КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1208
УДК 629.735.05:681.5:519.816:004.056

Кучерявий Микола Вікторовича
спірант
Інститут проблем математичних машин та систем
Національної академії наук України, Київ, Україна
ORCID:0009-0005-0017-9797
bu9free@gmail.com

Гулак Геннадій Миколайович
доктор технічних наук, професор,
професор кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
Інститут проблем математичних машин та систем
Національної академії наук України, Київ, Україна
ORCID ID: 0000-0001-9131-9233
hulak@kubg.edu.ua

ФОРМАЛІЗОВАНА МОДЕЛЬ ОЦІНЮВАННЯ ГАРАНТОЗДАТНОСТІ СИСТЕМ УПРАВЛІННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ

Анотація. Інтенсивне впровадження безпілотних літальних апаратів у військових, цивільних, моніторингових і логістичних застосуваннях актуалізує вимоги до стійкості та безперервності роботи їхніх систем управління. Такі системи є розподіленими кіберфізичними структурами, що поєднують телеметричні підсистеми, канали зв'язку, програмні модулі обробки даних, алгоритми прийняття рішень і виконавчі механізми керування польотом. У реальних умовах експлуатації вони зазнають впливу стохастичних відмов, деградації каналів зв'язку, програмних збоїв, обмежень обчислювальних ресурсів і цілеспрямованих інформаційних впливів, що ускладнює забезпечення гарантоздатності. Метою роботи є розроблення формалізованої інтегральної моделі оцінювання гарантоздатності систем управління БПЛА, яка узгоджує різнорідні критерії функціонування та забезпечує багатокритеріальний вибір конфігурацій з урахуванням часових і ресурсних обмежень. Модель реалізовано у вигляді формалізованого обчислювального контуру, що передбачає формування вектора стану, нормування показників, їх зважене агрегування, перевірку обмежень та прийняття рішення щодо допустимості конфігурації. Розроблено алгоритм обчислення інтегрального показника з лінійною складністю відносно кількості модулів системи та врахованих ризикових факторів, що забезпечує придатність підходу для вбудованих і периферійних обчислень у системах реального часу. Запропоновано метод аналізу чутливості для ідентифікації критичних чинників деградації. Проведено сценарну апробацію для типових режимів роботи, включно зі штатним функціонуванням, погіршенням параметрів зв'язку, зростанням кіберризику та їх комбінованим впливом. Отримані результати підтверджують адекватність моделі та її практичну доцільність для моніторингу й адаптивної реконфігурації систем управління БПЛА.

Ключові слова: безпілотні літальні апарати, алгоритмізація, система управління, гарантоздатність, обчислювальна складність, багатокритеріальна оптимізація, аналіз чутливості, затримка керування.

ВСТУП

Інтенсивний розвиток безпілотних літальних апаратів (БПЛА) та розширення сфер їх застосування у військових, цивільних, моніторингових і логістичних системах зумовлюють підвищені вимоги до стійкості та безперервності функціонування їхніх систем управління. Система управління БПЛА є складною розподіленою кіберфізичною структурою, що інтегрує програмні модулі обробки даних, телеметричні підсистеми, канали зв'язку, алгоритми прийняття рішень та виконавчі механізми керування польотом [1-2, 7-8]. Надійність функціонування такої системи визначає не лише ефективність виконання місії, а й рівень безпеки експлуатації, особливо в умовах невизначеності, динамічних навантажень, деградації апаратних компонентів і можливих кіберзагроз.

У сучасних умовах експлуатації системи управління БПЛА піддаються впливу стохастичних відмов, змін характеристик каналів зв'язку, програмних збоїв та інформаційних атак, що ускладнює забезпечення їх гарантоздатності [2-4, 7]. Під гарантоздатністю у межах даного дослідження розуміється інтегральна властивість системи зберігати керованість, функціональну придатність та інформаційну стійкість у межах заданих часових і ресурсних обмежень [9-10]. Наявні підходи до оцінювання цієї властивості здебільшого базуються на окремому аналізі показників надійності, готовності чи безпеки, що не дозволяє сформувати узгоджену обчислювальну модель їх комплексного впливу на функціонування системи управління [19, 21]. Тому актуальною є задача формалізації гарантоздатності як об'єкта математичного та алгоритмічного моделювання [5, 11], що дає змогу перейти від фрагментарних характеристик до інтегрального кількісного показника, придатного для оптимізації.

У роботі застосовано комплекс методів дослідження, що включає математичне моделювання для формалізації показників надійності, готовності, функціональної безпеки та кіберстійкості [12], методи багатокритеріальної оптимізації для побудови інтегральної функції гарантоздатності [14, 19], елементи теорії ймовірностей і стохастичних процесів для опису деградаційних явищ, а також алгоритмічний аналіз для оцінювання обчислювальної складності запропонованого підходу [5, 16]. Додатково використано методи аналізу чутливості для визначення впливу окремих параметрів системи на інтегральний показник гарантоздатності, що дозволяє виявляти критичні компоненти та визначати напрями підвищення стійкості функціонування.

Наукова новизна дослідження полягає у розробленні формалізованої інтегральної моделі оцінювання гарантоздатності систем управління БПЛА, яка поєднує різнорідні функціональні та інформаційні критерії в єдиній багатокритеріальній структурі та враховує часові й ресурсні обмеження функціонування. Уперше запропоновано математичну постановку задачі оптимізації гарантоздатності як задачі багатокритеріальної оптимізації з визначенням вагових коефіцієнтів та обмежень на затримку керування і обчислювальні ресурси [14, 19, 21]. Розроблено алгоритм обчислення інтегрального показника гарантоздатності з лінійною обчислювальною складністю відносно кількості компонентів системи та факторів ризику, що забезпечує можливість його використання в режимі реального часу [12]. Також формалізовано підхід до аналізу чутливості інтегральної функції до зміни параметрів, що дозволяє визначати критичні умови втрати функціональної стійкості.

Теоретичне значення роботи полягає у розвитку методів математичного та алгоритмічного моделювання гарантоздатності складних розподілених кіберфізичних систем [9, 18, 20]. Запропонована модель розширює підходи до інтегрального оцінювання функціональної стійкості шляхом впровадження багатокритеріальної

оптимізаційної структури, що може бути використана для подальшого розвитку стохастичних, адаптивних та прогнозних моделей підтримки керованості [17]. Практичне значення дослідження полягає у можливості реалізації запропонованої моделі та алгоритму в програмних модулях моніторингу та підтримки прийняття рішень систем управління БПЛА, що дозволяє здійснювати кількісне оцінювання рівня гарантоздатності, обирати оптимальні конфігурації резервування, адаптивно перерозподіляти ресурси та забезпечувати своєчасну реконфігурацію системи в умовах деградації її компонентів.

Постановка проблеми. Системи управління безпілотними літальними апаратами є складними розподіленими кіберфізичними структурами, ефективність яких залежить від здатності зберігати керованість, коректність обробки телеметрії та стабільність прийняття рішень в умовах невизначеності [9, 18]. Функціонування таких систем відбувається під впливом стохастичних відмов, деградації каналів зв'язку, варіативних навантажень, обмежених обчислювальних ресурсів і кіберзагроз [2-4, 7-8], що підвищує вимоги до їх гарантоздатності [9-11].

Наявні підходи до оцінювання стійкості систем управління здебільшого розглядають показники надійності, готовності, безпеки та кіберстійкості ізольовано, без урахування їх взаємозв'язку та впливу часових і ресурсних обмежень [9-12]. Відсутність інтегрованої обчислювальної моделі ускладнює кількісне оцінювання гарантоздатності та порівняння альтернативних конфігурацій системи.

Додатковою проблемою є багатокритеріальний характер задачі: підвищення окремих показників часто супроводжується зростанням затримок або витрат ресурсів, що потребує узгодження суперечливих критеріїв у межах єдиної оптимізаційної постановки. Тому актуальною є розробка формалізованої математичної та алгоритмічної моделі оцінювання гарантоздатності, яка інтегрує різнорідні показники функціонування системи та дозволяє здійснювати їх багатокритеріальну оптимізацію з урахуванням обмежень.

