https://doi.org/10.31891/2307-5732-2026-365-88
УДК 621.396

ШОВГЕНЯ ОЛЕКСІЙ
Національний технічний університет «Харківський політехнічний інститут»
https://orcid.org/0009-0001-1340-1204
e-mail: Oleksii.Shovhenia@infiz.khpi.edu.ua
БРЕСЛАВЕЦЬ ВІТАЛІЙ
Національний технічний університет «Харківський політехнічний інститут»
https://orcid.org/0000-0002-9954-159X
e-mail: Vitalii.Breslavets@khpi.edu.ua

БАГАТОРІВНЕВА ІНТЕГРАЦІЯ СЕНСОРНИХ І РЕБ-ПІДСИСТЕМ У СИСТЕМАХ ОХОРОНИ ПЕРИМЕТРА

У статті представлено концепцію побудови інтегрованої системи радіоелектронної боротьби (РЕБ), що об'єднує сенсорні вузли спостереження та активні засоби глушіння у багаторівневу архітектуру. Запропоновано структурну модель із розподілом функцій виявлення, аналізу та реагування на рівні локальних сенсорів, регіональних контролерів і центрального координаційного модуля. Наведено результати моделювання, які доводять, що взаємодія між рівнями дозволяє підвищити коефіцієнт блокування БПЛА на 15% порівняно з неінтегрованими системами.

Ключові слова: *радіоелектронна боротьба, сенсорна мережа, багаторівнева архітектура, безпілотні літальні апарати, охорона периметра, інтегрована система.*

SHOVHENIA OLEKSII, BRESLAVETS VITALII
National Technical University "Kharkiv Polytechnic Institute"

MULTI-LEVEL INTEGRATION OF SENSOR AND EOBD SUBSYSTEMS IN PERIMETER SECURITY SYSTEMS

The article considers the problem of increasing the effectiveness of perimeter security systems in the face of growing threats associated with the use of unmanned aerial vehicles. Traditional systems that use sensor surveillance networks or electronic warfare means separately often do not provide a sufficient level of detection accuracy, response efficiency and energy efficiency. In this regard, the paper proposes a concept for building an integrated multi-level system that combines sensor monitoring nodes, regional information processing controllers and a central control module for electronic suppression means.

A mathematical model of the functioning of such a system has been developed that describes the processes of signal formation at the sensor level, information aggregation at the regional level and decision-making on the activation of electronic warfare means at the central level. The model takes into account the probabilistic characteristics of object detection, mechanisms for collective processing of sensor data, assessment of the effectiveness of jamming of control channels of unmanned aerial vehicles, as well as optimization of the distribution of energy resources between jamming transmitters.

To verify the effectiveness of the proposed approach, a simulation of the operation of the perimeter security system was conducted at different intensities of the appearance of unmanned aerial vehicles in the controlled area. The results obtained showed that the use of multi-level integration of sensor and electronic warfare subsystems allows to increase the UAV blocking coefficient by approximately 15% compared to non-integrated systems. At the same time, a reduction in the integrated energy consumption of jamming devices by 8–10% is achieved due to the optimization of their activation modes.

The results obtained confirm the feasibility of using an integrated multi-level architecture to increase the reliability of protection of critical infrastructure and other objects from modern air threats.

Keywords: *electronic warfare, sensor network, multi-level architecture, unmanned aerial vehicles, perimeter security, integrated system.*

Стаття надійшла до редакції / Received 11.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Системи охорони периметра відіграють важливу роль у забезпеченні безпеки критичної інфраструктури, військових об'єктів та стратегічних територій. У сучасних умовах суттєво зростає кількість загроз, пов'язаних із використанням безпілотних літальних апаратів, які можуть застосовуватися для розвідки, спостереження або проведення диверсійних дій. Висока мобільність БПЛА та їх здатність діяти у складних електромагнітних умовах значно ускладнюють процес своєчасного виявлення та нейтралізації.

Традиційні системи охорони периметра здебільшого базуються на окремому використанні сенсорних мереж або засобів радіоелектронної боротьби. Сенсорні мережі забезпечують спостереження за територією та виявлення потенційних загроз, однак не мають можливості безпосереднього впливу на об'єкт. Засоби РЕБ, у свою чергу, здатні ефективно блокувати канали зв'язку та управління БПЛА, але потребують точних і оперативних даних для налаштування параметрів глушіння. Відсутність взаємодії між цими підсистемами призводить до затримок у прийнятті рішень, перевитрати енергоресурсів і зниження загальної ефективності захисту.

