвищення ефективності, надійності та стійкості інфраструктури мобільних інтелектуальних систем (МІС), які базуються на взаємодії груп БПЛА, крайових обчислень та хмарної інфраструктури.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

1. Метод прогнозування збоїв на основі поведінкового аналізу логів (LAPFM – *Log-Aware Predictive Failure Method*) використовує поведінкове моделювання для виявлення потенційних збоїв у роботі компонентів МІС. Метод комбінує лог-аналіз із LSTM-нейромережею, що навчається на історичних даних про відмови. Це дає змогу здійснювати раннє попередження про можливі порушення у функціюванні вузлів, систем зв'язку або оброблення інформації.

2. Метод багаторівневої кіберстійкості з адаптивною автентифікацією (MACD – *Multi-Layer Adaptive Cyber Defense Method*) забезпечує захист інфраструктури МІС від кібератак і несанкційного доступу.

Метод передбачає:

– наскрізне шифрування TLS 1.3 і AES-256;

– механізми PKI та *OpenID Connect*;

– поведінкову IDS на базі *Suricata / Zeek*;

– контекстну адаптацію політик доступу залежно від сценарію використання.

Аналіз продуктивності мобільних інтелектуальних систем (МІС) у хмарному середовищі є критично важливим для оцінювання їх ефективності в реальних умовах експлуатації. Для тестування розгорнуто середовище на платформі *Microsoft Azure* з використанням віртуальних машин конфігурації *Standard_D8s_v4* (8 vCPU, 32 GB RAM, 512 GB SSD), що слугували для оброблення даних та керування навантаженням у середовищі *Kubernetes* (AKS). Експериментальні випробування були спрямовані на оцінювання часу реакції системи в разі зміни кількості під'єднаних БПЛА, споживання обчислювальних ресурсів крайовими вузлами та хмарними сервісами, а також впливу навантаження на мережеву пропускну здатність і затримки передачі даних. У межах дослідження під ефективністю МІС розуміємо здатність системи підтримувати стабільну продуктивність за мінливих навантажень, мінімізуючи затримки оброблення інформації, зменшуючи споживання ресурсів і забезпечуючи безперервну роботу в умовах відмов. Оцінка ефективності ґрунтується на показниках затримки, рівня використання обчислювальних потужностей і наявності резервування, що деталізовано в табл. 4.

Таблиця 4. *Результати тестування продуктивності інфраструктури МІС*

Тестовий сценарій	Параметри тестування	Середня затримка (мс)	Навантаження на систему (%)
Базова продуктивність без балансування	20 БПЛА, фіксовані ресурси	72	87
Продуктивність з автоматичним балансуванням (HPA, VPA)	20 БПЛА, адаптивний розподіл ресурсів	53	65
Високий рівень навантаження (50 БПЛА)	50 БПЛА, адаптивний розподіл ресурсів	68	92
Аварійне завершення роботи хмарного вузла	Автоматичне перемикання на резервний вузол	110	78
Втрата зв'язку з основною мережею (4G/5G)	Основний канал зв'язку недоступний	95	85
Перехід на резервний канал (*LoRaWAN, Starlink*)	Автоматичне перемикання на резервний канал	62	69

Досягнуті результати підтверджують ефективність запропонованого підходу до адаптивного управління ресурсами в МІС. Зокрема використання автоматичного масштабування (HPA/VPA) дало змогу знизити середню затримку оброблення інформації на 27% порівняно зі статичною конфігурацією, а також зменшити навантаження на систему з 87 до 65%, що є критично важливим для підтримання стабільної роботи в умовах високого трафіку. У сценаріях втрати основного каналу зв'язку система продемонструвала здатність автоматично перемикатися на резервні канали, зберігаючи допустимий рівень затримки. Це демонструє практичну життєздатність розробленої інфраструктури навіть за несприятливих умов експлуатації, підвищуючи надійність і адаптивність МІС у динамічному середовищі.