З погляду комп'ютерних наук задача зводиться до побудови обчислювальної функції $G(X(t))$ над різнорідними метриками, її інкрементального обчислення у потоковому режимі та багатокритеріального вибору конфігурації в просторі Ω за часових і ресурсних обмежень. Тому ключовими є нормування показників, узгодження шкал, контроль обчислювальних витрат і формування Парето-компромісів.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях, пов'язані з гарантоздатністю (dependability) систем управління БПЛА, розвиваються переважно у кількох взаємопов'язаних напрямах: надійність/готовність апаратно-обчислювальної платформи та бортових обчислень; відмовостійке керування, виявлення та діагностування відмов; кібербезпека, довіра та кіберстійкість; системні огляди, які узагальнюють виклики на рівні UAV-мереж і обчислювальних систем. Так, у роботі Ahmed et al. [1] систематизовано підходи до UAV computing platforms із фокусом на апаратні збої та проблеми надійності на різних рівнях стеку, що підкреслює вагомість "обчислювального" компонента гарантоздатності для систем автономного керування. У площині безпеки й захисту від навмисних впливів значний пласт літератури присвячено загрозам на апаратному, програмному, комунікаційному та сенсорному рівнях; зокрема, Mekdad et al. [2] пропонують систематичну класифікацію загроз і механізмів захисту, демонструючи, що для БПЛА критичним є поєднання аналізу уразливостей із характеристиками надійності/доступності, оскільки атаки безпосередньо впливають на якість керування та виконання місій.

Паралельно активізувалися дослідження, орієнтовані на забезпечення стійкості керування при відмовах сенсорів/виконавчих механізмів і в умовах складних середовищ. Представницьким є напрям fault-tolerant control (FTC), де запропоновано практично-орієнтовані рішення для мультироторних платформ, що демонструють зниження деградації траєкторного керування при часткових відмовах і невизначених збуреннях [3]. Водночас зростає роль методів fault detection and diagnosis (FDD), що розглядаються як базовий рівень інтелектуальної підтримки гарантоздатності, оскільки забезпечують раннє виявлення небезпечних станів і зменшують імовірність "мовчазної деградації" керуючих контурів; у 2025 році [4] опубліковано ґрунтовний огляд FDD-методологій для БПЛА, який узагальнює сучасні підходи та підкреслює необхідність інтеграції діагностики з механізмами реконфігурації та прийняття рішень.

Окремий блок робіт фокусується на формальному аналізі надійності/готовності та використанні марковських/напівмарковських моделей для оцінювання ймовірності працездатності компонентів і системних конфігурацій. Зокрема, у [5] для літальних платформ із надлишковими роторами запропоновано підхід на основі напівмарковського моделювання, спрямований на кількісне оцінювання надійності/готовності ремонтопридатних конфігурацій, що є методологічно релевантним для формалізації частини критеріїв гарантоздатності. Однак такі підходи, як правило, зосереджені на одному класі показників (наприклад, reliability/availability) і не формують єдину інтегральну функцію, яка б узгоджувала різнорідні критерії з часовими та ресурсними обмеженнями керування.

Останнім часом посилилася увага до довіри, репутації та кіберстійких архітектур як складових гарантоздатності в середовищах із активним противником і мережевою невизначеністю. Огляд систем довіри/репутації для UAV-мереж підкреслює, що довіра стає інструментом підвищення надійності взаємодії та якості даних у динамічних мережах БПЛА, але зазвичай розглядається в контексті комунікаційної надійності та безпеки даних, без прямого узгодження з інтегральними показниками керованості та затримок [6]. Водночас у [7] запропоновано кіберстійку "відкриту" архітектуру керування дроном із декомпозицією монолітної системи на компоненти та моделлю оцінювання впливу кіберзагроз на систему, що є важливим кроком до системного поєднання безпеки та експлуатаційної стійкості. Додатково, оглядові публікації 2025 року, орієнтовані на взаємодію кібербезпеки та ШІ в UAV-системах, акцентують ризики несанкціонованого доступу, підміни навігаційних сигналів, атак на канали керування та залежність стійкості від якості моделей і телеметрії, що прямо підтримує необхідність формалізованого врахування "кіберскладової" у гарантоздатності [8].

Найбільш узагальнювальним трендом стали систематичні огляди гарантоздатності UAV-мереж і обчислювальних систем, у яких dependability трактується як сукупність reliability, availability, safety та resilience, а основними джерелами загроз визначаються відмови компонентів, роз'єднання мережі, енергетичні обмеження, програмні дефекти та вплив реального середовища [9]. Паралельно виходять огляди з тематики стійкості роїв БПЛА, де узагальнюються механізми відновлення та метрики оцінювання, але наголошується на фрагментарності підходів і складності переходу від часткових показників до системного рівня оцінки. Також запропоновано [10-11] систематичний огляд метрик безпеки UAV-операцій, що охоплює, зокрема, метрики продуктивності, комунікацій та надійності, однак не задає єдиної оптимізаційної постановки, у якій ці метрики узгоджуються з обмеженнями керування.

Узагальнення зазначених результатів дозволяє зробити висновок, що сучасні дослідження суттєво просунулися в окремих компонентах гарантоздатності (FTC/FDD

[3-4, 12], апаратна надійність, кіберстійкі архітектури [5, 7-8], довіра в UAV-мережах та системні огляди [9-11]), однак у більшості робіт відсутня єдина формалізована обчислювальна модель, яка інтегрує різнорідні критерії гарантоздатності в межах багатокритеріальної оптимізації з явними часовими та ресурсними обмеженнями, характерними для систем керування БПЛА. Саме ця прогалина визначає доцільність подальшої розробки формалізованої моделі оцінювання гарантоздатності та забезпечує основу для алгоритмічного порівняння конфігурацій, аналізу чутливості та подальшої адаптивної реконфігурації системи керування.

Мета статті. Метою статті є розроблення формалізованої математичної моделі оцінювання гарантоздатності систем управління безпілотними літальними апаратами на основі багатокритеріальної оптимізації [14, 19], що забезпечує інтеграцію показників надійності, готовності, функціональної безпеки, кіберстійкості та часових параметрів у єдину обчислювальну структуру. Досягнення поставленої мети передбачає формалізацію інтегрального показника гарантоздатності як функції взаємопов'язаних критеріїв функціонування системи управління, постановку задачі її оптимізації з урахуванням часових і ресурсних обмежень [14, 21], а також розроблення алгоритму обчислення інтегрального показника з оцінюванням його обчислювальної складності. Реалізація запропонованого підходу має забезпечити можливість кількісного аналізу рівня гарантоздатності систем управління БПЛА та створити основу для подальшого розвитку адаптивних механізмів підтримки їх функціональної стійкості.

Далі наведено формалізацію інтегральної моделі гарантоздатності та її багатокритеріальну постановку з часовими й ресурсними обмеженнями. Після цього описано алгоритм обчислення показника в режимі реального часу, виконано сценарну апробацію з формуванням Парето-множини та подано аналіз чутливості для ідентифікації критичних факторів деградації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Формалізація моделі гарантоздатності. Для побудови формалізованої моделі гарантоздатності систему управління безпілотним літальним апаратом доцільно розглядати як багатокомпонентну динамічну структуру, стан якої змінюється у часі [9, 18]. Кожен момент часу характеризується сукупністю параметрів, що відображають різні аспекти функціонування системи.

Для забезпечення узгодженого оцінювання гарантоздатності в умовах реального часу доцільно виділити мінімальний набір взаємодоповнювальних характеристик, які охоплюють безвідмовність, відновлюваність, безпеку керування, кіберризик та часову придатність контурів керування [7, 16]. Стан системи управління пропонується описувати вектором параметрів:

$$X(t) = \langle R(t), A(t), S(t), C(t), L(t) \rangle, \quad (1)$$

де $R(t)$ – функція надійності системи, $A(t)$ – готовність, $S(t)$ – показник функціональної безпеки, $C(t)$ – рівень кіберстійкості, $L(t)$ – затримка керування.

