

**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**  
**Військовий інститут телекомунікацій та інформатизації**  
**імені Героїв Крут**

---

**MINISTRY OF DEFENCE OF UKRAINE**  
**Military Institute of Telecommunications and Informatization Technologies**  
**named after Heroes of Kruty**



**Системи і технології зв'язку, інформатизації та кібербезпеки**  
**№ 4**

---

**Communication, informatization and cybersecurity systems and technologies**  
**№ 4**

У збірнику викладено статті наукових та науково-педагогічних працівників, докторантів, ад'юнктів (аспірантів), курсантів, здобувачів інституту та інших установ (організацій) за наступними науковими напрямками:

перспективи розвитку телекомунікаційних систем, комплексів та засобів спеціального призначення;

захист інформації в спеціальних інформаційно-комунікаційних системах;

стан і розвиток автоматизованих систем управління військами та зброєю;

інформаційні системи та мережі, системи підтримки прийняття рішень спеціального призначення;

бойове застосування систем зв'язку та автоматизації Збройних сил України;

теорія і практика кібербезпеки та інформаційної боротьби в комп'ютеризованих системах і мережах.

Запрошуємо до співробітництва всі зацікавлені установи та організації, які проводять наукові дослідження та науково-технічні розробки за даними напрямками.

The book contains articles of scientific and teaching staff, post graduate students, adjuncts, institute applicants and other institutions (organizations) applicants in the following fields:

prospects of telecommunications systems, development, facilities and means of special purpose;

in special information protection and communication systems;

automated systems state and development of army weapons;

information systems and networks, decision support systems for special purposes;

combat use of communications systems and automation of Armed Forces of Ukraine;

theory and practice of cyber security and information warfare in computerized systems and networks.

All interested institutions and organizations, who conduct research and development in the directions state, are invited for cooperation.

**Редакційна колегія:**

<b>Головний редактор:</b>	<i>Романюк В. А.</i> , д-р техн. наук, професор	
<b>Заступник головного редактора:</b>	<i>Радзівілов Г. Д.</i> , канд. техн. наук, професор	
<b>Відповідальний секретар:</b>	<i>Нестеренко М. М.</i> , канд. техн. наук, доцент	
<b>Члени редколегії:</b>	<i>Беляков Р. О.</i> , канд. техн. наук, доцент; <i>Гуржій П. М.</i> , канд. техн. наук; <i>Жук О. В.</i> , д-р техн. наук; <i>Жук О. Г.</i> , канд. техн. наук; <i>Ковальчук Л. В.</i> , д-р техн. наук, професор; <i>Креденцер Б. П.</i> , д-р техн. наук, професор, пров. наук співр.;	<i>Могилевич Д. І.</i> , д-р техн. наук, професор; <i>Романов О. І.</i> , д-р техн. наук, професор; <i>Самохвалов Ю. Я.</i> , д-р техн. наук, професор; <i>Сова О. Я.</i> , д-р техн. наук, ст. наук. співр.;
	<i>Лінков І. Ю.</i> , д-р техн. наук, Senior Scientific and Technical Manager, US Army Engineer Research and Development Center, Concord;	<i>Толопа С. В.</i> , д-р техн. наук, професор; <i>Штаненко С. С.</i> , канд. техн. наук, доцент

**Системи і технології зв'язку, інформатизації та кібербезпеки:** збірник наукових праць / за заг. ред. В. А. Романюка. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2023. № 4. 126 с.

**ISSN 2786-6610**

Всі наукові статті, включені до збірника, прорецензовані фахівцями з відповідних галузей та отримали позитивний відгук.

При передрукуванні матеріалів обов'язкове посилання на збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Статті, розміщені у збірнику, затверджені Вченою радою Військового інституту телекомунікацій та інформатизації імені Героїв Крут (протокол засідання № 6 від 28.11 2023 року).

Науковий профіль видання:  
125 Кібербезпека;  
126 Інформаційні системи та технології;  
255 Озброєння та військова техніка

Засновник – Військовий інститут телекомунікацій та інформатизації імені Героїв Крут  
(код за ЄДРПОУ 24978555).

Свідоцтво про державну реєстрацію видання: КВ № 25184-15124 Р від 20.07.2022.

Адреса редакції: 01011, м. Київ, вул. Князів Острозьких, 45/1. Тел. 256-22-73.

Електронна адреса: [naukaviti@gmail.com](mailto:naukaviti@gmail.com)

Відповідальні за випуск: Головка О. Є., Куцаєв В. В.

Зам. 216. Друк. арк. 15,75. Ум.-друк. арк. 14,64. Обл.-вид. арк. 13,62.

Формат паперу 60×84/8. Тираж 50 прим.

Адреса друкарні ВІТІ імені Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

## З М І С Т

1.	<b>Беляков Р. О., Фесенко О. Д., Остапчук В. М., Радзівілов Г. Д.</b> Методика управління позиціонуванням комунікаційних аероплатформ FANET в умовах радіоелектронної протидії	5
2.	<b>Бернацький А. П.</b> Метод планування шляху автономного наземного робота з використанням модифікації динамічного двонаправленого RRT-алгоритму	16
3.	<b>Данилюк І. А., Радченко М. М., Шаповал В. М., Сидоркін П. Г.</b> Методика раціонального вибору безпілотного авіаційного комплексу для побудови телекомунікаційних аероплатформ	32
4.	<b>Легкобит В. С., Стоцький І. В., Карпенко А. О.</b> Підвищення точності класифікації об'єктів на місцевості на основі поєднання сенсорних модальностей із використанням бінарної кросетропії як функції втрат	44
5.	<b>Мельник Б. О., Овчаренко І. В., Новікова І. В.</b> Техніко-економічна оцінка ремонту озброєння та військової техніки	55
6.	<b>Романюк В. А., Гримуд А. Г.</b> Аналіз правил побудови траєкторії польоту для збору даних телекомунікаційною аероплатформою з вузлів безпроводової сенсорної мережі	65
7.	<b>Субач І. Ю., Власенко О. В.</b> Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення	82
8.	<b>Хорошко В. О., Клімович С. О., Янковський О. Г.</b> Контроль та діагностування послідовних цифрових структур	93
9.	<b>Чевардін В. Є., Юрченко О. В., Залужний О. В., Пелешок Є. В.</b> Аналіз конкурентних атак на моделі машинного навчання систем кіберзахисту	100
10.	<b>Штаненко С. С., Самохвалов Ю. Я., Толюпа С. В.</b> Підхід до визначення технічного стану мікропроцесорних систем, реалізованих на програмно-реконфігурованій логіці	110
	<b>Автори номера</b>	124
	<b>Пам'ятка автору</b>	126

**C O N T E N T S**

1.	<b>R. Bieliakov, O. Fesenko, V. Ostapchuk, H. Radzivilov</b> Methodology positional controlling of communications aerial platform in FANET in the minds of influction of radio electronic countermeasures	5
2.	<b>A. Bernatskyi</b> Method for planning the way of UGV using a modification of dynamic bi-directional RRT algorithm	16
3.	<b>I. Danyliuk, M. Radchenko, V. Shapoval, P. Sidorkin</b> Method of rational choice of unmanned aircraft for construction of telecommunication aeroplatforms	32
4.	<b>V. Legkobyt, I. Stotskiy, A. Karpenko</b> Improving the accuracy of object classification on the ground based on a combination of sensory modalities using binary cross-tropism as a loss function	44
5.	<b>B. Melnyk, Ig. Ovcharenko, Ir. Novikova</b> Technical and economic assessment of the repair of weapons and military equipment's repair	55
6.	<b>V. Romaniuk, A. Hrymud</b> Analysis of the rules for constructing a flight trajectory of a communication aerial platform for data collection from nodes of a wireless sensor network	65
7.	<b>I. Subach, O. Vlasenko</b> Architecture of intelligent SIEM for detecting cyber incidents in databases of military information and communication systems	82
8.	<b>V. Khoroshko, S. Klimovych, O. Yankovskyi</b> Control and diagnostics of sequential digital structures	93
9.	<b>V. Chevardin, O. Yurchenko, O. Zaluzhnyi, Ye. Peleshok</b> Analysis of adversarial attacks on the machine learning models of cyberprotection systems	100
10.	<b>S. Shtanenko, Y. Samokhvalov, S. Toliupa</b> Approach to determining the technical state of microprocessor systems implemented on software-reconfiguration logic	110
	<b>About authors</b>	124
	<b>Memo to the author</b>	126

УДК 681.518

канд. техн. наук Беляков Р. О. ORCID: 0000-0001-9882-3088 (ВІТІ ім. Героїв Крут)

Фесенко О. Д. ORCID: 0000-0002-2114-5327 (ВІТІ ім. Героїв Крут)

Остапчук В. М. ORCID: 0000-0001-5686-0198 (ВІТІ ім. Героїв Крут)

канд. техн. наук, професор Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)

## МЕТОДИКА УПРАВЛІННЯ ПОЗИЦІЮВАННЯМ КОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ FANET В УМОВАХ РАДІОЕЛЕКТРОННОЇ ПРОТИДІЇ

У статті розглядається методика управління позиціонуванням комунікаційних аероплатформ (далі – КА) в мережі FANET в умовах радіоелектронної протидії для досягнення цільової функції: підвищення точності управління навігаційними параметрами (переміщенням) комунікаційних аероплатформ (зменшення відхилення від цільової траєкторії).

У роботі показано процес управління параметрами позиціонування КА FANET під час розгортання, функціонування та управління процесом ротації головного вузла повітряної комунікаційної підмережі.