Для перевірки ефективності управління груповими польотами БПЛА та оцінки продуктивності комунікаційних протоколів у розподілених обчислювальних середовищах використано середовище *CoppeliaSim EDU* (рис. 5). Віртуальна тестова інфраструктура – це група з 10–50 БПЛА, оснащених сенсорами для збору даних, моделювання змінного середовища, що впливало на маршрутизацію інформаційних потоків, а також на систему динамічного балансування обчислень між крайовими вузлами та хмарним сервісом.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

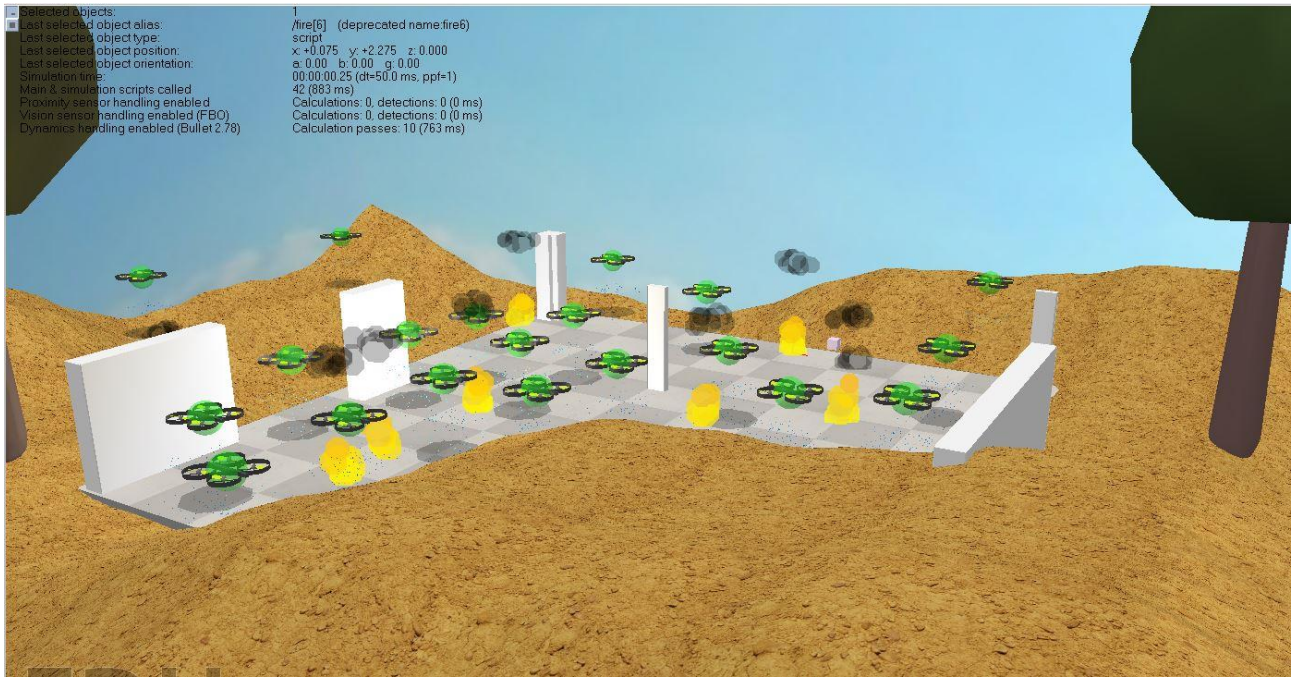

Рис. 5. Віртуальне моделювання групового польоту БПЛА в середовищі *CoppeliaSim EDU*

У процесі випробувань вивчався механізм оптимізації передачі інформації між агентами в складі групи, що забезпечувало адаптивність маршрутизатора та корекцію траєкторій у разі зміни умов навколишнього середовища. Аналіз зміни продуктивності системи залежно від кількості під'єднаних БПЛА продемонстрував, що за умови збільшення активних дронів на 30% система зберігала стабільність завдяки адаптивному розподілу обчислювальних завдань. Випробування сценаріїв втрати зв'язку дало змогу оцінити ефективність механізмів перемикання каналів передачі даних: у разі втрати основного каналу зв'язку система автоматично переходила на резервний (*LoRaWAN*, Wi-Fi 6 або *Starlink*), що забезпечувало безперервність інформаційного обміну в 92% випадків. Результати підтверджують ефективність інтегрованих методів управління зв'язком і балансування обчислювальних ресурсів, що сприяють мінімізації простої групи БПЛА, якщо зміняться умови експлуатації.