Інтегральний рівень гарантоздатності визначається як функція зазначених параметрів. Метою є максимізація інтегрального показника гарантоздатності за умови виконання ресурсних, часових та безпекових обмежень, що формалізує задачу як багатокритеріальну оптимізацію в просторі допустимих конфігурацій [14, 16].

Оптимізаційна задача формулюється як: $\max G\ (X)$, де $G(X)$ – інтегральна функція гарантоздатності.

Оскільки система функціонує в умовах обмежених ресурсів і часових вимог, вводяться такі обмеження:

$$L(t) \leq L_{max}, \tag{2}$$

що означає неперевищення допустимої затримки керування, та [16]

$$Res(t) \leq Res_{max}, \tag{3}$$

де $Res(t)$ – поточні обчислювальні витрати системи [9]. Таким чином, задача оцінювання гарантоздатності набуває вигляду задачі багатокритеріальної оптимізації з обмеженнями. У практичній реалізації $Res(t)$ може оцінюватися як зважена сума CPU time, RAM та пропускної здатності обміну: $Res(t) = w_{cpu}T_{cpu}(t) + w_{mem}M(t) + w_{bw}B(t)$, з подальшим нормуванням.

Наступним кроком є визначення аналітичних моделей для кожної складової вектора стану (1), щоб забезпечити їх сумісність у межах єдиного інтегрального показника та можливість подальшої оптимізації.

Надійність системи управління характеризує ймовірність її безвідмовної роботи протягом інтервалу часу. За припущення експоненційного закону відмов вона описується виразом:

$$R(t) = e^{-\lambda t}, \tag{4}$$

де λ – інтенсивність відмов. Експоненційний закон використано як базове наближення для ділянки сталої інтенсивності відмов; у подальших дослідженнях можливе розширення моделі на неекспоненційні або вікові закони розподілу.

Готовність системи відображає здатність виконувати функції з урахуванням можливості відновлення після відмов. Вона визначається співвідношенням:

$$A(t) = \frac{MTBF}{MTBF+MTTR}, \tag{5}$$

де $MTBF$ – середній час безвідмовної роботи, $MTTR$ – середній час відновлення. Такий показник дозволяє врахувати баланс між надійністю та швидкістю відновлення.

Кіберстійкість пропонується оцінювати через інтегральну функцію ризику, яка враховує ймовірності реалізації загроз та їхній вплив. Ризик визначається як [16]:

$$Risk = \sum_{i=1}^{m} P_i \cdot W_i, \tag{6}$$

де P_i – ймовірність і-го кіберінциденту, W_i – ваговий коефіцієнт наслідків, m – кількість ризикових факторів. Крім того, $P_i \in [0,1], W_i \in [0,1]$, а $Risk$ нормується так, щоб $Risk \in [0,1]$.

Відповідно рівень кіберстійкості визначається як доповнення до одиниці:

$$C(t) = 1 - Risk, \tag{7}$$

Чим менший інтегральний ризик, тим вищий рівень кіберстійкості.

Функціональна безпека пов'язана з імовірністю втрати керування або некоректного виконання команд [3-4, 12]. Вона визначається як:

$$S(t) = 1 - P_{loss\_control}, \tag{8}$$

де $P_{loss\_control}$ – імовірність втрати керованості.

Затримка керування є критичною характеристикою систем реального часу [16]. Вона складається з трьох компонентів:

$$L(t) = L_{comm} + L_{proc} + L_{decision}, \tag{9}$$

де враховано затримку передачі даних, обробки та прийняття рішень. Оскільки критерії мають різну фізичну природу та суперечливі тенденції (наприклад, посилення захисту може збільшувати затримку), інтеграцію доцільно виконати через нормовану зважену агрегацію із явною штрафною складовою за порушення часової придатності керування.

Для узгодження всіх критеріїв у межах єдиної оцінки пропонується зважена багатокритеріальна функція:

$$G(t) = aR + \beta A + \gamma S + \delta C - \theta \frac{L}{L_{max}}, \tag{10}$$

де вагові коефіцієнти $a, \beta, \gamma, \delta, \theta$ задовольняють умову нормування:

$$a + \beta + \gamma + \delta + \theta = 1, \tag{11}$$

Обмеження (2)–(3) задають "жорстку" допустимість, тоді як штрафна складова в (10) реалізує "м'яку" перевагу конфігурацій із меншими затримками всередині допустимої області.

Позитивні складові підвищують гарантоздатність, тоді як зростання затримки зменшує її значення. Вагові коефіцієнти можуть визначатися експертним методом, методом аналізу ієрархій (AHP) або шляхом нормалізації пріоритетів конкретної місії [19, 21]. У базовому варіанті дослідження для демонстрації моделі застосовано рівномірний розподіл ваг, що дозволяє уникнути суб'єктивного перекосу в оцінюванні окремих критеріїв.

Для візуального узагальнення формули (10) наведено структурну схему, яка відображає надходження нормованих критеріїв до блока зваженої інтеграції та формування інтегрального показника гарантоздатності.

На рис. 1 зображено логіку формування інтегрального показника гарантоздатності $G(X)$ шляхом зваженої інтеграції основних функціональних критеріїв: надійності $R(t)$, готовності $A(t)$, функціональної безпеки $S(t)$, кіберстійкості $C(t)$ та затримки керування $L(t)$. Усі показники подаються на блок зваженої інтеграції відповідно до формули (10), після чого формується узагальнений інтегральний показник, який використовується для оцінювання рівня гарантоздатності системи управління в режимі реального часу.

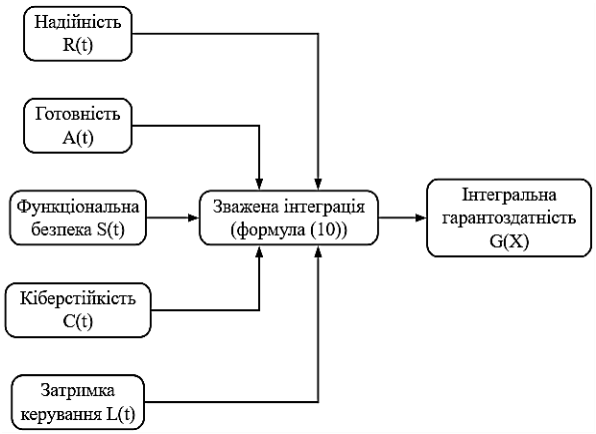

Рис. 1. Структурна схема інтеграції складових показників у моделі гарантоздатності системи управління БПЛА

Якщо рис. 1 відображає логіку обчислення інтегрального показника, то на архітектурному рівні важливо показати, де саме цей модуль розміщується в контурі керування та які дані отримує/повертає для підтримки реконфігурації.

Відповідно на рис. 2 зображено узагальнену архітектуру системи управління безпілотним літальним апаратом із інтегрованим модулем оцінювання гарантоздатності $G(X)$. Основний функціональний контур включає сенсорну підсистему, модуль попередньої обробки та оцінювання стану, контур керування та виконавчі механізми, які формують замкнений цикл керування польотом. Модуль оцінювання гарантоздатності $G(X)$ отримує телеметричні дані, параметри стану системи, інформацію про режим функціонування та відгук виконавчих механізмів. На основі цих даних формується інтегральний показник гарантоздатності відповідно до співвідношень (1)–(11) та обмежень (2)–(3). У разі виявлення зниження рівня гарантоздатності або перевищення обмежень за затримкою чи ресурсами, модуль передає сигнали до підсистеми моніторингу та реконфігурації. Підсистема моніторингу забезпечує адаптацію параметрів керування та діагностики, що дозволяє здійснювати динамічну реконфігурацію системи та підтримувати її функціональну стійкість у режимі реального часу.