Здійснено оцінку відхилення навігаційних параметрів КА з використанням імітаційного моделювання. Формалізовано процес визначення координат КА за прийнятими сигналами (зондами) по основному каналу передачі. В статті показано застосування резервного каналу на базі LoRa для збереження управління в умовах втрати GPS-сигналів, що може стати підґрунтям для оцінки енерговитрат КА мережі в процесі інформаційного обміну. Процес адаптивного підлаштування навігаційних параметрів КА в роботі пропонується здійснювати з використанням фільтра Калмана.

Наукова новизна методики полягає у застосуванні науково-методичного апарату тригонометричних перетворень каналної матриці і розрахунку азимутального та елеваційного кута для додаткового корегування навігаційних параметрів позиціонування КА відносно мобільної базової станції.

Такий підхід дозволяє досягти оптимізації цільових функцій процесу управління позиціонуванням та забезпечення прийняття рішень в реальному часі. Результати імітаційного моделювання підтверджують можливість забезпечення меншого відхилення навігаційних параметрів до 30 м відносно відомого рішення із застосуванням алгоритму PSO 340–400 м по висоті.

**Ключові слова:** комунікаційні мережі, FANET, LoRa, комунікаційні аероплатформи, топологія, траєкторія польоту, прогнозування, фільтрація Калмана, енергоефективність, продуктивність мережі, радіоелектронна протидія

**R. Bieliakov, O. Fesenko, V. Ostapchuk, H. Radzivilov Methodology positional controlling of communications aerial platform in FANET in the minds of influction of radio electronic countermeasures.**

The article considers the method of controlling the positioning of communication aerial platforms in the FANET network in the conditions of radio-electronic countermeasures to achieve the target function: increasing the accuracy of managing the navigation parameters (movement) of communication aerial platforms (reducing the deviation from the target trajectory). The work shows the process of controlling the parameters of FANET communication aerial platforms positioning in the process of deployment, operation, and control of the rotation process of the main node of the air communication subnet.

The deviation of the navigation parameters of the communication aerial platforms was estimated using simulation modeling. The process of determining the coordinates of the communication aerial platforms based on the received signals (probes) on the main transmission channel has been formalized. The article shows the use of a backup channel based on LoRa, to maintain control in conditions of loss of GPS signals, which can become the basis for estimating the energy consumption of the communication aerial platforms network in the process of information exchange. The process of adaptive adjustment of the navigation parameters of the communication aerial platforms is proposed to be carried out using the Kalman filter. The scientific novelty of the method consists in the application of a scientifically methodical apparatus of trigonometric transformations of the channel matrix and calculation of azimuthal and elevation angles for additional correction of navigation parameters by positioning the communication aerial platforms relative to the mobile base station.

This approach allows you to achieve optimization of the target functions of the positioning management process and ensure real-time decision-making. The results of simulation modeling confirm the possibility of providing a smaller deviation of navigation parameters up to 30 m compared to the known solution using the PSO algorithm 340–400 m in height.

**Keywords:** communication networks, FANET, LoRa, communication aerial platforms, topology, flight path, forecasting, Kalman filtering, energy efficiency, network performance, electronic countermeasures.

**Постановка задачі.** Забезпечення зв'язку в інтересах підрозділів Збройних Сил України (далі – ЗСУ) стикається зі зростаючою тенденцією радіоелектронної протидії з боку російського агресора. Внаслідок таких дій виникає низка задач щодо функціонування засобів зв'язку ЗСУ з урахуванням обмежень. Одним із можливих рішень є розгортання мереж FANET [1; 2].

Необхідно зазначити, що складність застосування мереж класу FANET у зонах активних бойових дій полягає у тимчасовій або повній відсутності сигналів супутникових систем, які використовуються для корекції навігаційних параметрів комунікаційних аероплатформ, що обумовлює впровадження нових підходів і методик для реалізації процесу управління траєкторією. Це обмеження спонукає застосовувати додатковий комплекс програмно-апаратних засобів, додаткових каналів управління для компенсації шумів та направлених завад, застосовувати складні математичні перетворення та алгоритми фільтрації тощо. Один зі шляхів удосконалення процесу корекції навігаційних параметрів комунікаційних аероплатформ в умовах радіоелектронної протидії є використання резервних низькошвидкісних каналів зв'язку типу Long Range (далі – LoRa). Необхідно зазначити, що низькошвидкісні канали зв'язку типу LoRa не є єдиним можливим підходом для забезпечення функціонування в умовах активної радіопротидії, і також можуть піддаватися впливам завад, суттєво погіршуючи свої характеристики [3].

Однак, особливістю LoRa є можливість адаптивної зміни структури повідомлення, тобто використання завадостійкого кодування, для зменшення імовірності втрати пакетів навіть при переважаючій за рівнем перешкод. Так, у статті [4] наведено математичну модель FANET із застосуванням в якості резервного додатковий низькошвидкісний канал типу LoRa в умовах складної заводої обстановки, що надихнуло авторів до написання статті в цій предметній області.

Отже, вирішення наукової задачі забезпечення мінімального відхилення траєкторії КА в процесі польоту під час тимчасового або повного зникнення опорного сигналу глобальної супутникової системи для компенсації похибки позиціонування КА, що наростає із часом, є актуальним.

**2. Аналіз останніх публікацій.** Процес управління положенням КА, що знайшли своє застосування як окремо, так і у складі FANET, супроводжується значною кількістю публікацій.

У [5] використовуються алгоритми машинного навчання з підкріпленням для прогнозування 3D-траєкторії польоту КА, однак оптимізація часу функціонування мережі не розглядалася, також не було враховано модель шуму.

У [6] авторами запропонована модель управління розгортанням та оперативного управління КА FANET мережі. В статті визначено, що прогнозування відхилення маршруту польоту здійснюється завдяки алгоритму Калмана. Однак детально процес прийняття рішення з управління КА не розкритий, також не наведено, які навігаційні параметри застосувались, що суттєво впливає на результат прогнозування.

Так, в статті [7] показано спосіб побудови топології FANET, а саме процес забезпечення зв'язності між наземною станцією управління та КА, завдяки управлінню параметрами позиціонування безпілотної літальної апаратури (далі – БпЛА). Авторами запропоновано алгоритм побудови топології FANET з урахуванням алгоритму оптимізації рою частинок (Particle Swarm Optimization, PSO). Численні результати показують, що запропонований алгоритм досягає значного приросту продуктивності порівняно зі схемою побудови топології, яка застосовує моделі алгоритмів на основі нормального розподілу. Однак автори застосовують лінійну імітаційну модель у двомірній площині, що ускладнює процес оцінки впливу високої динаміки переміщення на параметри позиціонування КА, також у статті не досліджено вплив шуму на процеси обміну даними.

У науковому дослідженні [8] представлено процеси управління комунікаційними вузлами (КА) мережі на основі повнозв'язної домінуючої множини параметрів, суть якої полягає у вирішенні задачі багатокритеріальної оптимізації, а саме управлінні параметрами потужності, передачі та положенні вузлів під час побудови первинної топології. Автори розробили групу алгоритмів для побудови та підтримки топології за допомогою дискретизованого за часом підходу. Результати симуляції показують, що запропонований спосіб має кращу продуктивність під час управління КА порівняно із загальним алгоритмом оптимізації рою частинок. Однак автори статті не розглядали випадки розгортання мережі FANET під час зникнення опорних сигналів глобальних супутникових систем, крім того, авторами було застосовано допущення щодо представлення моделі БпЛА як довільної точки в просторі, що не дозволяє застосувати запропонований алгоритм для забезпечення мінімально допустимого відхилення навігаційних параметрів в умовах радіоелектронної протидії (далі – РЕП). Можливість динамічного управління топологією, траєкторією переміщення КА, їхнім взаємним розміщенням, локацією точок зависання та інтервалами обміну даними з повітряними комунікаційними вузлами суттєво впливає на ефективність інформаційного обміну [9].

Таким чином, у статті запропоновано застосувати для управління позиціонуванням КА під час зникнення глобальних систем позиціонування найпоширеніший алгоритм – фільтр Калмана, та оцінити його ефективність щодо існуючого рішення на основі алгоритму PSO – фільтра частинок.

**Метою статті** є розробка методики управління параметрами позиціонування КА в умовах РЕП.

**Виклад основного матеріалу.** Розглядаються елементи повітряної мережі КА на етапі розгортання (польоту до визначених географічних координат) під час втрати опорного сигналу глобальної системи навігації внаслідок впливу РЕП.

КА підтримують однакові протоколи інформаційного обміну, мають обмежені дальність радіозв'язку і швидкість обміну. Кожен вузол мережі має власну систему управління, діє в кооперації з іншими вузлами мережі і КА.

БпЛА (КА) обладнані: прийомопередавачем із можливістю переналагодження на резервний низькошвидкісний канал LoRa; антенною системою МІМО 2\*2; інерціальною навігаційною системою та приймачем GPS-сигналів глобальної навігаційної супутникової системи.

Роль центру управління повітряної мережі виконує мобільна базова станція (далі – МБС) (рис. 1), що обладнана комунікаційним обладнанням MU-MIMO, відносно якої відбувається коригування навігаційних параметрів позиціонування КА.

Процес управління кожною КА FANET здійснюється через МБС, яка має можливість адаптації променю діаграми направленості антени від широкого, на початковому етапі пошуку сусідніх вузлів КА – КА, до вузьконаправленого – при передачі даних вибраному головному вузлу КА відносно МБС.