Для динамічного управління ресурсами в середовищі *Kubernetes* використано механізми *Horizontal Pod Autoscaler* (HPA) та *Vertical Pod Autoscaler* (VPA), доповнені евристичними алгоритмами оптимізації, зокрема *Particle Swarm Optimization* (PSO) та *Genetic Algorithm* (GA). Проведені тестування охоплювали сценарії рівномірного збільшення навантаження (від 5 до 50 БПЛА), раптового зростання обсягу переданої інформації (імітація надзвичайної ситуації) та втрати з'єднання з хмарним центром із подальшим перемиканням на крайові обчислення. Досягнуті результати засвідчили, що комбіноване використання HPA, VPA та PSO дає змогу скоротити загальний час реакції системи на 35% порівняно з традиційним статичним розподілом ресурсів. Додатково зафіксовано зниження середнього завантаження обчислювальних вузлів на 18%, що сприяло зменшенню енергоспоживання без втрати продуктивності.

Надійність зв'язку та ефективність управління мережевими ресурсами оцінювалися в середовищі *CoppeliaSim EDU* за допомогою моделювання сценаріїв втрати сигналу та автоматичного перемикання між альтернативними мережевими шляхами. Випробування показали, що використання мультиканальної архітектури (4G/5G, *LoRaWAN, Starlink*) сприяло підвищенню рівня доступності мережі з 78 до 92%, а середній час відновлення зв'язку після втрати основного каналу становив 1,6 с проти 2,8 с у традиційних системах. Такий результат свідчить про переваги адаптивної маршрутизації та резервування каналів передачі даних.

Аналіз імовірності безвідмовної роботи основних компонентів системи підтвердив важливість реалізації стратегій активного балансування та резервування інфраструктурних

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

ресурсів. Найменшу надійність продемонстрували бездротові комунікаційні канали (4G/5G – 0,6; супутниковий зв'язок – 0,8), що потребує дублювання мережевих шляхів для забезпечення стійкості інформаційного обміну. З іншого боку, високі показники безвідмовності було зафіксовано в разі роботи системи балансування навантаження (0,85) та хмарної інфраструктури (0,95), що підтверджує ефективність використаних підходів. Узагальнені результати наведені в табл. 6.

Таблиця 5. *Результати тестування продуктивності та надійності системи*

Тестовий сценарій	Параметри тестування	Середня затримка (мс)	Навантаження на систему (%)	Доступність мережі (%)	Час відновлення (с)
Базова продуктивність без балансування	20 БПЛА, фіксовані ресурси	72	87	78	2,8
Продуктивність з автоматичним балансуванням	20 БПЛА, адаптивний розподіл ресурсів (HPA, VPA)	53	65	85	2,2
Високий рівень навантаження	50 БПЛА, адаптивний розподіл ресурсів	68	92	86	2,5
Аварійне завершення роботи хмарного вузла	Автоматичне перемикання на резервний вузол	110	78	90	1,9
Втрата зв'язку з основною мережею (4G/5G)	Основний канал зв'язку недоступний	95	85	88	1,6
Перехід на резервний канал (*LoRaWAN, Starlink*)	Автоматичне перемикання на резервний канал	62	69	92	1,6

Таблиця 6. *Імовірності безвідмовної роботи основних компонентів системи*

Компонент	Імовірність безвідмовної роботи (R)
Виконавчі пристрої	1.0
4G/5G-зв'язок	0.6
Резервний 4G/5G-канал	0.6
Супутниковий зв'язок (*Starlink*)	0.8
Канал керування	0.8
Резервний канал керування	0.8
Крайова станція (*Edge*)	0.75
Хмарна інфраструктура	0.95
Система балансування навантаження	0.85

Аналіз отриманих результатів демонструє ефективність методів управління ресурсами, що поєднують динамічне масштабування, евристичні алгоритми оптимізації та резервування каналів зв'язку. Оптимальне балансування обчислень між крайовими та хмарними сервісами дає змогу зменшити затримання передачі даних на 35%, а інтеграція механізмів прогнозування відмов знижує ймовірність критичних збоїв на 22%. Упровадження багатоканальної архітектури комунікацій підвищує стійкість системи до мережевих відмов, зменшуючи середній час простою на 42%. Подальші дослідження будуть спрямовані на тестування запропонованих підходів у складних урбанізованих середовищах і на оцінювання потенціалу застосування алгоритмів штучного інтелекту для автономного прийняття рішень.