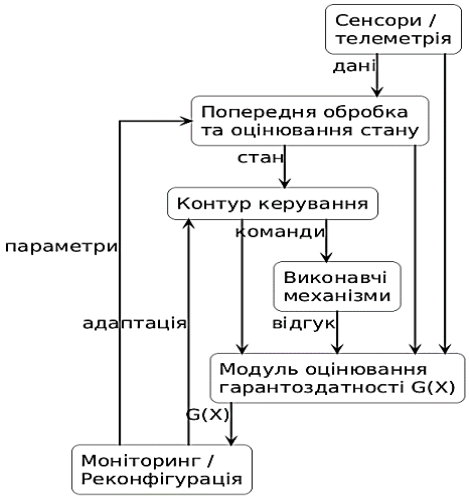

Рис. 2. Узагальнена архітектура системи управління БПЛА з інтеграцією модуля оцінювання гарантоздатності

Задача пошуку оптимального стану системи формулюється як:

$$max\, G\,(X),\ X \in \Omega, \tag{12}$$

де Ω – множина допустимих конфігурацій. Парето-оптимальність забезпечує вибір таких рішень, для яких неможливо покращити один критерій без погіршення іншого [19]. У практичній реалізації це означає аналіз множини альтернативних конфігурацій системи управління з урахуванням ресурсних та часових обмежень [14, 21], після чого здійснюється ранжування допустимих варіантів за значенням інтегральної функції $G(X)$. Такий підхід дозволяє поєднати багатокритеріальну природу задачі з однокритеріальним механізмом прийняття рішення на основі агрегованого показника гарантоздатності.

Для застосування постановки (12) у практичних системах керування необхідно отримувати значення $G(X)$ оперативно, з передбачуваною обчислювальною складністю та контролем ресурсних обмежень, що зумовлює розроблення відповідного алгоритму обчислення.

Алгоритм оцінювання та складність. Для практичної реалізації запропонованої математичної моделі розроблено алгоритм обчислення інтегрального показника гарантоздатності, який забезпечує послідовне формування складових критеріїв та їх узгоджену інтеграцію в єдину функцію оцінювання. Алгоритм орієнтований на використання в системі моніторингу стану управління безпілотним літальним апаратом у режимі реального часу [16] та передбачає обробку як поточних телеметричних даних, так і статистичних характеристик функціонування системи.

Вхідними даними алгоритму є телеметричні параметри функціонування модулів системи управління [18], статистичні показники відмов (зокрема інтенсивність відмов, MTBF та MTTR), набір актуальних ризикових факторів із відповідними ваговими коефіцієнтами, параметри затримки передачі та обробки інформації, а також граничні допустимі значення затримки керування L_{max} і обчислювальних ресурсів Res_{max}. Результатом роботи алгоритму є інтегральний показник гарантоздатності G, який кількісно відображає поточний рівень функціональної стійкості системи управління.

Реалізація алгоритму передбачає послідовне виконання таких етапів. На першому етапі здійснюється зчитування та агрегування телеметричних даних від усіх функціональних модулів системи [18]. Далі на основі інтенсивності відмов обчислюється функція надійності $R(t)$, після чого визначається показник готовності $A(t)$ з урахуванням статистичних характеристик безвідмовної роботи та відновлення. На наступному етапі формується інтегральна оцінка ризику, що дозволяє визначити рівень кіберстійкості $C(t)$. Паралельно оцінюється показник функціональної безпеки $S(t)$, який характеризує імовірність збереження керованості системи. Після цього розраховується сумарна затримка керування $L(t)$ як сума комунікаційної, обчислювальної та алгоритмічної складових.

Отримані значення підставляються до інтегральної функції, внаслідок чого формується узагальнений показник гарантоздатності G [9]. На завершальному етапі здійснюється перевірка виконання обмежень: якщо виконується умова $L(t) \le L_{max}$ та $Res(t) \le Res_{max}$, обчислений показник приймається як допустимий результат; у протилежному випадку формується сигнал про перевищення допустимих параметрів функціонування. Після цього алгоритм повертає значення інтегрального показника G, яке може бути використане для подальшого аналізу або прийняття управлінських рішень [10, 18-19]. Запропонований алгоритм забезпечує узгоджене обчислення всіх складових

гарантоздатності та може бути інтегрований у програмне забезпечення системи управління БПЛА для адаптивного контролю її функціонального стану.

Для забезпечення відтворюваності обчислювальної процедури наведено блок-схему, яка деталізує послідовність обчислення складових критеріїв, перевірку обмежень та формування вихідного показника для модулів моніторингу й реконфігурації.

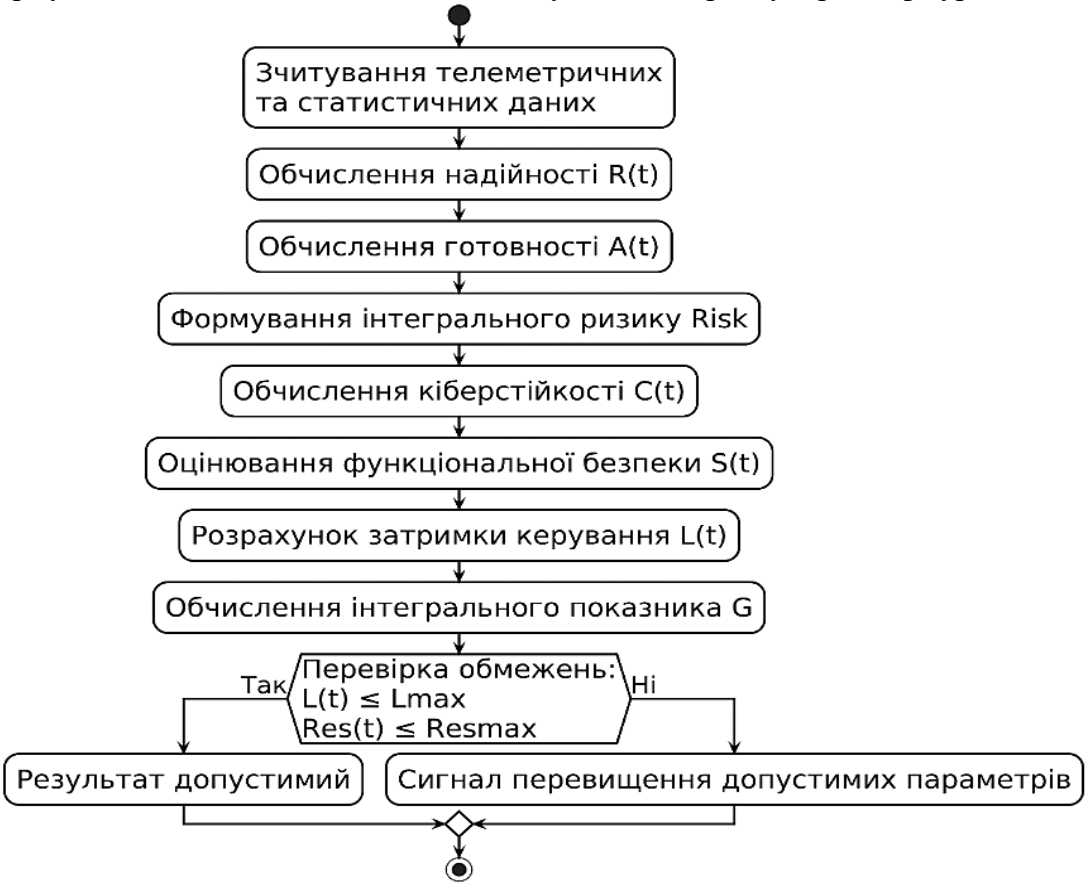

Рис. 3. Блок-схема алгоритму обчислення інтегрального показника гарантоздатності

На рис. 3 представлено послідовність реалізації алгоритму оцінювання гарантоздатності системи управління БПЛА. Алгоритм передбачає зчитування телеметричних і статистичних даних, поетапне обчислення складових показників (надійності, готовності, інтегрального ризику, кіберстійкості, функціональної безпеки та затримки керування), формування інтегрального показника G відповідно до зваженої функції (10) та перевірку виконання обмежень за затримкою керування і використанням ресурсів. У разі дотримання обмежень результат приймається як допустимий, інакше формується сигнал про перевищення граничних параметрів.