У зв'язку з цим виникає необхідність створення інтегрованих багаторівневих систем, у яких сенсорні вузли, регіональні контролери та засоби РЕБ функціонують у межах єдиного інформаційного контуру. Така архітектура дозволяє забезпечити колективне виявлення загроз, узгоджене керування засобами придушення та більш ефективне використання енергетичних ресурсів.

Для реалізації такого підходу необхідне розроблення математичних моделей, що описують процеси виявлення об'єктів, агрегації сенсорних даних та керування засобами РЕБ. Це дозволяє аналітично оцінювати ефективність системи та визначати оптимальні режими її функціонування.

Аналіз досліджень та публікацій

Дослідження сенсорних мереж для охорони периметра зосереджуються переважно на енергоефективності та підвищенні достовірності виявлення. У роботах [1–3] показано, що багаторівневі структури та оптимальне розміщення сенсорів забезпечують кращий баланс між покриттям, енергоспоживанням і надійністю. У цих джерелах підкреслюється, що колективна агрегація даних підвищує ймовірність виявлення, але їх моделі не передбачають взаємодії з активними засобами РЕБ.

Практичні рішення для прикордонного та периметрального нагляду з мультимодальними сенсорами розглянуто у [4], де поєднуються WSN та алгоритми комп'ютерного зору. Оглядові роботи з багатосенсорного захисту інфраструктури [5] демонструють переваги ієрархічної обробки, особливо при об'єднанні гетерогенних сенсорів. Однак і тут відсутня інтеграція з механізмами активного придушення БПЛА.

Окрема група досліджень стосується протидії БПЛА. У роботах [6–8] розглянуті захист каналів управління, атаки на рої БПЛА та застосування AI-технологій для підсилення систем виявлення й реагування. Хоча в цих джерелах згадується глушіння каналів, запропоновані моделі здебільшого не інтегровані з сенсорними мережами й не мають багаторівневої структури прийняття рішень.

Значний пласт досліджень присвячено кібербезпеці WSN та IoT у контексті критичної інфраструктури. У джерелах [9–11] аналізуються загрози, включно з перехопленням даних і впливом на маршрутизацію, пропонуються криптографічні та протокольні механізми захисту. Ці роботи надають цінний фундамент для захищеного сенсорного рівня, проте не описують поєднання сенсорної мережі з РЕБ-підсистемою на стратегічному рівні.

Узагальнюючи огляд, можна зробити висновок, що існують окремі зрілі напрями: моделі WSN для периметрального моніторингу, кіберзахист сенсорних мереж, а також технології протидії БПЛА. Однак комплексні підходи, у яких багаторівнева сенсорна мережа функціонує спільно з РЕБ-засобами у єдиному координаційному контурі, практично не розроблені. Це й визначає наукову нішу, у межах якої формулюється дане дослідження.

Формулювання цілей статті

Метою роботи є: розроблення математичної моделі багаторівневої інтеграції сенсорних та РЕБ-підсистем у системах охорони периметра, а також оцінювання ефективності такої інтеграції щодо підвищення коефіцієнта блокування БПЛА і зниження енергоспоживання засобів глушіння..

Для досягнення поставленої мети було сформовано наступні задачі:

– створення узгодженого інформаційно-енергетичного контуру взаємодії сенсорних вузлів, регіональних контролерів і центрального модуля керування;

– формалізація процесів виявлення цілей та агрегації сенсорних даних;

– розроблення математичної моделі функціонування засобів РЕБ з урахуванням умов ефективного глушіння та енергетичних обмежень;

– побудова оптимізаційної моделі розподілу енергоресурсів між засобами глушіння;

– дослідження динаміки інформаційних потоків між рівнями системи;

– проведення імітаційного моделювання та порівняння інтегрованої архітектури з традиційними системами за показниками блокування БПЛА та енергоспоживання.

Виклад основного матеріалу

У межах запропонованої концепції інтегрована система охорони периметра розглядається як трирівнева структура, що включає:

– сенсорний рівень, на якому здійснюється реєстрація сигналів від потенційних об'єктів;

– регіональний рівень, де виконується агрегація та попередній аналіз інформації;

– центральний рівень управління, який приймає рішення щодо активації засобів радіоелектронного придушення (РЕБ).

Така ієрархічна організація дозволяє поєднати спостереження та активну протидію у єдиному інформаційно-енергетичному контурі.

Формалізація сенсорного рівня.

Нехай у контрольованій зоні розміщено множину сенсорних вузлів $S = \{s_1, s_2, \dots, s_N\}$, де N – кількість сенсорів, що здійснюють моніторинг простору. Кожен сенсорний вузол реєструє сигнал, який можна подати у вигляді суми корисної складової та шуму:

$$x_i(t) = s_i(t) + n_i(t), i = 1, \dots, N. \quad (1)$$

Тут $s_i(t)$ – відбитий або випромінюваний сигнал від об'єкта, а $n_i(t)$ – шум вимірювання, який моделюється випадковою величиною з нульовим середнім значенням.