Під час впливу РЕП можливі чотири типові сценарії:

- нормальне функціонування (номінальний режим);
- зникнення GPS, основний інформаційний канал функціонує – корекція цільових координат позиціонування КА здійснюється за сигналами від МБС по основному каналу;
- зникнення GPS, основний інформаційний канал не функціонує/якість каналу незадовільна – відбувається переналаштування на резервний канал, корекція цільових координат позиціонування КА здійснюється за сигналами від МБС по резервному каналу LoRa;
- втрати основного, резервного каналу управління та сигналу глобальних супутникових систем – виконується процедура аварійного повернення «додому» або посадка.

**Вихідні дані:**

кількість КА, якими здійснює управління одна МБС,  $N_{КА}$ ;

початкова енергія батареї  $E_{КА}$ ;

визначена висота зависання  $h$  КА;

відстань між КА  $d \leq d_{max}$ ;

інтервали відправки службової інформації  $\Delta t$ ;

функція вихідних навігаційних параметрів локальної системи координат КА

$$p_{local}(t) = [lat(t), lon(t), alt(t), v(t), \theta(t), \psi(t), \phi(t)];$$

$lat(t), lon(t), alt(t)$  – широта, довгота та висота в час  $t$ ;

$v(t)$  – швидкість КА;

$\theta(t), \psi(t), \phi(t)$  – кути орієнтації (кут нахилу, курс, крен);

функція прогнозованих навігаційних параметрів КА на МБС;

$$p^*(t + \Delta t) = [lat(t + \Delta t), lon(t + \Delta t), alt(t + \Delta t), v(t + \Delta t), \theta(t + \Delta t), \psi(t + \Delta t), \phi(t + \Delta t)]. \quad (1)$$

**Допущення:** Обмін даними між КА здійснюється за нормальних погодних умов.

Кожна КА оновлює свої координати через GPS у випадку його наявності.

Під час впливу РЕП можливі чотири типові сценарії:

- нормальне функціонування (номінальний режим);
- зникнення GPS, основний інформаційний канал функціонує – корекція цільових

координат позиціонування КА здійснюється за сигналами від МБС по основному каналу;

- зникнення GPS, основний інформаційний канал не функціонує/якість каналу незадовільна – відбувається переналаштування на резервний канал, корекція цільових координат позиціонування КА здійснюється за сигналами від МБС по резервному каналу LoRa;
- втрати основного, резервного каналу управління та сигналу глобальних супутникових систем – виконується процедура аварійного повернення «додому» або посадка.

**Необхідно:**

Забезпечити мінімальне відхилення позиціонування в просторі КА в умовах роботи засобів РЕП противника відносно заздалегідь визначених координат на етапі планування за критерієм мінімального відхилення положення в просторі, шляхом управління параметрами позиціонування.

$$\left| (p_{local}(t) - p^*(t)) \right| \xrightarrow{\Delta} min. \quad (2)$$

Для рішення поставленої задачі для виконання цільової функції пропонується:

- побудувати математичну модель корегування навігаційними параметрами КА в умовах РЕП противника;

- розробити алгоритм управління та взаємодії (обміну даними) між КА та МБС в умовах зникнення глобальних супутникових сигналів;

- застосувати алгоритм Калмана для мінімізації відхилення навігаційних параметрів КА, враховуючи фізико-математичну модель позиціонування КА;

- здійснити оцінку ефективності відхилення отриманих навігаційних параметрів польоту КА відносно еталонних параметрів (з GPS) в умовах впливу РЕП.

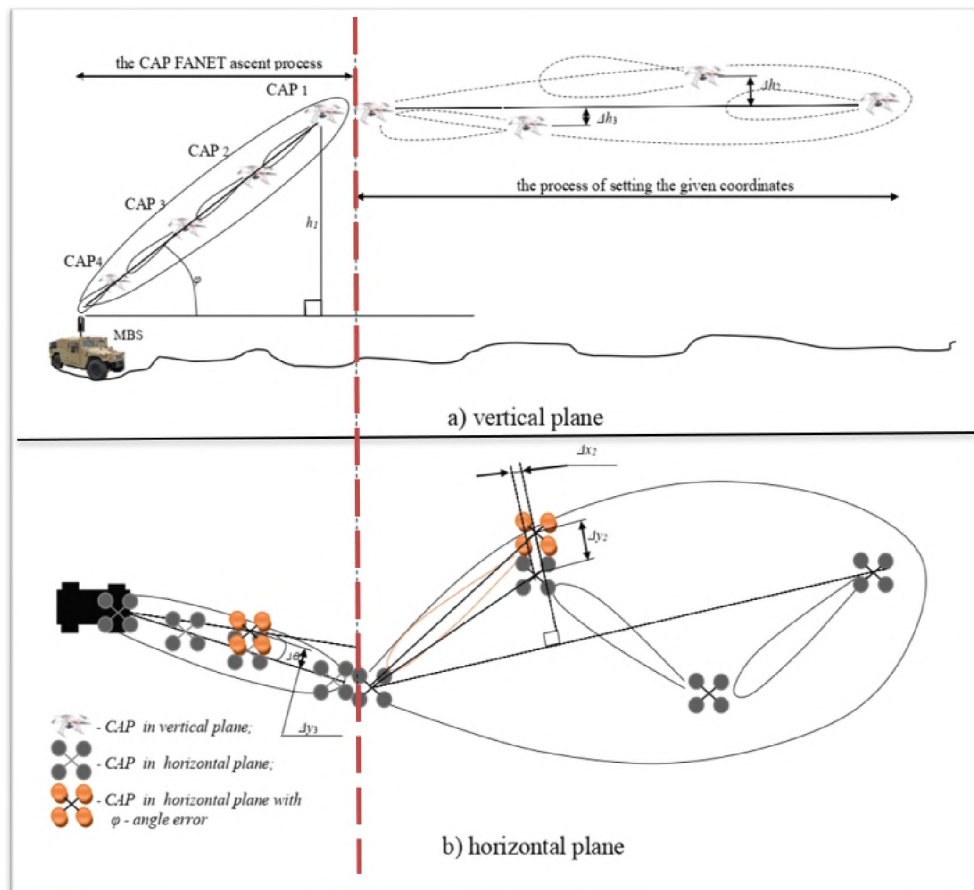
На рисунку 1 показано алгоритм процесу польоту КА від МБС: рисунок 1,  $a$  – у вертикальній площині, рисунок 1,  $b$  – у горизонтальній площині, політ до визначених географічних координат, розрахованих на етапі планування. Процес розльоту КА відбувається послідовно, від КА<sub>1</sub> до КА<sub>4</sub>, далі відбувається набір встановленої висоти зависання  $h$  відносно визначених географічних координат МБС.

Процес розльоту після набору висоти кожним КА (рис. 1,  $a, b$ ) позначено вертикальною пунктирною лінією червоного кольору. На рисунку 1,  $a$  показано  $\Delta h$  – похибку висоти відносно визначених координат, кут  $\varphi$  – елевацийний кут КА відносно МБС, що визначає особливість управління КА, тобто корекцію параметрів навігації на основі розрахунків коефіцієнтів каналної матриці.



На рисунку 1,  $b$   $\Delta y, \Delta x$  – відхилення у горизонтальній площині відносно встановлених географічних координат як результат обчислення похибки показників інерціальної навігаційної системи, тобто визначення власних координат КА відносно МБС.

Далі необхідно розглянути етапи побудови методики управління позиціонуванням КА FANET в умовах впливу РЕП противника.



**Рис. 1.** Процес розгортання FANET підмережі [10]:  
 а – процес розльоту КА(CAP) у вертикальній площині;  
 б – процес розльоту КА(CAP) у горизонтальній площині

Однією із ключових особливостей методики є застосування резервного каналу зв'язку на базі алгоритму LoRa для забезпечення передачі пакетів даних, що включають в себе процес прогнозування і розрахунки параметрів позиціонування КА. Для забезпечення управління позиціонуванням (заданими координатами) застосовується алгоритм фільтрації Калмана.

Обробка навігаційних параметрів вектора стану КА здійснюється на МБС на основі запропонованої методики із канальних матриць для корекції позиціонування КА завдяки використанню властивостей рознесеного прийому сигналів.

*Математична модель корегування навігаційними параметрами КА в умовах РЕП противника.*

Для визначення позиції КА в просторі відносно МБС під час зникнення опорних сигналів глобальної супутникової системи застосовуються матричні операції:  $x_{lMBS} = (x_l, y_l, z_l)$  – вектор положення КА в локальній системі координат, а  $x_{gMBS} = (x_g, y_g, z_g)$  – вектор положення МБС в глобальній системі координат (на основі GPS) [9].

Зв'язок між векторами можна виразити через матрицю обертання, тобто процес повороту **Rot** та вектора зсуву **Div** (3):

$$x_{gMBC} = \mathbf{Rot}x_{IKA} + \mathbf{Div}. \quad (3)$$

Матриця обертання  $\mathbf{Rot}$  складається з трьох ортонормованих стовпців, які представляють напрямки осей локальної системи координат в глобальній системі координат,  $\mathbf{Rot} = [u_x \ u_y \ u_z]$ ; вектор зсуву  $\mathbf{Div}$  дорівнює різниці між початком локальної системи координат і початком глобальної системи координат (4):

$$\mathbf{Div} = (o_{gMBC} - o_{IKA})^2. \quad (4)$$

Для зворотного перетворення з глобальних координат в локальні координати потрібно помножити обидві частини рівняння на  $\mathbf{Rot}^T$  (транспоновану матрицю обертання) і відняти  $\mathbf{Div}$  (5):

$$x_{IKA} = \mathbf{Rot}^T(x_{gMBC} - \mathbf{Div}). \quad (5)$$

Кожне повідомлення на прийомній стороні КА, які обладнані антеною МІМО 2\*2 на БПЛА, приймається і формується канална матриця (6), на МБС із системою 4\*4 – (7).

