Вячеслав ХАРЧЕНКО,
доктор технічних наук,
завідувач кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»,
ORCID: https://orcid.org/0000-0001-5352-077X
e-mail: v.kharchenko@csn.khai.edu

Герман ФЕСЕНКО,
доктор технічних наук,
професор кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»,
ORCID: https://orcid.org/0000-0002-4084-2101
e-mail: h.fesenko@csn.khai.edu

DOI: https://doi.org/10.32620/pls.2025.8.78

БЕЗПІЛОТНІ ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОМУНІКАЦІЙ І ПОДОЛАННЯ НЕБЕЗПЕЧНИХ ПРОСТОРІВ: МЕТОДОЛОГІЧНІ ЗАСАДИ ТА ПРОЄКТНІ РІШЕННЯ

Анотація. *Розглянуто методологію застосування безпілотних інтелектуальних систем для моніторингу, трансформації та безпечного подолання небезпечних просторів, що виникли внаслідок російської військової агресії. Автори пропонують уніфіковане поняття небезпечного простору (Dangerous Space) та чотирьохетапний операційний цикл для роботи з ним. Технологічною основою є різнорідні безпілотні комплекси, об'єднані за принципом сервісної моделі DUFaaS (Dependable UxV Fleet as a Service). Для забезпечення якості та безпеки систем розроблено модель оцінки якості штучного інтелекту, метод аналізу ризиків XMECA/IMECA та моделі надійності групових місій. Результати досліджень апробовані в проєктах, зокрема, при розробці систем доповненої реальності для саперів, алгоритмів розгортання мереж LiFi та симуляторів динамічних середовищ.*

Ключові слова: *небезпечний простір, безпілотні інтелектуальні системи, критична інфраструктура, стійкість, кібербезпека, рої безпілотників.*

Мотивація. Російська повномасштабна агресія проти України призвела до формування значної кількості небезпечних просторів (НП), що становлять загрозу життю людей та функціонуванню критичної інфраструктури (КІ). До таких просторів належать: 1) мінні поля та акваторії, що перешкоджають гуманітарному розмінуванню, відновленню сільського господарства та промислових об'єктів; 2) зруйновані будівлі та об'єкти КІ (наприклад, Трипільська ТЕС), що потребують моніторингу, оцінки стану та пошуку постраждалих; 3) території лісових пожеж, спричинених обстрілами та зміною клімату, які потребують системного моніторингу та ліквідації; 4) інші зони підвищеного ризику, де неможливо ефективно застосовувати традиційні технічні засоби та системи зв'язку.

Ці виклики обумовлюють нагальну потребу в розробці інноваційних методів та технологій для: 1) оперативного моніторингу параметрів небезпечних просторів; 2) безпечного подолання цих просторів людьми та технікою; 3) трансформації небезпечних зон у безпечні; 4) гарантованого забезпечення зв'язку в умовах руйнувань для прийняття рішень кризовими центрами.

Концептуальні основи досліджень. В рамках дослідження запропоновано уніфіковане визначення: небезпечний простір (Dangerous Space, DS) – це двовимірна або тривимірна область, яка становить значну фізичну та/або кіберзагрозу для безпеки людей, стану природних ресурсів і перешкоджає ефективному функціюванню технічних та комунікаційних систем. Робота з НП структурована навколо чотирьох головних завдань (Tasks, T):

T1. Моніторинг НП. Виявлення, ідентифікація та оцінка параметрів простору (розміри, тип загрози, її інтенсивність, динаміка) для підтримки прийняття рішень.

T2. Трансформація НП. Повне або часткове перетворення небезпечного простору на

безпечний відповідно до вимог щодо розмірів цільової зони та допустимого рівня зниження небезпеки (наприклад, розмінування ділянки під прокладання дороги).

Т3. Безпечне подолання НП. Забезпечення проходження через НП людей, техніки або матеріалів з урахуванням обмежень на вхідні/вихідні точки та характеристики об'єктів.

Т4. Забезпечення зв'язку в НП. Організація передачі даних від джерел інформації, розташованих усередині НП (сенсори, розвідники), до центрів прийняття рішень (кризових центрів).