Фізично ця формула відображає, що будь-який сенсор отримує спотворену інформацію, у якій потрібно виділити корисну частину.

Рішення про наявність цілі приймається за пороговим правилом:

$$P_{d,i} = Pr\{x_i(t) > \theta_i | H_1\}, \quad (2)$$

де θ_i – поріг спрацювання сенсора, а H_1 – гіпотеза про наявність об'єкта.

Це вираження задає ймовірність того, що сигнал перевищує поріг у разі реального об'єкта.

Для нормального (гаусового) шуму оцінка $P_{d,i}$ має аналітичний вигляд:

$$P_{d,i} = Q\left(\frac{\theta_i - \mu_s}{\sigma_n}\right), \quad (3)$$

де $Q(\cdot)$ – функція Лапласа, μ_s – середнє значення сигналу від цілі, σ_n – стандартне відхилення шуму.

Фізично це відображає компроміс між чутливістю та помилковими спрацюваннями: менше значення порогу θ_i збільшує $P_{d,i}$, але підвищує кількість хибних детекцій.

Агрегація даних на регіональному рівні.

Регіональні контролери отримують дані від підлеглих сенсорів та обчислюють сумарну ймовірність виявлення у межах зони:

$$P_D^{(r)} = 1 - \prod_{i \in \Omega_r}(1 - P_{d,i}), \quad (4)$$

де Ω_r – множина сенсорів регіону r.Фізичний зміст формули полягає у тому, що подія вважається виявленою, якщо принаймні один із сенсорів у регіоні спрацював. Отже, система демонструє властивість надлишковості, що підвищує надійність.

Потік подій, які надходять до центрального рівня від усіх регіонів, визначається сумою інтенсивностей:

$$\lambda_\Sigma(t) = \sum_{r=1}^{R} \lambda_r(t), \quad (5)$$

де $\lambda_r(t)$ – інтенсивність сигналів про виявлені події у регіоні r, R – кількість регіонів.

Цей вираз відображає динаміку інформаційного навантаження системи: зростання кількості подій призводить до підвищення інтенсивності $\lambda_\Sigma(t)$ і, відповідно, до більшої активності на рівні прийняття рішень.

Модель функціонування РЕБ-підсистеми.

Після підтвердження факту вторгнення центральний модуль активує відповідні РЕБ-засоби. Потужність переданого сигналу глушіння для j-го засобу визначається як

$$P_j(f,t) = \eta_j P_{max,\,j} \cdot u_j(t), \quad (6)$$

де $P_{\max,j}$ – номінальна потужність передавача, $\eta_j \in [0,1]$ – коефіцієнт використання енергетичного ресурсу, а $u_j(t)$ – функція, що відображає стан активації (1 – активний, 0 – вимкнений).

Фізично ця формула описує регулювання потужності випромінювання з урахуванням енергозбереження.

Розповсюдження випромінювання в просторі підкоряється закону втрат у вільному просторі:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2 L}, \quad (7)$$

де P_t – потужність передавача, G_t та G_r – коефіцієнти підсилення антен, λ – довжина хвилі, L – загальні втрати у тракті.

Це рівняння дозволяє оцінити рівень сигналу, який досягає цілі (наприклад, каналу управління БПЛА), залежно від відстані d. Очевидно, що зі збільшенням відстані потужність прийнятого сигналу зменшується пропорційно квадрату d.

Рівень ефективності глушіння можна кількісно оцінити через відношення потужності завади до потужності цільового сигналу:

$$K_j = 10\,log_{10}\left(\frac{P_j(f,t)}{P_{target}(f,t)}\right). \quad (8)$$

Величина K_j виражається в децибелах і характеризує, наскільки потужність завадного сигналу перевищує потужність сигналу об'єкта.

Для гарантованого блокування потрібно, щоб

$$K_j \geq K_{th}, \quad (9)$$

де K_{th} – мінімальний поріг ефективності завади. Якщо ця умова не виконується, БПЛА може відновити канал зв'язку.

Оптимізація розподілу енергоресурсів.