Нехай n – кількість функціональних модулів системи управління БПЛА, m – кількість врахованих ризикових факторів. Обчислення показників надійності, готовності та затримки передбачає обробку даних для кожного модуля, що має складність $O(n)$. Формування інтегрального ризику потребує послідовної обробки всіх ризикових факторів зі складністю $O(m)$ [13, 15]. Інші операції виконуються за сталий час і не впливають на асимптотичну оцінку. Отже, сумарна обчислювальна складність алгоритму становить:

$$T(n,m) = O(n+m), \tag{13}$$

Лінійна складність забезпечує можливість застосування алгоритму в режимі реального часу без суттєвого навантаження на обчислювальні ресурси системи [16-17].

Для визначення впливу окремих параметрів на інтегральний показник розглядаються часткові похідні $\frac{\partial G}{\partial R} = a$, що характеризує внесок надійності, та $\frac{\partial G}{\partial L} = -\frac{\theta}{L_{max}}$, що відображає чутливість до затримки керування за фіксованих значень інших критеріїв та за умови нормування показників.

Сценарна апробація моделі та аналіз компромісних конфігурацій. Для перевірки працездатності запропонованої моделі оцінювання гарантоздатності проведено її сценарну апробацію в межах множини допустимих конфігурацій системи управління Ω [20]. Множина Ω формувалася як сукупність альтернативних варіантів побудови системи, що відрізняються рівнем резервування критичних модулів, інтенсивністю діагностичного моніторингу, параметрами кіберзахисту, а також допустимими межами використання обчислювальних ресурсів.

Сценарний аналіз здійснювався для чотирьох типових режимів функціонування системи управління БПЛА [13-15, 20]:

- S1 – штатний режим, що характеризується стабільними параметрами зв'язку та відсутністю активних кіберзагроз;
- S2 – деградація каналу зв'язку, що проявляється у зростанні затримки керування;
- S3 – підвищення кіберризику, пов'язане з імовірністю реалізації атак на інформаційні компоненти;
- S4 – комбінований вплив, який поєднує погіршення зв'язку та зростання ризику.

Для кожного сценарію здійснювалося обчислення інтегрального показника гарантоздатності G відповідно до функції (10) з перевіркою виконання обмежень (2)–(3) [16]. Отримані результати показали, що модель адекватно відображає вплив різнорідних факторів на загальний рівень гарантоздатності.

У сценарії S1 значення G є максимальним серед розглянутих варіантів і визначається високими значеннями надійності та кіберстійкості за фіксованих A та S. У сценарії S2 основним фактором зниження інтегрального показника стає збільшення нормалізованої затримки L/L_{max}, що приводить до зростання штрафної складової функції (10) [14]. У сценарії S3 зменшення G зумовлене зниженням рівня кіберстійкості C через зростання інтегрального ризику [15, 20]. У сценарії S4 спостерігається комбінований ефект, який призводить до більш істотного зниження гарантоздатності та може вивести систему в прикордонну область допустимих рішень.

Для числової демонстрації роботи інтегральної функції (10) використано рівномірний розподіл вагових коефіцієнтів ($a = \beta = \gamma = \delta = \theta = 0{,}2$), що забезпечує збалансоване врахування всіх критеріїв без пріоритетного зміщення окремих складових. У числовій апробації показники готовності A та функціональної безпеки S прийнято сталими (відповідно A=0,95, S=0,97), тоді як варіації виконано за R, C та L/L_{max} для демонстрації чутливості інтегральної функції до типових деградаційних факторів зв'язку та кіберризику. Результати обчислення інтегрального показника гарантоздатності наведено в табл. 1. Для ілюстрації чутливості інтегральної функції (10) до типових деградаційних факторів виконано сценарну оцінку за фіксованими вагами та нормалізацією затримки відносно L_{max}. Числові значення в таблиці наведено як демонстраційний приклад роботи моделі в умовах зміни параметрів зв'язку та кіберризику.

Числові значення в табл. 1 наведено як демонстраційний приклад (toy example) для ілюстрації поведінки інтегральної функції за контрольованої зміни L/L_{max} та C і не претендують на відтворення конкретної платформи БПЛА.

Таблиця 1

Числова апробація інтегрального показника гарантоздатності

Сценарій	Надійність (R)	Готовність (A)	Функціональна безпека (S)	Рівень кіберстійкості (C)	Нормалізована затримка керування (L/L_{max})	Інтегральний показник гарантоздатності (G)
S1	0,98	0,95	0,97	0,95	0,40	0,69
S2	0,98	0,95	0,97	0,95	0,80	0,61
S3	0,98	0,95	0,97	0,75	0,40	0,65
S4	0,92	0,95	0,97	0,70	0,85	0,54

Дані табл. 1 узгоджено ілюструють реакцію інтегральної функції (10) на зміну експлуатаційних умов. У штатному режимі S1 отримано G=0,69, що відповідає підвищеному рівню гарантоздатності за фіксованих A та S. У сценарії S2 значення G знижується до 0,61 переважно через зростання нормалізованої затримки L/L_{max}. У сценарії S3 зменшення G до 0,65 зумовлене спадом кіберстійкості C при незмінній часовій придатності. Найменше значення спостерігається у комбінованому сценарії S4 (G =0,54), що відображає сумарний ефект одночасної деградації зв'язку та зростання кіберризику.

Багатокритеріальний характер задачі зумовлює існування компромісних конфігурацій, вибір яких залежить від пріоритетів місії та вагових коефіцієнтів інтегральної функції. Аналіз показав, що існують варіанти побудови системи, які забезпечують підвищення кіберстійкості за незначного зростання затримки, а також конфігурації, у яких подальше підвищення захищеності супроводжується непропорційним зростанням часових витрат [14-15, 20]. Таким чином, отримані результати відображають компроміс між показниками R, C та L і дозволяють обґрунтовано обирати конфігурацію залежно від пріоритетів місії.

Для переходу від точкових оцінок у табличній формі до аналізу компромісів між критеріями наведемо графічне відображення залежності між часовою придатністю керування та інтегральною оцінкою, що дозволяє інтерпретувати результати у термінах Парето-оптимальності.

На рис. 4 представлено графічну інтерпретацію компромісу між нормалізованою затримкою керування L/L_{max} т та інтегральним показником гарантоздатності G для сценаріїв S1–S4. Точки S1–S4 ілюструють компромісні стани системи для різних сценаріїв функціонування [14, 22]. Зі зростанням нормалізованої затримки керування спостерігається зниження інтегрального показника гарантоздатності, що відображає конфлікт між часовими параметрами та загальною функціональною стійкістю системи.