Для виконання цих завдань запропоновано універсальний операційний цикл, що включає чотири етапи (Operations, Op):

Op1. Моніторинг та ідентифікація. Первинне або періодичне обстеження НП з використанням UxV з різними сенсорами. Результат – оновлена цифрова модель або цифровий двійник (Digital Twin) простору, що відображає всі загрози та перешкоди.

Op2. Специфікація та планування. На основі моделі формулюються конкретні цілі (наприклад, «розмінувати коридор завширшки 10м»), обираються оптимальні або раціональні алгоритми виконання (маршрутизації, розподілу ресурсів).

Op3. Розгортання та виконання. Практична реалізація плану шляхом введення в НП відповідних безпілотних систем (одиночних апаратів, роїв або флотів). Використовуються алгоритми багатоагентної координації та багатомаршрутного проходження.

Op4. Забезпечення надійності експлуатації. Супровід роботи системи з метою підтримки її працездатності, функційної безпеки та кібербезпеки протягом усього часу виконання місії, включаючи реагування на відмови та зовнішні впливи.

Технологічна основа досліджень. Ядром технологічного арсеналу є різнорідні безпілотні комплекси (UxV), що охоплюють всі середовища: UAV (Unmanned Aerial Vehicle, літальні), UGV (Unmanned Ground Vehicle, наземні), USV (Unmanned Surface Vessel, надводні), UUWV (Unmanned Underwater Vessel, підводні), UUGV (Unmanned Underground Vehicle, підземні).

Їхня ефективність досягається за рахунок комбінації таких ключових принципів:

1) Мультипросторова орієнтація. Застосування гетерогенних флотів для комплексного вирішення завдань. Наприклад: UAV + UGV (літальні апарати ведуть дистанційний моніторинг лісової пожежі, визначають фронт вогню, а наземні роботи здійснюють локалізацію, прокладання траншей або доставку вогнегасних засобів; UAV + USV + UUV (під час розмінування морської акваторії USV несе сонар для пошуку мін, UAV забезпечує координацію і зв'язок, а UUV проводить детальну ідентифікацію та знешкодження під водою).

2) Мультизадачність платформ. Один тип апаратів може виконувати різні функції. Наприклад, UAV може бути носієм сенсорів для моніторингу, ретранслятором зв'язку або платформою для детектування мін.

3) Мультисенсорне злиття даних (Sensor Fusion). Використання різних типів датчиків на одному безпілотнику або у рої для підвищення достовірності (оптичні та тепловізійні камери, радари, магнетометри, газоаналізатори, дозиметри).

4) Архітектурна надмірність та відмовостійкість. Застосування структурної, часової та інформаційної надмірності на всіх рівнях: від дубльованого бортового обладнання до можливості динамічної перебудови рою при втраті одного з апаратів. Реалізується принцип керованої деградації (managed degrading), коли система здатна виконувати місію навіть у зниженому режимі якості.

5) Dependable UxV Fleet as a Service (DUFaaS) – надійний флот UxV як послуга. Ця модель передбачає розгляд флоту безпілотників не як набору окремих пристроїв, а як єдиного сервісу, доступного для користувача (рятувальників, військових, енергетиків). Завданням сервісу є гарантоване виконання місії із заданими показниками готовності, часу виконання та безпеки, незалежно від внутрішніх відмов окремих апаратів або зовнішніх атак. Для оцінки такої системи ефективно використовується теорія масового обслуговування (Queuing Theory), де заявками є місії, а каналами обслуговування – доступні безпілотники флоту.

Методологічна основа досліджень. Для проектування, аналізу та забезпечення якості UxV-систем розроблено та адаптовано низку формальних моделей і методів:

1) Модель якості систем штучного інтелекту (ШІ). ШІ є ключовим компонентом для автономної навігації, розпізнавання об'єктів та прийняття рішень. Запропонована модель містить 46 характеристик, об'єднаних у групи, що виходять за межі технічної точності: довірчоздатність (trustworthiness), яка охоплює традиційні характеристики надійності та безпеки; поясненість (explainability), що є здатністю ШІ-моделі надавати зрозуміле для людини обґрунтування свого рішення (чому апарат визначив об'єкт як міну); відповідальність (responsibility) та етичність (ethics), які враховують соціальні та моральні аспекти роботи автономних систем; законність (lawfulness), яка характеризує відповідність нормативним вимогам. Ця модель дозволяє комплексно оцінювати та вибирати ШІ-рішення для конкретних завдань у НП [1].