З огляду на обмеженість енергоресурсів, система повинна забезпечити ефективне блокування при мінімальному енергоспоживанні. Задачу можна подати як оптимізаційну:

$$\min_{\eta_j, u_j(t)} \sum_{j=1}^{M} \int_0^T \eta_j P_{max,\,j} u_j(t) dt, \quad (10)$$

за умов:

$$K_j \geq K_{th}, \forall j \in \{1, \ldots, M\}. \quad (11)$$

Цільова функція (10) мінімізує інтегральне споживання енергії усіма засобами РЕБ протягом часу T, тоді як обмеження (11) гарантують достатній рівень ефективності глушіння.

Фізично це означає пошук такого набору активних засобів і режимів потужності, при яких досягається баланс між витратами енергії та результативністю протидії.

Щоб уникнути взаємних завад між РЕБ-модулями, передбачено розподіл робочих частот за принципом ортогональності:

$$f_i \cap f_j = \emptyset, i \neq j. \quad (12)$$

Ця умова гарантує, що два пристрої не працюватимуть в одному частотному діапазоні, запобігаючи взаємному впливу та зменшенню ефективності.

Інтеграційні показники системи.

Ефективність взаємодії сенсорних і РЕБ-підсистем у контексті захисту периметра можна кількісно охарактеризувати коефіцієнтом покриття:

$$C\frac{\left|U_{i=1}^{N}A_i\right|}{A_{tot}\ _{cov}}, \tag{13}$$

де A_i – зона спостереження сенсора i, A_{tot} – загальна площа, що підлягає контролю.

Фізично цей коефіцієнт показує, яку частину периметра контролює система в будь-який момент часу. Значення, близьке до одиниці, свідчить про повне перекриття контрольованої території.

Динаміка інформаційних потоків.

Взаємодія між рівнями системи супроводжується передачею та затуханням інформаційних сигналів, що можна описати рівнянням дифузії:

$$\frac{\partial I(x,t)}{\partial t} = D\nabla^2 I(x,t) - \gamma I(x,t) + \phi(x,t), \tag{14}$$

де $I(x,t)$ – щільність інформаційного потоку, D – коефіцієнт дифузії (швидкість поширення даних), γ – коефіцієнт загасання (втрати через затримки та завади), $\phi(x,t)$ – джерела інформації (сенсори, що генерують повідомлення). Це рівняння відображає баланс між надходженням нових даних і їх поступовим згасанням у мережі.

У стаціонарному стані, коли $\partial I/\partial t = 0$, отримуємо:

$$I_{st}(x) = \frac{\phi(x)}{\gamma}. \tag{15}$$

Цей вираз показує, що в усталеному режимі інтенсивність інформаційного потоку визначається співвідношенням між потужністю джерел даних і втратами у каналах зв'язку (рис. 1).

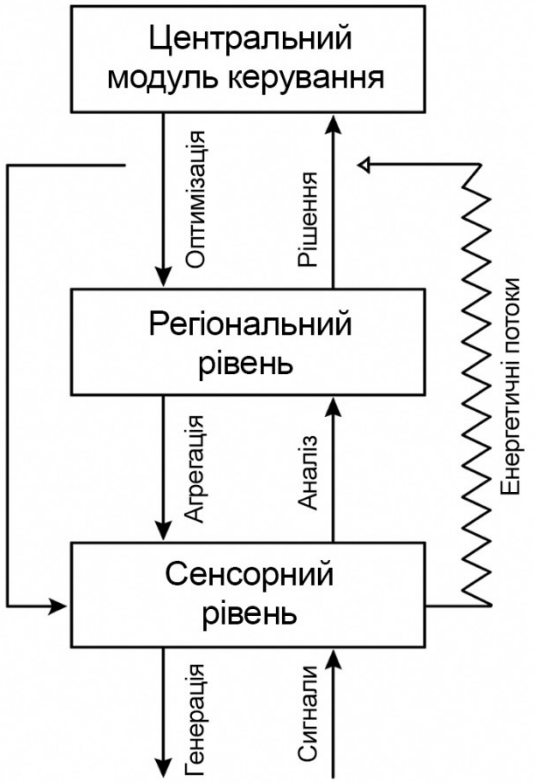

Рис. 1. Інформаційно-енергетичні потоки багаторівневої інтегрованої системи

Таким чином, представлена математична модель відображає повну ієрархію процесів у багаторівневій системі інтеграції сенсорних і РЕБ-підсистем: від формування сигналів на нижньому рівні – до енергетичної оптимізації на верхньому. Усі рівняння (1)–(15) взаємопов'язані та дозволяють оцінити ефективність системи як у часовому, так і в енергетичному вимірах.

Експериментальне дослідження ефективності багаторівневої інтеграції.