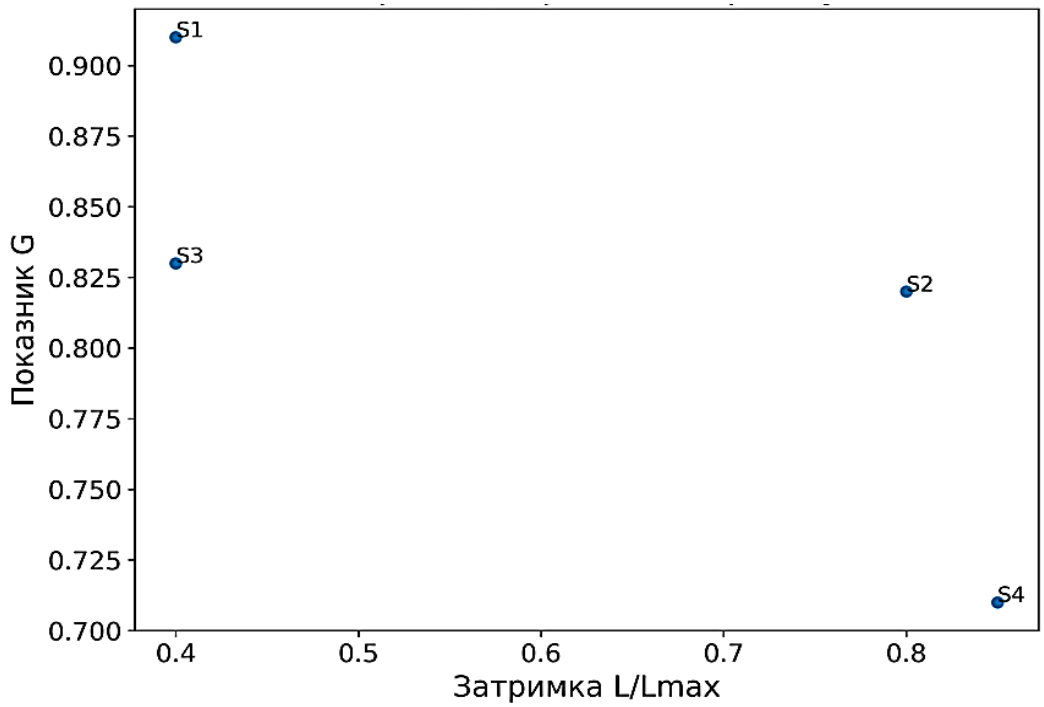

Рис. 4. Компроміс між нормалізованою затримкою керування та інтегральним показником гарантоздатності

Отримані результати підтверджують, що запропонована модель забезпечує не лише інтегральне оцінювання гарантоздатності, а й можливість структурованого вибору конфігурацій у просторі допустимих рішень Ω, що є ключовим для систем управління реального часу.

Аналіз чутливості та інтерпретація отриманих результатів. Для визначення критичних факторів, що найбільше впливають на інтегральний показник гарантоздатності, виконано аналіз чутливості функції (10) до зміни її складових параметрів [14]. Враховуючи лінійну структуру інтегральної функції, вплив кожного критерію визначається відповідним ваговим коефіцієнтом та нормалізацією показників.

Аналіз показав, що підвищення надійності R, готовності A, функціональної безпеки S та кіберстійкості C монотонно збільшує значення інтегрального показника G, тоді як зростання затримки керування L призводить до його зменшення через штрафну складову [13, 16]. При цьому характер впливу часових параметрів визначається співвідношенням L/L_{max}, що дозволяє враховувати допустимі межі для систем реального часу.

Результати сценарного аналізу підтвердили, що в умовах штатного функціонування визначальним фактором гарантоздатності є рівень надійності та готовності системи. Натомість у режимах деградації зв'язку або підвищеного кіберризику домінуючим стає вплив відповідно затримки або показника кіберстійкості [15, 20]. Таким чином, інтегральна модель дозволяє кількісно ідентифікувати, який саме фактор є критичним у конкретних умовах експлуатації.

Оскільки часові затримки є ключовим фактором деградації в реальних контурах керування, доцільно окремо проаналізувати вплив нормалізованої затримки на інтегральний показник за фіксованих значень інших критеріїв [16]. Для наочного підтвердження отриманої залежності побудовано графік чутливості (рис. 5) інтегрального показника гарантоздатності G до зміни нормалізованої затримки

керування L/L_{max} за фіксованих значень інших критеріїв. Така візуалізація дозволяє інтерпретувати штрафну складову в (10) як лінійний механізм "пригнічення" гарантоздатності зі зростанням затримки. З графіка видно монотонне лінійне зменшення G зі зростанням L/L_{max}, що узгоджується з аналітичним виразом (10) та похідною $\partial G/\partial L$ [16]. Отже, часові характеристики є одним із ключових факторів деградації гарантоздатності в режимах погіршення зв'язку [13], а параметр θ визначає "жорсткість" штрафу та зміщує оптимальні рішення у бік мінімізації затримки.

Встановлено, що зміна вагових коефіцієнтів суттєво впливає на вибір Парето-оптимальної конфігурації. Збільшення коефіцієнта θ зміщує оптимальні рішення у бік мінімізації затримки керування, що є доцільним для місій із жорсткими часовими вимогами [16, 22]. Натомість підвищення ваги δ призводить до вибору конфігурацій із зниженим інтегральним ризиком, навіть за умови зростання обчислювальних витрат або часу обробки.

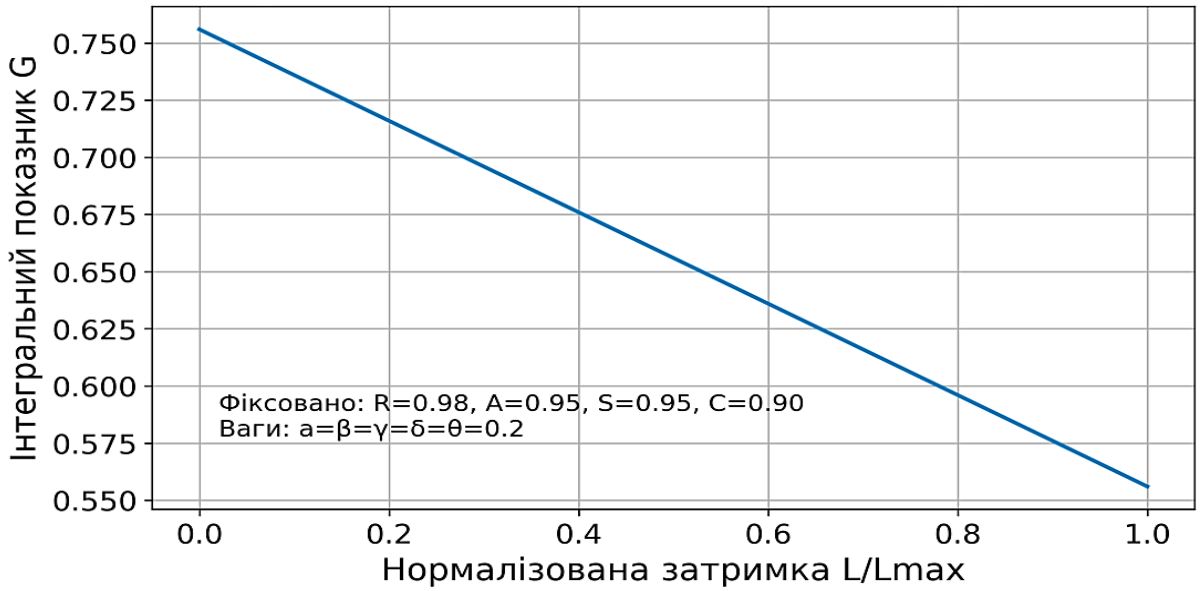

Рис. 5. Графік залежності інтегрального показника гарантоздатності G від нормалізованої затримки керування L/L_{max} (за фіксованих R, A, S, C)

Інтерпретація отриманих результатів свідчить, що запропонована модель є адаптивним інструментом підтримки прийняття рішень [17, 20]. Вона дозволяє не лише оцінювати поточний рівень гарантоздатності, але й прогнозувати наслідки зміни архітектурних або програмних параметрів системи управління. Зокрема, модель може бути використана для обґрунтування доцільності резервування окремих модулів, зміни параметрів кіберзахисту або перерозподілу обчислювальних ресурсів у разі наближення до граничних значень затримки.

Для підкреслення відмінності запропонованої інтегральної постановки від традиційних фрагментарних оцінок доцільно зіставити, які саме аспекти (часова придатність та ризик) враховуються різними підходами. З метою узагальнення отриманих результатів та демонстрації відмінностей запропонованого підходу від традиційних ізольованих оцінок проведено порівняльний аналіз критеріїв оцінювання гарантоздатності (табл. 2).