Під час прийому зондувального сигналу RTS канална матриця  $\mathbf{CH}_{RTS}^{KA1}$  для кожної КА може бути визначена як (6):

$$\mathbf{CH}_{RTS}^{KA1} = \begin{pmatrix} r_{11}^{KA1} & r_{12}^{KA1} \\ \vdots & \vdots \\ r_{41}^{KA1} & r_{42}^{KA1} \end{pmatrix}, \quad (6)$$

де  $r_{ij}^{KA1}$  – каналний коефіцієнт від  $i$ -тої передавальної антени базової станції до  $j$ -тої приймальної антени на КА (КА<sub>1</sub>).

Отримавши сигнал, КА надсилає CTS у відповідь (7):

$$\mathbf{CH}_{CTS}^{MBC} = \begin{pmatrix} r_{11}^{MBC} & \dots & r_{14}^{MBC} \\ r_{21}^{MBC} & \dots & r_{24}^{MBC} \end{pmatrix}. \quad (7)$$

Так, з кожним періодично відправленим зондом RTS буде здійснюватися підлаштування кутів орієнтації (рис. 1) шляхом обробки даних із каналної матриці та синхронізації із кутами Ейлера КА.

Математично елемент каналної матриці  $r_{ij}^a$ , ( $a = \overline{MBC, KA}$ ) можна виразити (8):

$$r_{ij}^a = \alpha_{ij} e^{j(\omega t + \phi_{ij})}, \quad (8)$$

де  $\alpha_{ij}$  – коефіцієнт затухання між  $i$ -тою передавальною антеною та  $j$ -тою приймальною антеною;  $\omega$  – кутова частота сигналу;  $t$  – час;  $\phi_{ij}$  – фазовий зсув між  $i$ -тою передавальною антеною та  $j$ -тою приймальною антеною.

Із рисунка 1 можливо визначити розрахункову координату  $z$ , що відповідатиме фактичній висоті  $h$  підйому КА (9):

$$h = d \cdot \sin(\varphi), \quad (9)$$

де  $d = 10^{\left(\frac{L(d) - L_0 - 20 \log_{10}(f)}{20}\right)}$  – відстань між антеною базової станції та антеною КА в метрах;  $L(d)$  – затухання сигналу в децибелах на відстані;  $L_0$  – константа затухання, залежить від конфігурації антен;  $f$  – частота сигналу в герцах;  $\varphi$  – елеваційний кут на КА (10).

Азимутальний  $\theta$  та елеваційний кут  $\varphi$  можливо визначити із коефіцієнтів каналної матриці (10), (11):

$$\varphi = \arccos\left(\frac{\sum |h_{ii}|}{2\sqrt{\sum |h_{ji}|^2}}\right); \quad (10)$$

$$\theta = \arctan\left(\frac{\sum \Im(h_{ij}h_{ji}^*)}{\sum \Re(h_{ii}h_{jj}^*) - \sum \Re(h_{ij}h_{ji}^*)}\right). \quad (11)$$

На основі (9)–(11) можливо розрахувати фактичні координати  $x$  та  $y$ , що відображено графічно на рисунку 1.

Отже, процес корекції навігаційних даних кожної КА на етапі набору висоти процесу зайняття визначених координат зависання (рис. 1, ліва частина) зі сторони мобільної базової станції відбуватиметься за алгоритмом, представленим нижче. Далі описано алгоритм управління КА з урахуванням впливу РЕП.

*Алгоритм управління позиціонуванням КА FANET складається з наступних шести етапів:*

1. Взліт КА з визначеним часовим інтервалом на визначені координати зависання.
2. Періодична оцінка власного місцезнаходження та корекція координат у випадку наявності сигналів GPS та задовільного рівня сигналу основного каналу КА-МБС.
3. Корекція траєкторії польоту під час набору висоти. МБС відправляє RTS-зонд КА для встановлення зв'язку та прогнозує параметри позиціонування КА з метою корекції навігаційних параметрів, адаптації діаграми направленості в горизонтальній і вертикальній площині, та з урахуванням похибки прогнозу по отриманому CTS-зонду формує коригуючий RTS-зонд на відправку. У випадку, коли МБС не отримує CTS-зонд у відповідь вперше – повторно відправляє зонд RTS, якщо знов збій, то система управління приймає рішення на зміну параметрів передачі та/або вузлової цільової функції, надсилає коригуючий RTS-зонд із урахуванням прийнятого рішення, та здійснюється оновлення даних про стан повітряної мережі для їхнього застосування під час зльоту наступних КА.
4. Призначення голови кластера КА<sub>ГК</sub>. МБС визначає КА, яка досягла висоти  $H_0$  першою; КА займає найближче географічне положення відносно МБС та відправляє АСК-зонд, що свідчить про готовність прийняття управління іншими КА за сигналами від МБС. МБС приймає рішення щодо призначення цієї КА головою кластера, визначає вихідну топологію та знову оновлює вихідні дані.
5. Політ КА на визначені координати та підтримка топології повітряної мережі. Інші КА, які досягли площини розльоту, коли голова кластера вже призначена, прямують на свої визначені координати, відправляючи RTS-зонду КА<sub>ГК</sub> та здійснюючи корекцію вже через голову кластера. На наступних кроках алгоритму МБС і КА<sub>ГК</sub> продовжують взаємодіяти для підтримки топології FANET та реалізують за необхідності зміну мережевих цільових функцій; МБС відправляє RTS-зонди КА<sub>ГК</sub> для встановлення зв'язку і передачі даних. КА<sub>ГК</sub> формує коригуючі RTS-зонди для корекції навігаційних даних КА-сусідів.
6. Ротація КА<sub>ГК</sub>, зліт нових КА та прийняття рішень на згортання. За критерієм максимуму часу функціонування  $T_f \geq T_{fmax}$ , або за командою від МБС здійснюється виконання рішень управління процесами відповідно до сценарію функціонування.

Отже, алгоритм управління параметрами позиціонування КА в FANET забезпечує виконання польотного завдання, що складається з основних етапів: визначення голови кластера, точного розрахунку базового маршруту польоту КА, адаптації ДН, корегування навігаційних даних КА і згортання FANET за потреби.

Реалізація алгоритму управління параметрами позиціонування КА FANET зі сторони КА дзеркально відображає роботу алгоритму на стороні МБС.

*Оцінка ефективності запропонованої методики.*

З метою оцінки ефективності запропонованої методики було проведено експеримент із використанням програмного середовища Python 3.9.1. та пакету бібліотеки pyLora на ПЕОМ.

*Вхідні дані моделювання:*

середня швидкість руху повітряного комунікаційного вузла на КА – 75 км/год;

площина функціонування FANET – 3\*5 км;

кількість КА, якими здійснює управління одна МБС, –  $N_{КА} = 4$ ;

початкова енергія батареї комунікаційного вузла  $E_{ка} = 12\ 800$  мА\*год;

висота зависання  $h$  КА – 700 м;

взаємна відстань між КА  $d$  до 800 м, розподіл вихідних точок зависання визначаються за рівномірним розподілом;

інтервали відправки зондів – до 2 с;

параметри резервного каналу LoRa [1–3]:  $n_{preamble}$  – кількість символів у преамбулі = 8;

$PL$  – розмір корисного навантаження в бітах = (36 байт, тобто 288 біт);  $SF$  – коефіцієнт розширення спектру = 12;  $BW$  – смуга пропускання – 125 кГц;  $CR$  – швидкість кодування 4/8, де перші 4 біти – корисне навантаження, а інші 4 біти – надлишкові біти для ідентифікації повідомлення та синхронізації параметрів діаграми направленості антени;  $P_{noise}$  – вплив РЕП на резервний канал LoRa у діапазоні 433–800 МГц;

параметри фільтра Калмана визначені у [7];

час моделювання процесів управління маршрутом польоту до визначених координат зависання КА  $\approx 20$  хв.

*Результат моделювання:*

$lat(t)$ ,  $lon(t)$ ,  $alt(t)$  – широта, довгота та висота за час моделювання  $t$ .

Оцінку ефективності відхилення отриманих навігаційних параметрів (результат застосування фільтра Калмана) польоту КА відносно еталонних параметрів з GPS в умовах зникнення глобальних супутникових систем та впливу РЕП здійснено за допомогою статистичного критерію середньоквадратичного відхилення.

Завдяки застосуванню методики на основі фільтрації Калмана [7] та порівняно з існуючим рішенням [8] на основі фільтра частинок (PSO) були отримані статистична вибірка значень цільової функції (аргументами якої є навігаційні параметри за широтою, довготою та висотою) та розрахунок середньоквадратичного відхилення RMSE навігаційних параметрів (табл. 1, 2), а графічні результати наведено на рисунках 2, 3.

Із графіків (рис. 2) видно результат відхилення географічних параметрів (широти, довготи та висоти) КА відносно прогнозованих, отриманих за допомогою фільтра Калмана (фрагмент 500 с) відносно еталонних параметрів із GPS-сигналами. Результати, наведені в таблиці 1, показують, що в основному відхилення збільшуються за висотою (в середньому 30 метрів за 500 секунд) відносно заданих координат.