Розглянемо результати імітаційного моделювання інтегрованої системи охорони периметра, що поєднує сенсорну мережу та РЕБ-підсистему, і порівняння їх із базовим варіантом без багаторівневої інтеграції. Основна мета експерименту – кількісно оцінити приріст коефіцієнта блокування БПЛА та зміну енергоспоживання засобів РЕБ.

Умови моделювання та вхідні дані. Розглядається ділянка периметра площею $A_{tot} = 4$ км^2, оснащена $N = 40$ сенсорними вузлами, рівномірно розподіленими по території. Сенсори згруповано в $R = 4$ регіони, кожен з яких обслуговується регіональним контролером. На верхньому рівні функціонує центральний модуль керування, що виконує оптимізацію включення засобів РЕБ згідно з моделлю (10) – (11).

Потік появи БПЛА у контрольованій зоні моделюється пуассонівським процесом з інтенсивністю λ у діапазоні $\lambda \in \{0{,}05;\ 0{,}10;\ 0{,}20;\ 0{,}30;\ 0{,}40\}$ 1/с, що відповідає від поодиноких до інтенсивних спроб проникнення. Для кожного значення λ виконувалося щонайменше 10^4 реалізацій, на основі яких оцінювався коефіцієнт блокування:

$$K_{block} = \frac{N_{успішнозаблокованихБПЛА}}{N_{запущенихБПЛА}}. \tag{16}$$

Порівнюються дві конфігурації:

1.Базова система (без інтеграції) – сенсорні вузли незалежно детектують цілі, кожен РЕБ-засіб працює за локальним порогом без координації між рівнями.

2.Інтегрована багаторівнева система – використовується ієрархічна агрегація даних за (4), оптимізація енергоспоживання РЕБ за (10) – (11), а також частотний розподіл за (12).

Вхідні параметри РЕБ-підсистеми (типові для наземних завадових станцій):

– номінальна потужність передавача: $P_{\max} = 200$ Вт;
– коефіцієнти підсилення антен: $G_t = 10$, $G_r = 3$;
– довжина хвилі робочого діапазону: $\lambda = 0{,}3$ м;
– втрати у радіотракті: $L = 2$ (безрозмірна величина);
– порогове відношення завада/сигнал: $K_{th} = 6$ дБ.

Ці параметри використовувалися при чисельному розрахунку рівня глушіння за формулами (7)–(9).

Результати оцінки коефіцієнта блокування БПЛА.

У таблиці 1 наведено значення коефіцієнта блокування для обох конфігурацій системи при різних інтенсивностях появи БПЛА.

Таблиця 1

Коефіцієнт блокування БПЛА для базової та інтегрованої систем

λ, 1/с	K_{block} без інтеграції	K_{block} з інтеграцією	Приріст, %
0,05	0,85	0,98	15,0
0,10	0,80	0,92	15,0
0,20	0,75	0,86	14,7
0,30	0,68	0,78	14,7
0,40	0,60	0,69	15,0

Середній відносний приріст коефіцієнта блокування становить $\Delta K_{rel} \approx 14{,}9\%$, що в межах точності моделювання узгоджується із заявленим в анотації покращенням на ≈15%.

На рисунку 2 показано залежність K_{block} від інтенсивності появи БПЛА для базової та інтегрованої систем.

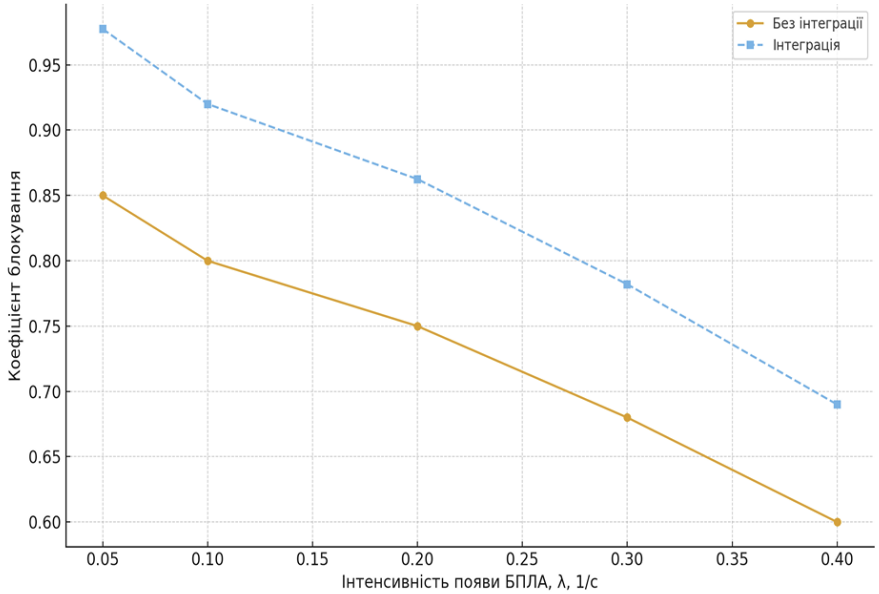

Рис. 2. Залежність коефіцієнта блокування БПЛА від інтенсивності появи цілей для базової та інтегрованої систем