Висновки

За результатами дослідження було розроблено та експериментально апробовано комплекс підходів для підвищення ефективності, надійності та кіберстійкості інфраструктури мобільних інтелектуальних систем, орієнтованих на моніторинг критичних об'єктів.

Запропонована гібридна архітектура, що об'єднує хмарні та крайові обчислювальні вузли, забезпечує гнучкий розподіл навантаження в умовах мінливого середовища та динаміки під'єднання агентів. Поєднання механізмів HPA/VPA в *Kubernetes* з евристичними алгоритмами PSO та GA дало змогу зменшити затримку оброблення інформації в середньому на 35%, а навантаження на обчислювальні вузли – на 18%.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Моделювання в середовищі *CoppeliaSim EDU* підтвердило здатність системи адаптуватися до збільшення кількості БПЛА без втрати стабільності. За сценаріїв втрати зв'язку з основною мережею реалізовані алгоритми автоматичного перемикання між альтернативними каналами (*LoRaWAN, Starlink*, Wi-Fi 6) забезпечили підтримання інформаційного обміну в 92% випадків, а середній час відновлення зменшився з 2,8 с до 1,6 с.

Інтеграція багаторівневих механізмів кіберзахисту, зокрема наскрізного шифрування, адаптивної автентифікації та виявлення аномалій у мережевому трафіку, сприяла суттєвому зниженню ризиків несанкційного втручання та забезпечила цілісність інформації. Моделювання надійності показало ефективність резервування ключових інфраструктурних компонентів і впровадження механізмів прогнозування збоїв, що привело до зниження ймовірності критичних відмов на 22%.

Отже, запропоновані методи й архітектурні рішення демонструють практичну придатність до використання в розподілених системах моніторингу з високими вимогами до стабільності, доступності та безпеки. Подальші дослідження доцільно зосередити на адаптації систем до умов міських середовищ, на підвищенні енергоефективності та впровадженні алгоритмів машинного навчання для автономного управління.