Таблиця 1

Середньоквадратичне відхилення навігаційних параметрів КА

КА	RMSE Latitude	RMSE Longitude	RMSE Altitude
1	0,37317	0,26015	16,67
2	0,301882	0,24906	23,89
3	0,311578	0,57083	24,45
4	0,299579	0,29085	30,56

Використовуючи імітаційне моделювання процесів управління позиціонуванням на основі **фільтра частинок (PSO)** були отримані графіки середнього значення втрати пакетів та дисперсії цього значення для кожної КА, внаслідок відхилення навігаційних параметрів за широтою, довготою та висотою (рис. 3).

На графіках (рис. 3) показано результат прогнозування географічних параметрів (широти, довготи та висоти) КА, отриманих завдяки існуючому рішення на основі фільтра частинок відносно еталонних параметрів із GPS-сигналами.

Результати, зведені до таблиці 2, показують, що максимум відхилення припадає по параметру висоти КА, і складає в середньому 340–400 метрів відносно координат точок зависання, заданих на етапі планування, що є більшим від запропонованої методики на 45 %. Результат моделювання дозволяє стверджувати, що велика розбіжність значень висоти КА корелює з постійним збільшенням частоти корекційних сигналів і, як наслідок, може прискорити розряд батареї.

Таблиця 2

**Середньоквадратичне відхилення навігаційних параметрів КА**

КА	RMSE Latitude	RMSE Longitude	RMSE Altitude
1	0,37317	1,26015	384,21
2	0,301882	1,24906	234,294
3	0,311578	0,57083	240,81
4	1,299579	2,29085	680,45

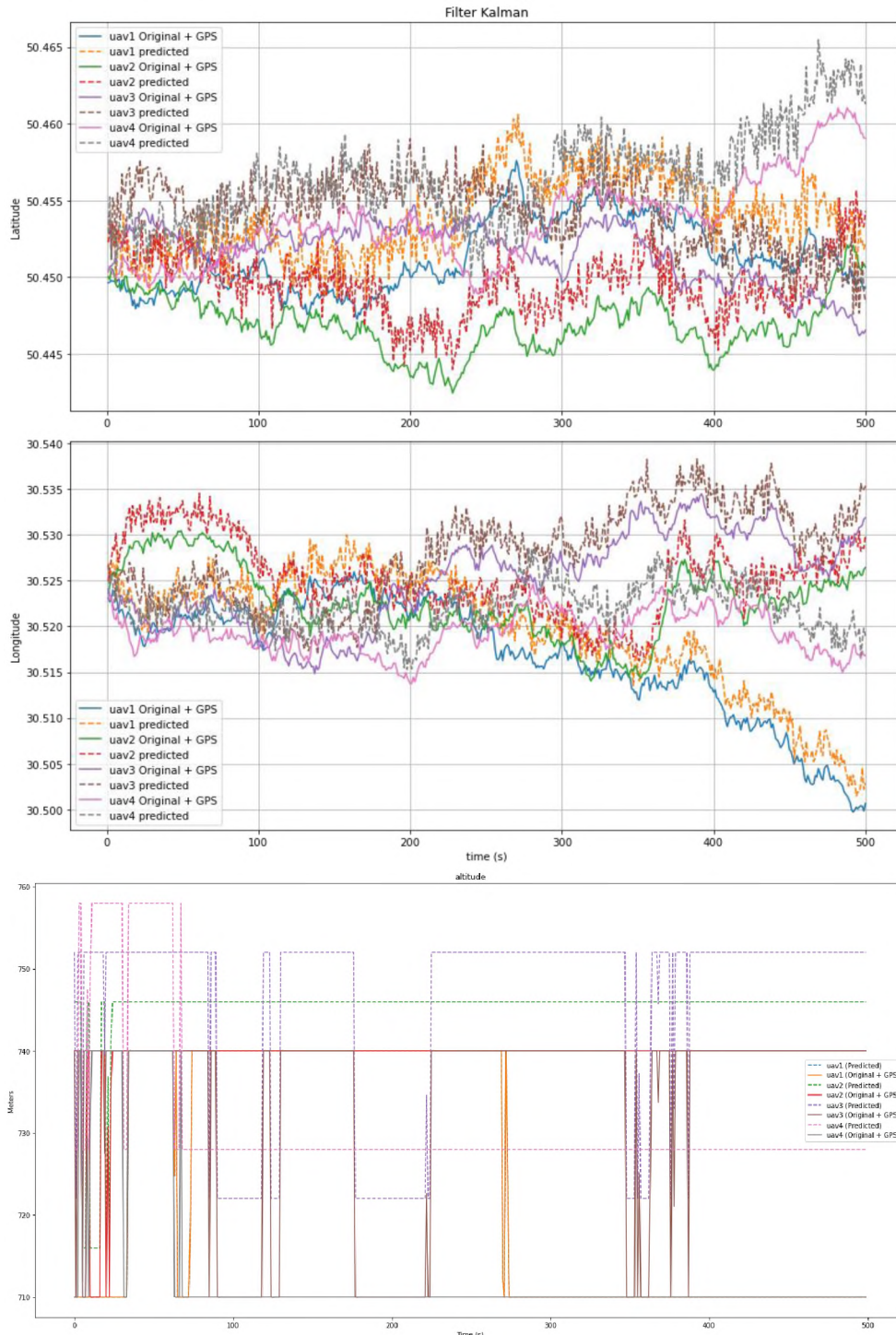


Рис. 2. Графіки результатів адаптивного прогнозування координат на основі фільтра Калмана (траєкторії польоту) відносно еталонної траєкторії з GPS

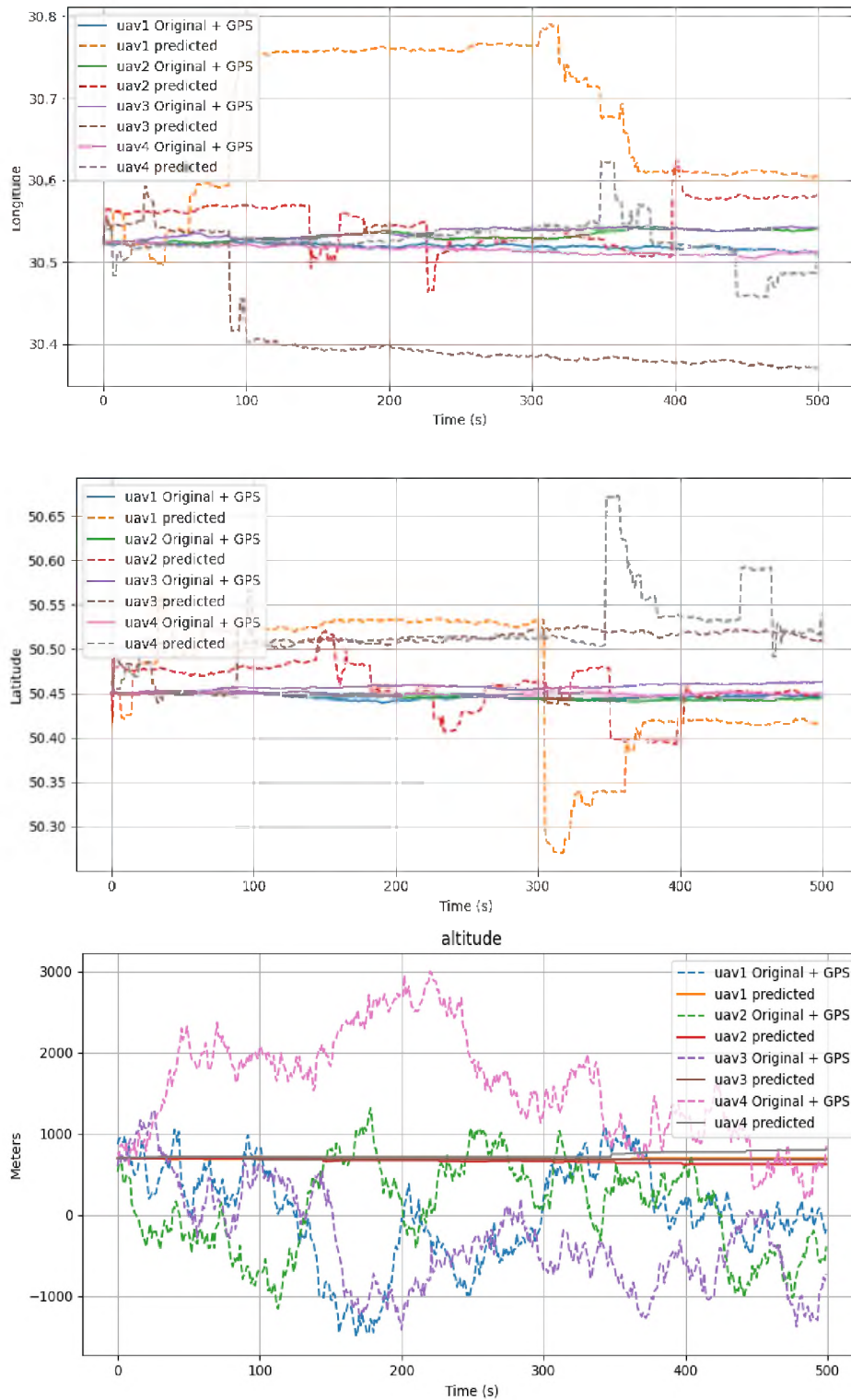


Рис. 3. Графіки результатів адаптивного прогнозування координат на основі фільтра частинок (траєкторії польоту) відносно еталонної траєкторії з GPS

**Висновки.** В роботі показано процес управління параметрами позиціонування КА у процесі розгортання, функціонування та управління процесом ротації головного вузла повітряної комунікаційної мережі. Описано математично та подано у вигляді структурних блок-схем алгоритми взаємодії між КА FANET та МБС в умовах РЕП або тимчасової відсутності сигналів глобальної супутникової системи. Здійснено оцінку кількості втрачених



пакетів у процесі управління та корекції навігаційних параметрів КА з наземного пункту управління – МБС та через голову кластера в процесі функціонування (оперативного управління).