Таблиця 2

Порівняння інтегрального підходу та ізольованих критеріїв оцінювання

Підхід	Урахування затримки керування	Урахування ризику	Інтегральний характер	Придатність для реального часу (online)
Окрема оцінка надійності *R*	Ні	Ні	Ні	Так*
Окрема оцінка кіберстійкості C	Ні	Так	Ні	Так*
Запропонована модель гарантоздатності	Так	Так	Так	Так

* *Примітка: ізольовані показники можуть обчислюватися в online-режимі, однак не забезпечують узгодження критеріїв у контурі керування та не підтримують інтегральний вибір компромісних конфігурацій за часових/ресурсних обмежень.*

Як видно з табл. 2, традиційні підходи не забезпечують комплексного врахування часових та ризикових характеристик системи. Запропонована інтегральна модельна відміну від ізольованих оцінок, підтримує online-оцінювання в контурі керування та враховує часові й ресурсні обмеження, а також поєднує всі ключові критерії в єдиній функції оцінювання, що забезпечує системність, адаптивність та придатність для використання в режимі реального часу.

Таким чином, результати аналізу чутливості підтверджують, що інтегральна багатокритеріальна модель забезпечує збалансоване врахування функціональних, інформаційних та часових характеристик і може бути використана як основа для формування адаптивної політики управління гарантоздатністю систем управління безпілотними літальними апаратами. Отримані результати підтверджують практичну придатність запропонованої моделі для інтеграції в системи управління БПЛА реального часу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено формалізований підхід до оцінювання гарантоздатності систем управління безпілотними літальними апаратами як інтегральної характеристики їх функціональної стійкості в умовах невизначеності, деградації компонентів і можливих кіберзагроз. Проведені формалізація, алгоритмізація та сценарна апробація узгоджено демонструють придатність моделі як інструмента оперативного моніторингу й вибору компромісних конфігурацій у просторі критеріїв. Аналіз чутливості доповнює результати, забезпечуючи інтерпретованість ідентифікації домінуючих факторів деградації в конкретних умовах експлуатації.

Запропонована модель забезпечує комплексне поєднання показників надійності, готовності, функціональної безпеки, кіберстійкості та часових параметрів у межах єдиної обчислювальної структури, що дозволяє перейти від фрагментарного аналізу окремих критеріїв до узгодженого інтегрального оцінювання стану системи управління.

Отримані результати підтвердили, що інтегральний підхід дає змогу кількісно відображати вплив різнорідних чинників на рівень гарантоздатності та адекватно реагує на зміни умов функціонування. У штатному режимі система зберігає високий рівень стійкості, тоді як у сценаріях деградації каналу зв’язку або зростання кіберризику спостерігається прогнозоване зниження інтегрального показника. Побудова Парето-множини дозволила виявити компроміс між часовими характеристиками та загальною стійкістю, що створює основу для обґрунтованого вибору конфігурації системи залежно

від пріоритетів конкретної місії. Аналіз чутливості продемонстрував керованість моделі та можливість ідентифікувати критичні фактори, які найбільше впливають на втрату функціональної стійкості.

Практична значущість дослідження полягає у можливості інтеграції запропонованого підходу в програмні модулі моніторингу систем управління БПЛА для підтримки прийняття рішень у режимі реального часу. Модель може використовуватися для оцінювання доцільності резервування, адаптивного перерозподілу ресурсів, посилення кіберзахисту та своєчасної реконфігурації архітектури системи в умовах наближення до граничних режимів функціонування.

Перспективи подальших досліджень пов’язані з поглибленням робастності моделі за рахунок врахування стохастичних збурень і неповноти телеметричних даних, автоматизованим налаштуванням вагових параметрів залежно від типу місії та експлуатаційних умов, а також інтеграцією прогнозних механізмів для раннього виявлення критичних режимів. Доцільним є також проведення експериментальної валідації на цифрових двійниках або апаратних стендах із кількісним оцінюванням ефективності реконфігураційних стратегій. Таким чином, запропонований підхід формує методичну основу для розвитку адаптивних систем управління гарантоздатністю безпілотних літальних апаратів у складних і динамічних середовищах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ahmed, F., & Jenihhin, M. (2022). A survey on UAV computing platforms: A hardware reliability perspective. *Sensors*, 22(16), 6286. https://doi.org/10.3390/s22166286
2. Mekdad, Y., Arış, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, 224, 109626. https://doi.org/10.1016/j.comnet.2023.109626
3. Khattab, A., Mizrak, I., & Alwi, H. (2024). Fault-tolerant control of an octorotor UAV using sliding mode for applications in challenging environments. *Annual Reviews in Control*, 57, 100952. https://doi.org/10.1016/j.arcontrol.2024.100952
4. Adaika, Z., Al-Haddad, L. A., Giernacki, W., et al. (2025). Fault detection and diagnosis methodologies for unmanned aerial vehicles: State of the art. *Journal of Intelligent & Robotic Systems*, 111, 63. https://doi.org/10.1007/s10846-025-02267-8
5. Mittal, N., Ivanova, N., Jain, V., & Vishnevsky, V. (2024). Reliability and availability analysis of high-altitude platform stations through semi-Markov modeling. *Reliability Engineering & System Safety*, 252, 110419. https://doi.org/10.1016/j.ress.2024.110419
6. Ogunbunmi, S., Chen, Y., Blasch, E., & Chen, G. (2024). A survey on reputation systems for UAV networks. *Drones*, 8(6), 253. https://doi.org/10.3390/drones8060253
7. d’Ambrosio, N., Perrone, G., Romano, S. P., & Urraro, A. (2024). A cyber-resilient open architecture for drone control. *Computers & Security*, 150, 104205. https://doi.org/10.1016/j.cose.2024.104205
8. Alsadie, D. (2025). Cybersecurity and artificial intelligence in unmanned aerial vehicles: Emerging challenges and advanced countermeasures. *IET Information Security*. Advance online publication. https://doi.org/10.1049/ise2/2046868
9. Zhang, Q., Furqan, M. D., Nutzhat, T., Machida, F., & Andrade, E. C. (2025). Dependability of UAV-based networks and computing systems: A survey. *arXiv preprint*, arXiv:2506.16786.
10. Hamid, A., Almoghathawi, Y., Alghazi, A., & Saleh, H. (2025). Enhancing resilience in UAV swarms: A literature review. *Journal of Safety Science and Resilience*, 100268. https://doi.org/10.1016/j.jnlssr.2025.100268
11. Asghari, O., Ivaki, N., & Madeira, H. (2025). UAV operations safety assessment: A systematic literature review. *ACM Computing Surveys*, 57. https://doi.org/10.1145/3723871
12. Gao, Z., Cecati, C., & Ding, S. X. (2015). A survey of fault diagnosis and fault-tolerant techniques—Part I: Fault diagnosis with model-based and signal-based approaches. *IEEE Transactions on Industrial Electronics*, 62(6), 3757–3767. https://doi.org/10.1109/TIE.2015.2417501

13. Kostiuk, Y., Bebeshko, B., Hulak, H., Skladannyi, P., Rzaeva, S., & Khorolska, K. (2024). Ensuring cybersecurity and data transmission performance in wireless networks. *Information Security*, 30(3), 365–375.
14. Atli, İ., Ozturk, M., Valastro, G., & Asghar, M. (2021). Multi-objective UAV positioning mechanism for sustainable wireless connectivity in environments with forbidden flying zones. *Algorithms*, 14(11), 302. https://doi.org/10.3390/a14110302
15. Skladannyi, P., Kostiuk, Y., Rzaeva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting various classes of network attacks. *Cybersecurity: Education, Science, Technology*, 3(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772
16. Ancel, E., Capristan, F., Foster, J., & Condotta, R. (2017). Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM). In *AIAA Aviation 2017 Forum*. https://doi.org/10.2514/6.2017-3273
17. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. https://doi.org/10.18372/2225-5036.31.20634
18. MahmoudZadeh, S., Yazdani, A., Kalantari, Y., Ciftler, B., Aidarus, F., & Al Kadri, M. O. (2024). Holistic review of UAV-centric situational awareness: Applications, limitations, and algorithmic challenges. *Robotics*, 13(8), 117. https://doi.org/10.3390/robotics13080117
19. Ramírez-Atencia, C., Rodríguez-Fernández, V., & Camacho, D. (2020). A revision on multi-criteria decision making methods for multi-UAV mission planning support. *Expert Systems with Applications*, 160, 113708. https://doi.org/10.1016/j.eswa.2020.113708
20. Kostiuk, Y., Skladannyi, P., Rzaeva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based smart grid environments. *Cybersecurity: Education, Science, Technology*, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
21. Ayvaz, E., Atay, Y., & Babaoğlu, İ. (2025). A cutting-edge approach to multi-UAV mission planning using enhanced constraint satisfaction. *Journal of Intelligent & Robotic Systems*, 111, 95. https://doi.org/10.1007/s10846-025-02279-4
22. Li, J., Li, J., Zhang, J., & Meng, W. (2026). A comprehensive review of path-planning algorithms for multi-UAV swarms. *Drones*, 10(1), 11. https://doi.org/10.3390/drones10010011