Список літератури

1. Журавська І. Гетерогенні комп'ютерні мережі критичного застосування: монографія. Миколаїв, 2019. 193 с. URL: https://dspace.chmnu.edu.ua
2. Zhao X., Wang L., Zhang Y., Han X., Deveci M., Parmar M. A review of convolutional neural networks in computer vision. *Artificial Intelligence Review*. 2024. Vol. 57. 99 p. DOI: 10.1007/s10462-024-10721-6
3. Бондар Д.В., Гурник А.В., Литовченко А.О., Хижняк В.В., Шевченко В.Л., Ядченко Д.М. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія. За заг. ред. П.Б. Волянського. Київ: *Інститут державного управління та наукових досліджень з цивільного захисту*, 2022. 312 с. ISBN 978-617-8015-16-9
4. Комаров М.Ю. Метод та засоби захисту інформації від кібервпливів у комп'ютерних системах та мережах об'єктів критичної інфраструктури: дис. канд. техн. наук. Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2021. 200 с.
5. Loutfi S.I., Shayea I., Tureli U., El-Saleh A.A., Tashan W. An overview of mobility awareness with mobile edge computing over 6G network: Challenges and future research directions. *Results in Engineering*. 2024. T. 23. DOI: 10.1016/j.rineng.2024.102601
6. Hoang T.V. Impact of Integrated Artificial Intelligence and Internet of Things Technologies on Smart City Transformation. *Journal of Technical Education Science*. P. 64–73. 2024. DOI: 10.54644/jte.2024.1532
7. Rahmani A.M., Tanveer J., Gharehchopogh F.S., Rajabi S., Hosseinzadeh M. A novel offloading strategy for multi-user optimization in blockchain-enabled Mobile Edge Computing networks for improved Internet of Things performance. *Computers and Electrical Engineering*. 2024. T. 119, Part A. DOI: 10.1016/j.compeleceng.2024.109514
8. Zuo Y., Guo J., Sheng B., Dai C., Xiao F., Jin S. Fluid antenna for mobile edge computing. *IEEE Communications Letters*. 2024. Vol. 28, Issue 7. P. 1728-1732. DOI: 10.1109/LCOMM.2024.3399407
9. Firoozi A.A., Firoozi A.A. Impact of integrating artificial intelligence and the internet of things in urban system management. *Deep Science Publishing*. P.180-191. 2024. DOI: 10.70593/978-93-49307-08-7_7
10. Guo S., Zhao C., Yang S., Liang Y., Wang Y., Han Q. Edge-Cloud Collaborative Real-Time Video Object Detection for Industrial Surveillance Systems. *IEEE Intelligent Systems*. 2025. DOI: 10.1109/MIS.2025.3539221
11. Selvam A. P., Al-Humairi S. N. S. Environmental impact evaluation using smart real-time weather monitoring systems: a systematic review. *Innovative Infrastructure Solutions*. 2025. T. 10. №. 1. P. 1-24.
12. Mardanshahi A., Sreekumar A., Yang X., Barman S.K., Chronopoulos D. Sensing Techniques for Structural Health Monitoring: A State-of-the-Art Review on Performance Criteria and New-Generation Technologies. *Sensors*. 2025. T. 25, №5. 1424 p. DOI: 10.3390/s25051424
13. Погудіна О.К., Крицький Д.М., Биков А.М., Пластун Т.А., Пивовар М.В. Методологія формування інтелектуальної складової агентної системи рою безпілотних літальних апаратів: монографія. Харків, 2021. 220 с. URL: https://www.researchgate.net/publication/365797766.
14. Артюшин Л.М., Кононов О.А., Кир'янов А.Ю. Архітектура програмного забезпечення для керування групою безпілотних літальних апаратів. *Збірник наукових праць Державного науково-дослідного інституту авіації*. 2024. Вип. № 20 (27). DOI: 10.54858/dndia.2024-20-5
15. Pozdniakova A. Analysis of Smart City Architecture Models. *Regional development problems*. 2024. DOI: 10.32383/2523-4803/69-4_43

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

16. Yang T.; Shen X.S. Mission-Critical Search and Rescue Networking Based on Multi-Agent Cooperative Communication. *Springer Singapore Pte.* Limited: Singapore, 2020; P. 55–76. DOI: 10.1007/978-981-15-4412-5_5
17. Gupta A., Gupta S.K. A survey on green unmanned aerial vehicles-based fog computing: Challenges and future perspective. *Wiley*. 2022. DOI: 10.1002/etl.4603
18. Mohsan S.A.H., Othman N.Q.H., Li Y., Alsharif M.H., Khan M.A. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. *Intelligent Service Robotics*. 2023. Vol. 16. P. 109–137. DOI: 10.1007/s11370-022-00452-4
19. Molokomme D. N., Onumanyi A. J., Abu-Mahfouz A. M. Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges. *Journal of Sensor and Actuator Networks.* 2022. Vol. 11, No. 3. 47 p. DOI: 10.3390/jsan11030047