2) Метод XMECA (eXtended Mode, Effects and Criticality Analysis). Це розширення класичного аналізу відмов для кіберфізичних систем. Особливо важливим є його підвид – IMECA (Intrusion Modes, Effects and Criticality Analysis) для аналізу кіберзагроз. Метод дозволяє: систематично виявляти всі можливі способи відмов або кібератак

на компоненти UxV-системи (наприклад, спотворення даних GPS, захоплення каналу управління, відмова сенсора); оцінити наслідки кожної відмови/атаки для виконання місії; визначити критичність кожної загрози (наприклад, за шкалою від 1 до 10); на основі матриці критичності обрати найбільш ефективні технічні, програмні або організаційні заходи для зниження ризику (наприклад, впровадження криптозахисту каналів, резервування навігаційних систем) [2-4].

3) Моделі надійності для планування місій Multi-UAV. Розроблено математичні моделі, які дозволяють оцінювати ймовірність успішного виконання групової місії з урахуванням надійності окремих апаратів, їх маршрутів через НП з різною інтенсивністю загроз, а також можливості взаємодопомоги у рої. Ці моделі є основою для алгоритмів автоматичного планування, що генерують не лише оптимальні за часом чи енергією маршрути, але й максимально надійні з точки зору збереження цілісності рою [5, 6].

Практична реалізація. Дослідницька методологія була опробована під час виконання міжнародних та українських проєктів, де, зокрема, були отримані такі результати:

1) Розроблено концепцію та моделі систем, де UGV або UAV співпрацюють з тренованими тваринами (наприклад, щурами) для пошуку вибухонебезпечних предметів [7].

2) Розроблено прототип системи доповненої реальності (Augmented Reality, AR), де сапер через спеціальні окуляри або планшет отримує на накладне зображення місцевості інформацію про виявлені UxV вибухонебезпечні предмети: тип, координати, ступінь загрози.

3) Розроблено алгоритми та програмне забезпечення для швидкого розгортання бездротових мереж зв'язку на основі видимого світла (LiFi) з використанням UAV. Ці мережі стійкі до радіоелектронного впливу і можуть бути розгорнуті в умовах руйнувань. Алгоритми «прямокутників» та «керованого водоспаду» дозволяють автоматично розміщувати UAV-ретранслятори, уникаючи перешкод і забезпечуючи безперервний канал зв'язку з кризовим центром [8].

4) Створено інструмент, що дозволяє моделювати складні динамічні середовища з рухомими перешкодами (дим, туман), статичними руїнами та джерелами небезпеки (пожежа, вибух). Симулятор автоматично будує маршрути для ланцюга UxV (наприклад, для організації зв'язку) за алгоритмом A* з подальшим уточненням. Це дозволяє проводити віртуальне планування місій та оцінювати їхню життєздатність до реального розгортання [9].

Висновки. Концепція небезпечного простору та запропонований операційний цикл формують універсальну методологічну основу. Абстрагуючись від конкретних загроз, вони дозволяють системно підходити до моніторингу, планування, виконання та забезпечення надійності робіт у будь-яких умовах ризику, спрощуючи розробку універсальних алгоритмів і технологічних рішень.

Практична реалізація методології ґрунтується на комбінації гетерогенних безпілотних систем, моделі DUFaaS та комплексного наукового забезпечення. Використання різнорідних роїв апаратів (UAV, UGV, USV) за сервісною моделлю «флот як послуга» забезпечує гнучкість і живучість, а тріада з якості ШІ, аналізу ризиків (XMECA/IMECA) та моделей надійності створює основу для створення функційних, стійких і соціально прийнятних систем.