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Mykola Kucheriavyi
PhD student
Institute for Problems of Mathematical Machines and Systems
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID:0009-0005-0017-9797
bu9free@gmail.com

Hennadii Hulak
Doctor of Sience, Professor,
Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
Institute for Problems of Mathematical Machines and Systems NASU, Kyiv, Ukraine
ORCID: 0000-0001-9131-9233
h.hulak@kubg.edu.ua

A FORMALIZED MODEL FOR ASSESSING THE DEPENDABILITY OF UNMANNED AERIAL VEHICLE CONTROL SYSTEMS BASED ON MULTI-CRITERIA OPTIMIZATION

Abstract. The intensive deployment of unmanned aerial vehicles in military, civilian, monitoring, and logistics applications increases the requirements for resilience and operational continuity of their control systems. Such systems represent distributed cyber-physical structures that integrate telemetry subsystems, communication channels, data processing modules, decision-making algorithms, and flight control actuators. Under real operating conditions, they are exposed to stochastic failures, communication degradation, software faults, computational resource constraints, and targeted information attacks, which complicates the assurance of dependability. The aim of this study is to develop a formalized integrated model for evaluating the dependability of UAV control systems that harmonizes heterogeneous operational criteria and enables multi-criteria configuration selection under temporal and resource constraints. The model is implemented as a formalized computational framework that includes state vector formation, indicator normalization, weighted aggregation, constraint verification, and decision-making regarding configuration admissibility. An algorithm for computing the integrated dependability indicator with linear complexity relative to the number of system modules and considered risk factors is developed, ensuring the suitability of the approach for embedded and edge computing in real-time systems. A sensitivity analysis method is proposed to identify critical degradation factors. Scenario-based validation is conducted for typical operational modes, including nominal operation, communication degradation, increased cyber risk, and their combined impact. The results confirm the adequacy of the model and its practical applicability for monitoring and adaptive reconfiguration of UAV control systems.

Keywords: unmanned aerial vehicles, algorithmization, control system, dependability, computational complexity, multi-criteria optimization, sensitivity analysis, control latency.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ahmed, F., & Jenihhin, M. (2022). A survey on UAV computing platforms: A hardware reliability perspective. *Sensors*, 22(16), 6286. https://doi.org/10.3390/s22166286
2. Mekdad, Y., Arış, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, 224, 109626. https://doi.org/10.1016/j.comnet.2023.109626
3. Khattab, A., Mizrak, I., & Alwi, H. (2024). Fault-tolerant control of an octorotor UAV using sliding mode for applications in challenging environments. *Annual Reviews in Control*, 57, 100952. https://doi.org/10.1016/j.arcontrol.2024.100952
4. Adaika, Z., Al-Haddad, L. A., Giernacki, W., et al. (2025). Fault detection and diagnosis methodologies for unmanned aerial vehicles: State of the art. *Journal of Intelligent & Robotic Systems*, 111, 63. https://doi.org/10.1007/s10846-025-02267-8

5. Mittal, N., Ivanova, N., Jain, V., & Vishnevsky, V. (2024). Reliability and availability analysis of high-altitude platform stations through semi-Markov modeling. *Reliability Engineering & System Safety*, 252, 110419. https://doi.org/10.1016/j.ress.2024.110419
6. Ogunbunmi, S., Chen, Y., Blasch, E., & Chen, G. (2024). A survey on reputation systems for UAV networks. *Drones*, 8(6), 253. https://doi.org/10.3390/drones8060253
7. d'Ambrosio, N., Perrone, G., Romano, S. P., & Urraro, A. (2024). A cyber-resilient open architecture for drone control. *Computers & Security*, 150, 104205. https://doi.org/10.1016/j.cose.2024.104205
8. Alsadie, D. (2025). Cybersecurity and artificial intelligence in unmanned aerial vehicles: Emerging challenges and advanced countermeasures. *IET Information Security*. Advance online publication. https://doi.org/10.1049/ise2/2046868
9. Zhang, Q., Furqan, M. D., Nutzhat, T., Machida, F., & Andrade, E. C. (2025). Dependability of UAV-based networks and computing systems: A survey. *arXiv preprint*, arXiv:2506.16786.
10. Hamid, A., Almoghathawi, Y., Alghazi, A., & Saleh, H. (2025). Enhancing resilience in UAV swarms: A literature review. *Journal of Safety Science and Resilience*, 100268. https://doi.org/10.1016/j.jnlssr.2025.100268
11. Asghari, O., Ivaki, N., & Madeira, H. (2025). UAV operations safety assessment: A systematic literature review. *ACM Computing Surveys*, 57. https://doi.org/10.1145/3723871
12. Gao, Z., Cecati, C., & Ding, S. X. (2015). A survey of fault diagnosis and fault-tolerant techniques—Part I: Fault diagnosis with model-based and signal-based approaches. *IEEE Transactions on Industrial Electronics*, 62(6), 3757–3767. https://doi.org/10.1109/TIE.2015.2417501
13. Kostiuk, Y., Bebeshko, B., Hulak, H., Skladannyi, P., Rzaeva, S., & Khorolska, K. (2024). Ensuring cybersecurity and data transmission performance in wireless networks. *Information Security*, 30(3), 365–375.
14. Atli, İ., Ozturk, M., Valastro, G., & Asghar, M. (2021). Multi-objective UAV positioning mechanism for sustainable wireless connectivity in environments with forbidden flying zones. *Algorithms*, 14(11), 302. https://doi.org/10.3390/a14110302
15. Skladannyi, P., Kostiuk, Y., Rzaeva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting various classes of network attacks. *Cybersecurity: Education, Science, Technology*, 3(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772
16. Ancel, E., Capristan, F., Foster, J., & Condotta, R. (2017). Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM). In *AIAA Aviation 2017 Forum*. https://doi.org/10.2514/6.2017-3273
17. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. https://doi.org/10.18372/2225-5036.31.20634
18. MahmoudZadeh, S., Yazdani, A., Kalantari, Y., Ciftler, B., Aidarus, F., & Al Kadri, M. O. (2024). Holistic review of UAV-centric situational awareness: Applications, limitations, and algorithmic challenges. *Robotics*, 13(8), 117. https://doi.org/10.3390/robotics13080117
19. Ramírez-Atencia, C., Rodríguez-Fernández, V., & Camacho, D. (2020). A revision on multi-criteria decision making methods for multi-UAV mission planning support. *Expert Systems with Applications*, 160, 113708. https://doi.org/10.1016/j.eswa.2020.113708
20. Kostiuk, Y., Skladannyi, P., Rzaeva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based smart grid environments. *Cybersecurity: Education, Science, Technology*, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
21. Ayvaz, E., Atay, Y., & Babaoğlu, İ. (2025). A cutting-edge approach to multi-UAV mission planning using enhanced constraint satisfaction. *Journal of Intelligent & Robotic Systems*, 111, 95. https://doi.org/10.1007/s10846-025-02279-4
22. Li, J., Li, J., Zhang, J., & Meng, W. (2026). A comprehensive review of path-planning algorithms for multi-UAV swarms. *Drones*, 10(1), 11. https://doi.org/10.3390/drones10010011

Отримано редакцією журналу / Received: 28.01.26
Прорецензовано / Revised: 17.02.26
Схвалено до друку / Accepted: 26.03.26

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023