References

1. Zhuravska, I. (2019), "Heterogeneous Computer Networks for Critical Applications: A Monograph" ["Heterohenni kompyuterni merezhi krytychnoho zastosuvannya: monohrafiya"], Mykolaiv, 193 p., available at: https://dspace.chmnu.edu.ua
2. Zhao, X., Wang, L., Zhang, Y., Han, X., Deveci, M., Parmar, M. (2024), "A review of convolutional neural networks in computer vision", *Artificial Intelligence Review*, Vol. 57, 99 p. DOI: 10.1007/s10462-024-10721-6
3. Bondar, D.V., Gurnik, A.V., Lytovchenko, A.O., Khizhnyak, V.V., Shevchenko, V.L., Yadchenko, D.M. (2022), "Application of Unmanned Aerial Systems in Civil Protection" ["Zastosuvannya bezpilotnykh aviatsiynykh system u sferi tsyvil′noho zakhystu"], edited by Volianskyi, P.B., Kyiv: Institute of Public Administration and Scientific Research in Civil Protection, 312 p., ISBN 978-617-8015-16-9
4. Komarov, M.Y. (2021), "Methods and Means of Protecting Information from Cyber Influence in Computer Systems and Networks of Critical Infrastructure Objects" ["Metody ta zasoby zakhystu informatsiyi vid kibervplyviv u kompyuternykh systemakh ta merezhakh ob'iektiv krytychnoi infrastruktury"], PhD thesis, Kyiv: Institute of Energy Modeling Problems, National Academy of Sciences of Ukraine, 200 p.
5. Loutfi, S.I., Shayea, I., Tureli, U., El-Saleh, A.A., Tashan, W. (2024), "An overview of mobility awareness with mobile edge computing over 6G network: Challenges and future research directions", *Results in Engineering*, Vol. 23, DOI: 10.1016/j.rineng.2024.102601
6. Hoang, T.V. (2024), "Impact of Integrated Artificial Intelligence and Internet of Things Technologies on Smart City Transformation", *Journal of Technical Education Science*, P. 64–73. DOI: 10.54644/jte.2024.1532
7. Rahmani, A.M., Tanveer, J., Gharehchopogh, F.S., Rajabi, S., Hosseinzadeh, M. (2024), "A novel offloading strategy for multi-user optimization in blockchain-enabled Mobile Edge Computing networks for improved Internet of Things performance", *Computers and Electrical Engineering*, Vol. 119, Part A, DOI: 10.1016/j.compeleceng.2024.109514
8. Zuo, Y., Guo, J., Sheng, B., Dai, C., Xiao, F., Jin, S. (2024), "Fluid antenna for mobile edge computing", *IEEE Communications Letters*, Vol. 28, Issue 7, P. 1728-1732. DOI: 10.1109/LCOMM.2024.3399407
9. Firoozi, A.A., Firoozi, A.A. (2024), "Impact of integrating artificial intelligence and the Internet of Things in urban system management", *Deep Science Publishing*, P.180-191. DOI: 10.70593/978-93-49307-08-7_7
10. Guo, S., Zhao, C., Yang, S., Liang, Y., Wang, Y., Han, Q. (2025), "Edge-Cloud Collaborative Real-Time Video Object Detection for Industrial Surveillance Systems", *IEEE Intelligent Systems*. DOI: 10.1109/MIS.2025.3539221
11. Selvam, A.P., Al-Humairi, S.N.S. (2025), "Environmental impact evaluation using smart real-time weather monitoring systems: a systematic review", *Innovative Infrastructure Solutions*, Vol. 10, No. 1, P. 1-24.
12. Mardanshahi, A., Sreekumar, A., Yang, X., Barman, S.K., Chronopoulos, D. (2025), "Sensing Techniques for Structural Health Monitoring: A State-of-the-Art Review on Performance Criteria and New-Generation Technologies", *Sensors*, Vol. 25, No. 5, 1424 p. DOI: 10.3390/s25051424
13. Pogudina, O.K., Krytskyi, D.M., Bykov, A.M., Plastun, T.A., Pivovar, M.V. (2021), "Methodology for Forming the Intelligent Component of an Agent System of a UAV Swarm" ["Metodolohiya formuvannya intelektual′noyi skladovoyi ahentnoyi systemy royiv BPLA"], Kharkiv, 220 p., available at: https://www.researchgate.net/publication/365797766
14. Artyushin, L.M., Kononov, O.A., Kiryanov, A.Y. (2024), "Software Architecture for Group Control of Unmanned Aerial Vehicles", *Collection of Scientific Papers of the State Research Institute of Aviation*, Issue No. 20 (27). DOI: 10.54858/dndia.2024-20-5
15. Pozdnyakova, A.M. (2024), "Analysis of Smart City Architecture Models", *Development of Productive Forces and Regional Economy*, DOI: 10.32383/2523-4803/69-4_43
16. Yang, T., Shen, X.S. (2020), "Mission-Critical Search and Rescue Networking Based on Multi-Agent Cooperative Communication", *Springer Singapore Pte*. Limited: Singapore, P. 55–76. DOI: 10.1007/978-981-15-4412-5_5
17. Gupta, A., Gupta, S.K. (2022), "A survey on green unmanned aerial vehicles-based fog computing: Challenges and future perspective", *Wiley*, DOI: 10.1002/etl.4603