У статті формалізовано процес визначення координат КА за прийнятими сигналами (зондами) по основному каналу передачі, причому враховано характеристики резервного каналу LoRa для збереження управління в умовах втрати GPS-сигналів. Процес адаптивного підлаштування навігаційних параметрів КА в роботі пропонується здійснювати з використанням фільтра Калмана.

Розроблена методика процесу управління позиціонуванням КА може забезпечити прийняття рішення в реальному часі, а результати імітаційного моделювання підтверджують можливість забезпечення меншого відхилення навігаційних параметрів до 30 м відносно відомого рішення із застосуванням алгоритму PSO 340–400 м по висоті.

**Напрямом подальшого дослідження** є застосування нейронних мереж для вироблення керуючих впливів для управління топологією FANET з урахуванням запропонованої в статті методики.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Al-Hajri M. S., Al-Sheikh M. S., Al-Sulaiman S. Analysis of RF interference on LoRa modulation // IEEE Access. 2022.
2. Al-Omari A. A., Al-Abed M. A., Al-Azzawi A. A. Performance of LoRaWAN in the presence of RF interference // International Journal of Electronics and Communications. 2022.
3. Performance Analysis of Long Range Communication for FANETs in Urban Environments, by S. A. Al-Ghamdi, M. A. Al-Hourani, and A. H. Al-Bayatti, published in the IEEE Transactions on Vehicular Technology journal in 2022.
4. A Robust and Efficient Positioning Approach for FANETs in the Presence of Jamming by X. Zhang, Y. Wang, and X. Wang, published in IEEE Transactions on Vehicular Technology. July 2022. Vol. 66. No. 7. P. 6097–6109.
5. Nguyen K. K., Duong T. Q., Do-Duy T., Claussen H., Hanzo L. 3D UAV Trajectory and Data Collection Optimization via Deep Reinforcement Learning // IEEE Transactions on Communications. 2022. DOI: doi.org/10.1109/TCOMM.2022.3148364.
6. Yan Yunfei, Peng Sun, Jieyong Zhang, Yutang Ma, Liang Zhao, Yueyi Qin. Dynamic QoS Prediction Algorithm Based on Kalman Filter Modification // Sensors. 2022. No. 22 (15). P. 5651. DOI: https://doi.org/10.3390/s22155651.
7. Polara Vishal, Jagdish Rathod. Cost Optimization Approach for MANET using Particle Swarm Optimization // International Journal on Recent and Innovation Trends in Computing and Communication. 2023. No. 11 (8). P. 90–98. DOI: https://doi.org/10.17762/ijritcc.v11i8.7927.
8. A Cooperative Positioning Scheme for FANETs in the Presence of Jamming and Uncertainties by Y. Wang, X. Zhang and X. Wang. Published in IEEE Transactions on Vehicular Technology. July 2023. Vol. 72. No. 7. P. 5826–5837.
9. Bieliakov R., Fesenko O. FANET management process simulation at the deployment and operation stage // Technology Audit and Production Reserves. 2023. No. 5 (2 (73)). P. 40–47. DOI: https://doi.org/10.15587/2706-5448.2023.290033.
10. Borkivska Olga, Zhurakovskiy Bohdan, Platonenko Artem. Smart City Information System Based On Lora Technology Annotation // Cybersecurity: Education, Science, Technique. 2022. No. 16 (4). P. 113–28. DOI: https://doi.org/10.28925/2663-4023.2022.16.113128.
11. A 3D MATLAB/Simulink Model of an Unmanned Aerial Vehicle for Control Design and Simulation by A. A. Al-Sheikhly, M. A. Al-Ghamdi and M. A. Al-Shehbaz // IEEE Transactions on Systems.
12. Bieliakov R., Fesenko O. Mobility model of a special purpose terrestrial communication network // Computer-Integrated Technologies: Education, Science, Production. 2023. No. 51. P. 130–138. DOI: https://doi.org/10.36910/6775-2524-0560-2023-51-17.

## МЕТОД ПЛАНУВАННЯ ШЛЯХУ АВТОНОМНОГО НАЗЕМНОГО РОБОТА З ВИКОРИСТАННЯМ МОДИФІКАЦІЇ ДИНАМІЧНОГО ДВОНАПРАВЛЕНОГО RRT-АЛГОРИТМУ

Проблема планування шляху безпілотних автономних наземних засобів завжди була гострою проблемою в галузі досліджень автономних наземних робототехнічних систем. З погляду на складність завдань під час проведення бойових дій в урбанізованому просторі щільної забудови міста з постійною зміною ландшафту, завдання, які покладаються на безпілотні автономні наземні засоби, постійно ускладнюються, а сценарії використання безпілотних автономних наземних засобів демонструють диверсифіковану тенденцію розвитку нових систем прийняття рішень безпілотних автономних наземних засобів. Швидкоплинність ведення сучасних бойових дій в урбанізованому просторі постає як складне і багатопланове завдання. Враховуючи складність процесу руху безпілотних автономних наземних засобів, на сучасному етапі розвитку робототехнічних систем, загальною тенденцією є відмова від дистанційного керування роботизованими комплексами з переходом до автоматичних режимів, що вимагає розробки, впровадження алгоритмів автоматичної взаємодії та руху військових мобільних робототехнічних систем. Задля вирішення проблеми пришивидження отримання рішень пошуку шляхів без зіткнень у режимі реального часу у двовимірному просторі пропонується застосувати модифікований динамічний двонаправлений алгоритм «швидке дослідження випадкового дерева із зірочкою» з реперними вузлами. Запропонований алгоритм є модифікацією алгоритму «швидке дослідження випадкового дерева із зірочкою» з реперними вузлами, з використанням методу двонаправленого жадібного пошуку для прискорення та вирішення проблеми односпрямованого алгоритму «швидке дослідження випадкового дерева» щодо його повільної швидкості пошуку, а також труднощів прийняття рішення у вузькому середовищі, викликаних сліпою випадковою вибіркою. В разі динамічного переміщення перешкоди така модифікація завдяки перевазі, що реперні вузли не потребують багато обчислень під час планування, у процесі ітераційної оптимізації шляху виконує оновлення інформації карти в режимі реального часу та відновлює пошкоджений вихідний шлях для завершення динамічного планування шляху.

**Ключові слова:** автономний наземний робот, вибіркового алгоритм, швидке дослідження випадкового дерева, планування шляху в реальному часі, двонаправлений жадібний пошук, відновлення шляху.

### ***A. Bernatskyi Method for planning the way of UGV using a modification of dynamic bi-directional RRT algorithm.***

The path planning problem of unmanned autonomous ground vehicles has always been an acute problem in the field of autonomous ground robotic systems research. From the point of view of the complexity of the tasks during the conduct of combat operations in the urbanized space of the densely built-up city with a constantly changing landscape, the tasks entrusted to the UGV are constantly becoming more difficult, and the scenarios of the use of the UGV demonstrate a diversified trend in the development of new management and control systems. The rapidity of conducting modern military operations in an urbanized space appears as a complex and multifaceted task. Considering the complexity of the UGV movement process, at the current stage of the development of robotic systems, the general trend is to abandon remote control of robotic complexes with the transition to automatic modes, which requires the development and implementation of algorithms for automatic interaction and movement of military mobile robotic systems. To solve the problems of the Rapidly-Exploring Random Tree \*Fixed Nodes algorithm regarding its low speed for obtaining track junctions and the impossibility of using it in a dynamic environment when planning a UGV path. To solve the problem of accelerating the acquisition of collision-free paths in real time in two-dimensional space, it is proposed to apply a modified dynamic bidirectional RRT\* algorithm with reference nodes. The algorithm is a modification of Rapidly-Exploring Random Tree \*Fixed Nodes using a bidirectional greedy search method to speed up and solve the problem of the unidirectional Rapidly-Exploring Random Tree algorithm regarding its slow search speed, as well as the difficulties of decision making in a narrow environment caused by blind random sampling. In the case of dynamic disturbance movement, taking advantage that reference nodes do not require much calculation in planning, in the process of iterative path optimization, the proposed algorithm updates the map information in real time and repairs the damaged output path to complete the dynamic path planning.

**Keywords:** UGV, Rapidly-Exploring Random Tree, selective algorithm, way real-time planning, bi-directional greedy search, way recovery.



### **Постановка завдання**

Планування шляху безпілотних автономних наземних засобів (далі – БАНЗ) завжди було гострою проблемою в галузі досліджень автономних наземних робототехнічних систем [1]. З погляду на складність завдань під час проведення бойових дій в урбанізованому просторі щільної забудови міста з постійною зміною ландшафту, завдання, які покладаються на БАНЗ, постійно ускладнюються, а сценарії використання БАНЗ демонструють диверсифіковану тенденцію розвитку [2], що вимагає розробки військових мобільних робототехнічних систем із системами прийняття рішень, здатними на самостійне (автономне) вирішення проблем пошуку шляху.

Використання математичного апарату алгоритмів планування шляху надає якісний ефект керування системою прийняття рішень БАНЗ. [3]. Проблематика побудови БАНЗ військового призначення передбачає пошук шляху без зіткнень, який з'єднує відомі початкову та цільову точку положення робота у просторовій системі, що складається з одного або групи складних геометричних тіл, задовольняючи при цьому обмеження, накладені складними перешкодами.