Практична значущість та перспективи розвитку підтверджені результатами проєктів та чітко окресленими напрямками. Розроблені інструменти – від летючих мереж LiFi до AR-інтерфейсів та симуляторів 3D-середовищ – формують готову технологічну базу. Майбутні дослідження можуть бути спрямовані на глибшу інтеграцію з цифровими двійниками, розвиток колективного інтелекту роїв та адаптацію систем для захисту нових видів КІ.

Бібліографічні посилання

1. Харченко В. С., Фесенко Г. В., Ілляшенко О. О. Базова модель нефункційних характеристик для оцінки якості штучного інтелекту. Radioelectronic and Computer Systems. 2022. No. 2(102). P.131–144. DOI: 10.32620/reks.2022.2.11.

2. Illiashenko O., Kharchenko V., Babeshko I., Fesenko H., Di Giandomenico F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Entropy. 2023. Vol. 25, no. 8, article no. 1123. P. 1–35. DOI: 10.3390/e25081123.

3. Kharchenko V., Illiashenko O., Fesenko H., Babeshko I. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis. Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science / ed. by A. Dziech, W. Mees, M. Niemiec. Cham, Switzerland : Springer, 2022. Vol. 1689. P. 66–79. DOI: 10.1007/978-3-031-20215-5_6.

4. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. Radioelectronic and Computer Systems. 2023. No. 4(108). P. 152–170. DOI: 10.32620/reks.2023.4.11.

5. Fesenko H., Illiashenko O., Kharchenko V., Leichenko K., Sachenko A., Scislo L. Methods and Software Tools for Reliable Operation of Flying LiFi Networks in Destruction Conditions. Sensors. 2024. Vol. 24, no. 17, article no. 5707. P. 1–32. DOI: 10.3390/s24175707.

6. Kharchenko V., Kliushnikov I., Rucinski A., Fesenko H., Illiashenko O. UAV Fleet as a Dependable Service for Smart Cities: Model-Based Assessment and Application. Smart Cities. 2022. Vol. 5, no. 3. P. 1151–1178. DOI: 10.3390/smartcities5030058.

7. Fedorenko G., Fesenko H., Kharchenko V., Kliushnikov I., Tolkunov I. Robotic-biological systems for detection and identification of explosive ordnance: concept, general structure, and models. Radioelectronic and Computer Systems. 2023. No. 2(106). P. 143–159. DOI: 10.32620/reks.2023.2.12.

8. Leichenko K., Fesenko H., Kharchenko V., Illiashenko O. Deployment of a UAV swarm-based LiFi network in the obstacle-ridden environment: algorithms of finding the path for UAV placement. Radioelectronic and Computer Systems. 2024. No. 1(109). P. 176–195. DOI: 10.32620/reks.2024.1.14.

9. Остапенко Л. Ю., Харченко В. С. Система для моделювання подолання перешкод і організації комунікацій в небезпечних просторах: структура та експериментальні дослідження. Системи управління, навігації та зв'язку. 2025. Том 3, № 81. С. 128–135. DOI: 10.26906/SUNZ.2025.3.128-135.

V. Kharchenko, H. Fesenko

Unmanned intelligent systems for providing communications and overcoming dangerous spaces: methodological foundations and design solutions.

Abstract. A methodology for applying unmanned intelligent systems to monitor, transform, and safely traverse dangerous spaces resulting from Russian military aggression is examined. The authors propose a unified concept of a Dangerous Space and a four-stage operational cycle for working within it. The technological foundation consists of heterogeneous unmanned complexes (integrated via the DUFaaS (Dependable UxV Fleet as a Service) model). To ensure system quality and security, an AI quality assessment model, the XMECA/IMECA risk analysis method, and reliability models for group missions are developed. The research results have been tested in projects, including the development of augmented reality systems for sappers, LiFi network deployment algorithms, and dynamic environment simulators.

Keywords: dangerous space, unmanned intelligent systems, critical infrastructure, resilience, cybersecurity, UAV swarms.

Зразок для цитування:

Харченко В., Фесенко Г. Безпілотні інтелектуальні системи для забезпечення комунікацій і подолання небезпечних просторів: методологічні засади та проєктні рішення. Пропілеї права та безпеки, 2025. №8. С. 294-297. DOI: https://doi.org/10.32620/pls.2025.8.78.