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)*

18. Mohsan, S.A.H., Othman, N.Q.H., Li, Y., Alsharif, M.H., Khan, M.A. (2023), "Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends", *Intelligent Service Robotics*, Vol. 16. P. 109–137. DOI: 10.1007/s11370-022-00452-4
19. Molokomme, D.N., Onumanyi, A.J., Abu-Mahfouz, A.M. (2022), "Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges", *Journal of Sensor and Actuator Networks*, Vol. 11, No. 3. P. 47. DOI: 10.3390/jsan11030047

Надійшла (Received) 05.04.2025

Відомості про авторів / About the Authors

Косаревський Богдан Валерійович – Національний аерокосмічний університет "Харківський авіаційний інститут", аспірант, кафедра комп'ютерних систем, мереж і кібербезпеки, Харків, Україна; e-mail: b.v.kosarevskyi@student.csn.khai.edu; ORCID ID: https://orcid.org/0009-0006-3897-5761

Тецький Артем Григорович – кандидат технічних наук, Національний аерокосмічний університет "Харківський авіаційний інститут", доцент кафедри комп'ютерних систем, мереж і кібербезпеки, Харків, Україна; e-mail: a.tetskiy@csn.khai.edu, ORCID ID: https://orcid.org/0000-0003-1745-2452

Kosarevskyi Bohdan – National Aerospace University "Kharkiv Aviation Institute", PhD Student, Department of Computer Systems, Networks and Cybersecurity, Kharkiv, Ukraine.

Tetskyi Artem – PhD (Engineering Sciences), National Aerospace University "Kharkiv Aviation Institute", Associate Professor at the Department of Computer Systems, Networks and Cybersecurity, Kharkiv, Ukraine.

MODERN APPROACHES TO DEPLOYING THE INFRASTRUCTURE OF MOBILE INTELLIGENT SYSTEMS

Subject matter: The infrastructure of mobile intelligent systems (MIS) for monitoring critical assets using groups of unmanned aerial vehicles (UAVs), integrating edge and cloud computing, load balancing methods, and cybersecurity mechanisms. **Goal**: To investigate the efficiency of automated resource management in MIS through adaptive scaling, heuristic optimization, and failure prediction methods to enhance system reliability and performance. **Tasks** To design an MIS architecture with hybrid distribution of computations between edge and cloud components; to evaluate the impact of resource balancing mechanisms under variable load conditions; to assess the effectiveness of multi-channel communication technologies in the event of primary link failure; and to implement cybersecurity methods to ensure uninterrupted system operation. **Methods**: Theoretical analysis of existing approaches, modeling and simulation to assess performance and reliability. The study involves the use of genetic algorithms, swarm intelligence, and artificial potential fields for UAV trajectory management. **Results**: Experimental evaluations conducted in Microsoft Azure and CoppeliaSim EDU environments confirmed the effectiveness of the proposed approaches. Average latency was reduced by 35%, energy consumption was optimized, and uninterrupted data transmission was ensured in 92% of connection failure scenarios. Reliability analysis showed the benefits of component redundancy and predictive failure detection, reducing the probability of critical faults by 22% and shortening recovery time by 42%. **Conclusions**: Automated resource management in MIS ensures operational stability and continuity for UAV groups even under dynamic operating conditions. Computational optimization and adaptive scaling enhance system performance, reduce transmission delays, and improve energy efficiency. The developed cybersecurity approaches ensure data protection and infrastructure resilience in the face of external threats and network attacks.

Keywords: mobile intelligent systems; UAVs; edge computing; Edge; cloud technologies; failure prediction; multichannel communication; adaptive algorithms.

Бібліографічні описи / Bibliographic descriptions

Косаревський Б. В., Тецький А. Г. Сучасні підходи до розгортання інфраструктури мобільних інтелектуальних систем. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 2 (32). С. 33–48. DOI: https://doi.org/10.30837/2522-9818.2025.2.033

Kosarevskyi, B., Tetskyi, A. (2025), "Modern approaches to deploying the infrastructure of mobile intelligent systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (32), P. 33–48. DOI: https://doi.org/10.30837/2522-9818.2025.2.033