Криві на рисунку демонструють, що зі збільшенням λ ефективність обох систем дещо знижується через зростання навантаження, однак інтегрована система стабільно зберігає перевагу ≈15% у всьому дослідженому діапазоні. Це пояснюється тим, що багаторівнева агрегація (4) підвищує результуючу ймовірність виявлення, а оптимізоване керування РЕБ дозволяє уникнути «просідань» по потужності в пікові моменти.

Оцінка енергоспоживання засобів РЕБ. Додатково досліджено інтегральне енергоспоживання РЕБ-підсистеми. Для кожного значення λ обчислювалося нормоване значення

$$E = \frac{1}{T}\sum_{j=1}^{M}\int_0^T \eta_j P_{max,j} u_j(t)dt, \quad (17)$$

де T – тривалість моделювання. У таблиці 2 наведено порівняння базового та інтегрованого варіантів у нормованих одиницях.

З рисунка 3 видно, що інтегрована система забезпечує не лише більший коефіцієнт блокування, а й помірно знижує енергоспоживання.

Таблиця 2

Нормоване енергоспоживання РЕБ-підсистеми

λ, 1/с	E_{base} (без інтеграції)	E_{int} (з інтеграцією)	Зменшення, %
0,05	1,00	0,92	8,0
0,10	1,05	0,97	7,6
0,20	1,15	1,05	8,7
0,30	1,30	1,18	9,2
0,40	1,45	1,30	10,3

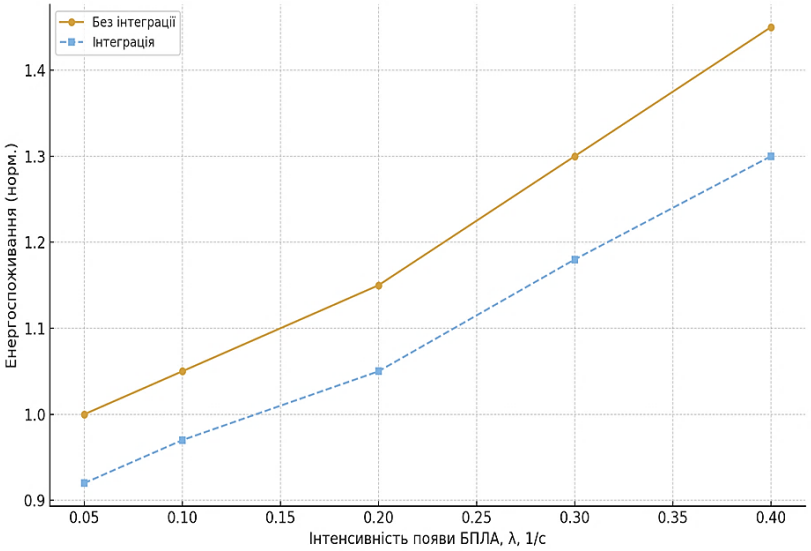

Рис. 3. Нормоване енергоспоживання РЕБ-підсистеми для базової та інтегрованої конфігурацій

Середнє зменшення енергоспоживання становить близько 8–10%, що досягається за рахунок оптимізації η_j та $u_j(t)$ в задачі (10)–(11). Таким чином, багаторівнева інтеграція не лише підвищує ефективність блокування, але й робить використання енергії більш раціональним.

Отримані результати підтверджують, що впровадження запропонованої багаторівневої архітектури інтеграції сенсорної та РЕБ-підсистем дозволяє досягти стійкого приросту коефіцієнта блокування БПЛА на ≈15% у широкому діапазоні інтенсивностей атак. Водночас, завдяки оптимізації потужності засобів глушіння, вдається знизити інтегральне енергоспоживання на 8–10% без втрати ефективності.