Тому актуальною науковою задачею є розробка ефективних алгоритмів пошуку маршруту переміщення робота без зіткнень в умовах динамічно змінних перешкод та обмеженого проходу.

### **Аналіз останніх публікацій**

Відомо багато прикладів досліджень проблематики планування шляху роботів.

Відповідно до тенденції розвитку алгоритмів планування шляху їх можна розділити на два основні класи: алгоритми на основі графів та алгоритми на основі вибірки.

Найбільш відомі серед алгоритмів планування шляху на основі графів містять алгоритм  $A^*$ , алгоритм Дейкстри, Флойда-Воршелл, Пріма та інші [4]. Традиційні алгоритми планування шляху не мають можливостей коригування шляху в умовах динамічного змінного середовища. Для того, щоб алгоритм пошуку шляху відповідав цілям планування реалізації БАНЗ, Йоав Фройнд и Роберт Шапире [5] одні з перших запропонували динамічний алгоритм  $A^*$ , якій можна застосовувати в динамічному середовищі у реальному часі. Пізніше Аїе Маув [6] розробив оптимізований варіант динамічного алгоритму  $iADA^*-RL$ . Кадрі та інші [7] представили модифіковану допоміжну функцію керування та посібник з оптимізації функції оцінювання  $D^*$ .

Завдяки використанню оптимальної роздільної здатності мапи та цілісності картини поля мапи [8], алгоритм пошуку шляху на графах може знайти оптимальне рішення пошуку шляху за відносно малий час. Але такі алгоритми вимагають растрового моделювання карти, що впливає на ступень універсальності і вимагає використання додаткових обчислювальних ресурсів для конвертації. Алгоритми пошуку за графами використовуються в растровому просторі, щоб зменшити загальну кількість станів, а потім визначити мінімальний шлях, складений з набору вузлів без колізій [9]. Враховуючи вище сказане, зауважимо, що *алгоритми планування шляху на основі графа* не підходять для ситуацій, які вимагають планування в реальному часі.

Сучасні методи планування шляху робота на основі вибірки переважно містять такі алгоритми, як ймовірнісні дорожні карти (RPM), алгоритм швидкого дослідження випадкового дерева (Rapidly exploring Random Tree, RRT) [10] та інші. Ці алгоритми засновано на інкрементній випадковій вибірці ефективного планування можливих шляхів. Алгоритм планування шляху, заснований на випадковій вибірці, уникає моделювання простору та швидко отримує шляхи. Він підходить для випадків, коли потрібна продуктивність у реальному часі. Однак спосіб генерації точок вибірки є випадковим. Шлях, отриманий RRT, зазвичай не є оптимальним, тому потрібна процедура оптимізації шляху. Такі алгоритми, як RRT і RRT\*, запроваджують методи повторного вибору батьківського вузла, повторного

підключення вузла та асимптотично збільшують цільовий шлях завдяки збільшенню точок вибірки. У випадку коли точки вибірки прагнуть до нескінченності, завдяки оптимізації, може бути отриманий оптимальний шлях [11].

Однак процес додавання точок вибірки для отримання асимптотично оптимального шляху є відносно довгим. Для покращення швидкості збіжності рішення шляху відомо про покращені версії цього алгоритму. Гаммелл та ін. [12] запропонували алгоритм informedRRT\*, якій змінює вибір простору вибірки і обмежує глобальну випадкову вибірку еліптичним простором. Тагері та інші [13] запропонували алгоритм пошуку, заснований на нечіткому жадібному RRT (FG-RRT), який генерує вагу вузлів-нащадків шляхом оцінки зміни якості. Адіятов та ін. [14] запропонували алгоритм пошуку Quick-RRT\* на основі подвійного дерева. Алгоритм планування шляху вирощує два дерева по черзі від початкової та кінцевої точки для покращення швидкості конвергенції. Оскільки кількість вузлів збільшується під час виконання процесу оптимального алгоритму RRT, обчислювальна складність і час роботи зростатимуть експоненціально до зростання. Щоб вирішити цю проблему, Spanogianopoulos та інші [15] запропонували алгоритм RRT\*FN (RRT фіксовані вузли), який може зменшити надлишкові кінцеві вузли на шляху та покращити швидкість планування. Але такий алгоритм можливо використовувати тільки в умовах статичних середовищ, що також унеможливорює повною мірою використання для системи прийняття рішень БАНЗ.

Отже, існуючі рішення (алгоритми) мають певні недоліки, такі як ресурсовимогливість, час виконання завдання або неефективна побудова довжини шляху при виконанні місії в умовах динамічних середовищ.

**Метою статті** є розробка алгоритму, який можна застосовувати в динамічних середовищах, завдяки використанню двонаправленого жадібного пошуку для покращення часу планування алгоритму, довжини рішення шляху, швидкості конвергенції, форми шляху, задля задоволення вимог планування шляху в реальному часі, дозволяючи БАНЗ швидко отримати оптимальний шлях без зіткнень у динамічних середовищах у режимі реального часу.

Окремим питанням є перевірка енергоефективності запропонованого метода.

#### **Виклад основного матеріалу**

##### **1. Теоретична складова модифікації алгоритму RRT\*FN.**

Подібно до методу модифікації алгоритму RRT, визначеного в літературі [16–18], простір станів  $X \subseteq R^n$  у задачі планування шляху визначається за допомогою сенсорів БАНЗ. Інформація про перешкоди, що міститься на цифровій карті, отримується за допомогою лазерного скануючого пристрою відстані (ЛІДАР) та формується як простір перешкод  $X_{obs} \subsetneq X$ , а доповнення простору перешкод до простору станів визначається як вільний простір  $X_f$ , де  $X_f = X_{obs}^c \cap X$ , тобто це простір, в якому робот може вільно рухатися.

Припустимо, що початковою точкою БАНЗ у просторі станів є  $p_{start} \in X_f$ , а рухомою цільовою точкою є  $p_{end} \in X_f$ . Набір точок шляху визначаємо як  $\sigma: [0; 1] \subset \mathbb{R} \rightarrow X_f$ . Тоді правило шляху перетворюється на розв'язання множини точок  $\sigma[0; 1]$  у вільному просторі  $X_f$ . Якщо зв'язок між точкою  $p \in \sigma[0; 1]$  і точкою  $p$  не перетинається з множиною точок  $\sigma[0; 1]$ , то визначаємо функцію вартості шляху  $c(\sigma)$ , що дорівнює лінії евклідової відстані, яка з'єднує набір точок рішення шляху  $\sigma$  (1).

$$c(\sigma) = \sum_{i=1}^n \left\| \sigma\left(\frac{i}{n}\right) - \sigma\left(\frac{i-1}{n}\right) \right\|, \quad (1)$$

де  $n$  – кількість елементів у множині  $\sigma$ , а можливий шлях  $\sigma$  у просторі не є єдиним. Визначимо  $\Sigma$  як множину всіх можливих  $\sigma$ , а  $C: \Sigma \rightarrow R_{\geq 0}$  – множина всіх шляхів.

Для задачі рішення оптимального шляху, вартість шляху використовується як оціночний індекс для оцінки рішень шляху. Чим нижча вартість шляху тим кращий шлях, тоді задача розв'язання оптимального шляху перетворюється на розв'язання  $\sigma^*$ , яке мінімізує вартість шляху у вільному просторі  $X_f$ . Тобто ми маємо (2):

$$\sigma^* = \operatorname{argmin} \{c(\sigma) \mid \sigma(0) = p_{start}, \sigma(1) = p_{end}, \forall s \in [0,1], \sigma(s) \in X_f\}. \quad (2)$$

Для ситуації динамічного рішення, коли положення БАНЗ і перешкоди змінюються,  $p_{start}$  і  $p_{end}$  можуть бути не унікальними, тому набір початкових точок і цільових точок шляху визначається як  $P_{end}, \sigma(0) \in P_{start}, \sigma(1) \in p_{end}$ . Тоді визначення (2) отримує наступний вигляд (3):

$$\sigma^* = \operatorname{argmin} \{c(\sigma) \mid \sigma(0) = P_{start}, \sigma(1) = P_{end}, \forall s \in [0,1], \sigma(s) \in X_f\}. \quad (3)$$

Алгоритм RRT є найбільш типовим алгоритмом планування шляху на основі вибірки. Цей алгоритм може випадково генерувати точки вибірки з простору, використовувати початкову точку як кореневий вузол і з'єднувати лінії від найближчих вузлів вибірки без зіткнень. Напрямок зростає відповідно до заданого розміру кроку досягнення мети розширення дерева. Як тільки станеться зіткнення між з'єднаннями листового вузла та цільової точки, планування шляху буде завершено.

Основні кроки алгоритму:

*Крок 1:* Дано простір карти  $M$ , де  $p_{start}$  – початкова точка, а завдання цільової точки очікуються.

*Крок 2:* Отримаємо  $p_{rand}$  шляхом випадкової вибірки в просторі.

*Крок 3:* Починаємо зростати із найближчої точки перетину вузла та зростаєте до  $p_{rand}$  із розміром кроку  $s$ . Новостворену точку визначаємо як  $p_{new}$ .

*Крок 4:* Існує певна ймовірність того, що точка вибірки не буде рости вздовж випадкової точки вибірки  $p_{rand}$ , а вибере зростання безпосередньо до кінцевої точки  $p_{end}$ .

*Крок 5:* Якщо дерево росте до  $p_{end}$  або лінія, що з'єднує  $p_{new}$  та  $p_{end}$ , не перетинає перешкоди, генерується можливий шлях  $\sigma$ .