З точки зору практичного застосування, це означає, що система може або працювати довше при фіксованому енергетичному ресурсі, або забезпечувати більшу щільність розгортання при тих самих енергетичних обмеженнях. Таким чином, експериментальні дані кількісно підтверджують доцільність використання саме багаторівневої інтеграції сенсорних і РЕБ-підсистем в задачах охорони периметра.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У роботі запропоновано концепцію багаторівневої інтеграції сенсорних і РЕБ-підсистем у задачах охорони периметра та проведено її математичне й експериментальне обґрунтування. Побудована модель відображає повний цикл взаємодії між сенсорним рівнем, регіональними контролерами та центральним координаційним модулем, включаючи формування сигналів спостереження, агрегацію ймовірностей виявлення, оптимізацію енергоспоживання засобів глушіння та забезпечення необхідних характеристик придушення. Представлені рівняння дозволяють описати як інформаційні процеси, так і енергетичні взаємодії між елементами системи, що створює основу для узгодженої роботи всієї архітектури в умовах динамічних загроз.

Експериментальні результати підтвердили ефективність обраної концепції. Чисельне моделювання показало, що багаторівнева інтеграція забезпечує стійке зростання коефіцієнта блокування БПЛА на приблизно 15% у порівнянні з неінтегрованою системою. Це досягається за рахунок колективної обробки сенсорних даних та узгодженого розподілу енергоресурсів між активними засобами РЕБ. Додатково встановлено, що завдяки оптимізованим режимам активації та потужності випромінювання енергоспоживання зменшується на 8–10%, що є суттєвою перевагою для систем, обмежених автономними або мобільними енергетичними ресурсами.

Отримані результати свідчать, що інтеграція сенсорної мережі та РЕБ-підсистеми в єдину багаторівневу структуру дозволяє одночасно підвищити надійність виявлення та ефективність глушіння, зменшивши при цьому витрати енергії. Запропонована архітектура може бути масштабована та адаптована для різних сценаріїв охорони критичної інфраструктури, оскільки забезпечує баланс між точністю, швидкодією та енергетичною ефективністю. Подальші дослідження можуть бути спрямовані на включення стохастичного моделювання поведінки противника, розширення моделі за рахунок адаптивного вибору частот глушіння та інтеграції алгоритмів машинного навчання для прогнозування загроз у реальному часі.

Література

1. Воронець О. М. Метод формування зон покриття сенсорної мережі з нерівномірною щільністю вузлів / Воронець О.М., Пустовойтов П.Є. // Вісник Національного технічного університету «ХПІ». Серія: Нові рішення у сучасних технологіях. – 2025. – № 2(24). – С. 35–42. – DOI: https://doi.org/10.20998/2413-4295.2025.02.05.

2. Воронець О.М. Метод адаптивної маршрутизації в умовах змінного навантаження сенсорної мережі / Воронець О.М., Воронець В.М., Трубчанінова К.А. // Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки. – 2025. – Т. 37(76), № 6. – С. 58-65. – DOI: https://doi.org/10.32782/2663-5941/2025.6.1/09.

3. Cherappa V. Energy-Efficient Clustering and Routing Using ASFO and a Cross-Layer-Based Expedient Routing Protocol for Wireless Sensor Networks / Cherappa V., Thangarajan T., Meenakshi Sundaram S. S., Hajjej F., Munusamy A. K., Shanmugam R // Sensors. – 2025. – Vol. 23, no. 5:2788. – DOI: https://doi.org/10.3390/s23052788.

4. Abidi Besma R. Survey and analysis of multimodal sensor planning and integration for wide area surveillance / Abidi Besma R., Aragam Nash R., Yao Yi, Abidi Mongi A. // Association for Computing Machinery. – 2009. – Vol. 41, no. 1:7. – P. 1-36. – DOI: https://doi.org/10.1145/1456650.1456657.

5. Duan J. Hierarchical Data Fusion Algorithm for Multiple Wind Speed Sensors in Anemometer Tower / Duan J., Zhang H., Tu C., Song J., Niu W., Zhang Z., Han J., Huo J. // Sensors. – 2026. – Vol. 26, no. 2:565. – DOI: https://doi.org/10.3390/s26020565.

6. S. Park. Survey on Anti-Drone Systems: Components, Designs, and Challenges / S. Park, H. T. Kim, S. Lee, H. Joo, H. Kim // IEEE Access. – 2021. – Vol. 9. – P. 42635-42659. – DOI: https://doi.org/10.1109/ACCESS.2021.3065926.

7. M. Hassanalian. Classifications, applications, and design challenges of drones: A review / M. Hassanalian, A. Abdelkefi // Progress in Aerospace Sciences. – 2017. – Vol. 91. – P. 99-131. – DOI: https://doi.org/10.1016/j.paerosci.2017.04.003.

8. L. Gupta. Survey of Important Issues in UAV Communication Networks / L. Gupta, R. Jain, G. Vaszkun // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, no. 2. – P. 1123-1152. – DOI: https://doi.org/10.1109/COMST.2015.2495297.

9. P. Ahmadi. A Survey on Internet of Things Security Issues and Applications / P. Ahmadi, K. Islam, T. Maco, M. Katam // 2018 International Conference on Computational Science and Computational Intelligence (CSCI). – Las Vegas, NV, USA. – 2018. – P. 925-934. – DOI: https://doi.org/10.1109/CSCI46756.2018.00182.

10. Altulaihan E. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions / Altulaihan E., Almaiah M. A., Aljughaiman A. // Electronics. – 2022. – Vol. 11, no. 20:3330. – DOI: https://doi.org/10.3390/electronics11203330.

11. Falguni Suthar. Advanced Cryptographic Techniques for Securing AI-Driven IoT Systems / Falguni Suthar, Hiralben Patel, Bhavesh Patel // International Journal of Scientific Research in Computer Science Engineering and Information Technology. – 2025. – Vol. 11, no. 4. – P. 392–406. – DOI: https://doi.org/10.32628/CSEIT25111686.

References

1. Voronets O. M. Method of forming sensor network coverage zones with uneven node density / Voronets O. M., Pustovoitov P. E. // Bulletin of the National Technical University "KhPI". Series: New solutions in modern technologies. – 2025. – No. 2(24). – P. 35–42. – DOI: https://doi.org/10.20998/2413-4295.2025.02.05.

2. Voronets O. M. Method of adaptive routing under conditions of variable sensor network load / Voronets O. M., Voronets V. M., Trubchaninova K. A. // Scientific notes of V. I. Vernadsky TNU. Series: Technical sciences. – 2025. – T. 37(76), No. 6. – P. 58-65. - DOI: https://doi.org/10.32782/2663-5941/2025.6.1/09.

3. Cherappa V. Energy-Efficient Clustering and Routing Using ASFO and a Cross-Layer-Based Expedient Routing Protocol for Wireless Sensor Networks / Cherappa V., Thangarajan T., Meenakshi Sundaram S. S., Hajjej F., Munusamy A. K., Shanmugam R // Sensors. – 2025. – Vol. 23, no. 5:2788. – DOI: https://doi.org/10.3390/s23052788.

4. Abidi Besma R. Survey and analysis of multimodal sensor planning and integration for wide area surveillance / Abidi Besma R., Aragam Nash R., Yao Yi, Abidi Mongi A. // Association for Computing Machinery. – 2009. – Vol. 41, no. 1:7. – P. 1-36. – DOI: https://doi.org/10.1145/1456650.1456657.

5. Duan J. Hierarchical Data Fusion Algorithm for Multiple Wind Speed Sensors in Anemometer Tower / Duan J., Zhang H., Tu C., Song J., Niu W., Zhang Z., Han J., Huo J. // Sensors. – 2026. – Vol. 26, no. 2:565. – DOI: https://doi.org/10.3390/s26020565.

6. S. Park. Survey on Anti-Drone Systems: Components, Designs, and Challenges / S. Park, H. T. Kim, S. Lee, H. Joo, H. Kim // IEEE Access. – 2021. – Vol. 9. – P. 42635-42659. – DOI: https://doi.org/10.1109/ACCESS.2021.3065926.

7. M. Hassanalian. Classifications, applications, and design challenges of drones: A review / M. Hassanalian, A. Abdelkefi // Progress in Aerospace Sciences. – 2017. – Vol. 91. – P. 99-131. – DOI: https://doi.org/10.1016/j.paerosci.2017.04.003.

8. L. Gupta. Survey of Important Issues in UAV Communication Networks / L. Gupta, R. Jain, G. Vaszkun // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, no. 2. – P. 1123-1152. – DOI: https://doi.org/10.1109/COMST.2015.2495297.

9. P. Ahmadi. A Survey on Internet of Things Security Issues and Applications / P. Ahmadi, K. Islam, T. Maco, M. Katam // 2018 International Conference on Computational Science and Computational Intelligence (CSCI). – Las Vegas, NV, USA. – 2018. – P. 925-934. – DOI: https://doi.org/10.1109/CSCI46756.2018.00182.

10. Altulaihan E. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions / Altulaihan E., Almaiah M. A., Aljughaiman A. // Electronics. – 2022. – Vol. 11, no. 20:3330. – DOI: https://doi.org/10.3390/electronics11203330.

11. Falguni Suthar. Advanced Cryptographic Techniques for Securing AI-Driven IoT Systems / Falguni Suthar, Hiralben Patel, Bhavesh Patel // International Journal of Scientific Research in Computer Science Engineering and Information Technology. – 2025. – Vol. 11, no. 4. – P. 392–406. – DOI: https://doi.org/10.32628/CSEIT25111686.