Незважаючи на те, що алгоритм RRT має імовірнісну повноту і може швидко отримувати можливі рішення в просторі, його процес пошуку рішень є випадковим, тобто *слітим*. Це, зокрема, відображається в тому факті, що  $p_{rand}$  отримується шляхом випадкової вибірки, роблячи напрямок росту дерева випадковим. До того ж в алгоритмі не вистачає розширення пам'яті вузла, що призводить до надмірності.

Алгоритм RRT\* є оптимізованим алгоритмом RRT. Завдяки якому асимптотично оптимальний шлях можна отримати завдяки отриманню достатньої кількості точок вибірки під час ітерації оновлення. Алгоритм додає дві операції: *повторний вибір батьківського вузла та повторне підключення вузла*.

*Повторний вибір батьківського вузла:* з  $p_{new}$  як центром і потенційними батьківськими вузлами в області з радіусом  $R$ , обчислюється вартість шляху цих вузлів. Вибираємо вузол з найменшою вартістю шляху як новий батьківський вузол і проводимо поєднання. Якщо на шляху є колізія, вибираємо інший альтернативний батьківський вузол.

*Повторне підключення вузла:* використовуючи  $p_{new}$  як центр, вибираємо діапазон із радіусом  $R$  і пробуємо змінити батьківський вузол вузла в межах діапазону на  $p_{new}$ . Якщо це може зменшити загальну вартість шляху, від'єднаємо вузол від його батьківського вузла та підключаємо до  $p_{new}$ . Якщо в з'єднанні виникне колізія, з'єднання буде розірвано, а інші вузли в межах діапазону продовжуватимуть вибиратися та послідовно перевірятися.

Якщо випадкова точка вибірки  $p_n$  береться на оптимальному шляху  $\sigma^*$  від  $p_{start}$  до  $p_{end}$  у просторі, вартість шляху буде зменшена, оскільки  $p_n$  стає батьківським вузлом свого сусіднього вузла. Після достатньої вибірки завжди отримаємо (4):

$$\begin{cases} L\{p_1, p_2, \dots, p_n\} = L^*, \\ \forall p \in L, p_{rand}(x) = p, x \in (0, iter). \end{cases} \quad (4)$$

де  $iter$  – кількість ітерацій. Асимптотична оптимальність алгоритму доведена. Оскільки алгоритм розширює масштаб пошуку, операції повторного вибору батьківського вузла та повторного підключення вузла перетинають усі точки в дереві, що призводить до величезного навантаження на пам'ять.

Алгоритм  $RRT^*FN$  є модифікацією алгоритму задля підвищення ефективності пошуку шляхом фіксації кількості вузлів.

Алгоритм  $RRT^*FN$  (фіксовані вузли  $RRT^*$ ) вводить концепцію максимальної кількості вузлів на основі алгоритму  $RRT^*$ . Цей алгоритм встановлює максимальну кількість вузлів, дозволена в дереві. Коли кількість вузлів у просторі станів більше попередньо встановленої кількості вузлів, довільно видаляється бездітний листовий вузол, за винятком кінцевого вузла.

Алгоритм  $RRT^*FN$  містить такі кроки:

*Крок 1:* Те саме, що крок 1–3 алгоритму  $RRT$ .

*Крок 2:* Виконується повторний вибір батьківського вузла та повторне підключення вузла.

*Крок 3:* Кожного разу, коли генерується  $p_{new}$ , перевіряємо кількість вузлів у просторі. Якщо кількість вузлів перевищує максимальну  $Nodes_{FIX}$ , довільно видаляються бездітні листові вузли останнього вузла, що не є шляхом ( $p_{delete} \in p_{leaf} \text{ except } p_{new}$ ).

*Крок 4:* Коли дерево розростається до рівня  $p_{end}$  або лінія, що з'єднує  $p_{new}$  і  $p_{end}$ , не перетинається з перешкодою, генерується можливий шлях  $\sigma$ .

*Крок 5:* Повторяємо кроки 1–3 задля виконання асимптотичної оптимізації рішення шляху.

Пропонується удосконалений алгоритм, що поєднує стратегію двонаправленого жадібного пошуку з алгоритмом  $RRT^*FN$  для вирішення проблеми сліпоти в односторонньому зростанні дерева. Алгоритм  $RRT^*FN$  у швидкості пошуку не має переваги над алгоритмом  $RRT^*$  та може лише зменшити надлишкову вибірку точок, яких слід уникати. Надлишкове зростання має ефект обмеження розміру дерева для покращення швидкості роботи програми, коли кількість ітерацій є великою та великий розмір дерева. Після додавання стратегії двостороннього жадібного пошуку, шлях запланований алгоритмом, має більш очевидну спрямованість, а початковий шлях можна отримати відносно швидко.

Жадібний двосторонній пошук вимагає встановлення двох випадкових дерев пошуку, дерева 1 і дерева 2, у початковій і цільовій точках одночасно. Два дерева ростуть назустріч одне одному відповідно, і під час зростання використовується жадібна стратегія.

1) Встановлено, що початкова точка  $p_{start}$  і  $p_{end}$  двох дерев є кінцевими точками один одного.

2) Після того, як Дерево 1 генерує новий вузол  $p_{new}$ , він продовжує рости від  $p_{new}$  до вузла, найближчого до себе від Дерева 2 (щоб гарантувати мінімізацію вартості шляху), доки не зіткнеться з іншим або не досягне цілі.

3) Якщо після зростання кількість послідовних вузлів Дерева 1 перевищує кількість вузлів іншого дерева, тоді задача зростання переходить до Дерева 2.

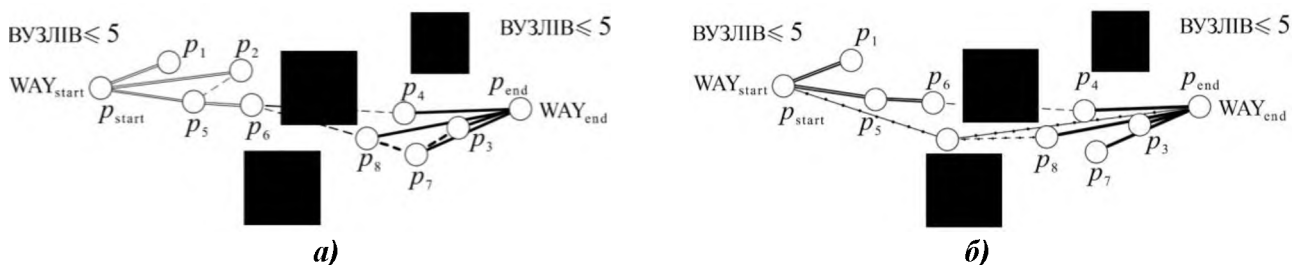


Рис. 1. Схематична діаграма двостороннього жадібного пошуку:  
а – процес зростання; б – остаточний шлях

Використання стратегії двостороннього жадібного пошуку з алгоритмом  $RRT^*FN$  для покращення одностороннього випадкового зростання до цільового вузла дерева є

виправленням недоліка низької продуктивності. Загальний принцип роботи покращеного алгоритму показаний на рисунку 1.

Із початкової точки  $p_{start}$  і цільової точки  $p_{end}$  будуємо два дерева і жадібно розвиваємо одне до одного. Подвійна лінія є деревом початкової точки, а товста лінія – це кінцеве дерево. Чорні квадрати – перешкоди на шляху. Вузли в просторі генеруються в порядку з нижніми індексами. Якщо вказано кількість вузлів у кожному дереві не більше 5, коли  $WAY_{start} \cap WAY_{end} \neq 0$ , означає, що два дерева з'єдналися.

Як видно з рисунка 1, алгоритм BD-RRT\*FT, який додає двонаправлену стратегію жадібного пошуку, має більш очевидну спрямованість, ніж алгоритм RRT\*FN, рішення шляху також має тенденцію бути оптимальним зі збільшенням процесу ітерації.

Складність фактичного робочого середовища БАНЗ полягає в тому, що початковий запланований шлях може бути пошкоджено під час роботи БАНЗ. Наприклад, під час бойових дій перешкода була зсунута, або з одиничного блока перешкода під впливом вибухової хвилі змінила свій розмір чи перетворилася на групу перешкод в просторі на карті, які не були заздалегідь внесені до списку перешкод.

Одночасно, коли алгоритм динамічного програмування оновлює інформацію про навколишнє середовище, точки відбору проб поступово збільшуватимуться з часом. Чим більший розмір дерева, тим більше навантаження на динамічний алгоритм при оновленні в реальному часі, що сповільнить швидкість роботи

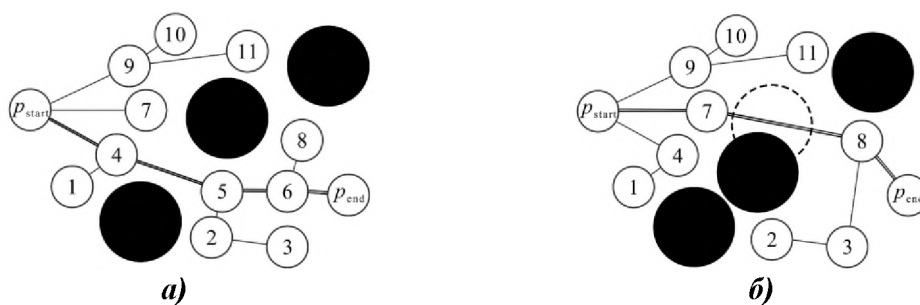
Щоб вирішити вищевказані проблеми алгоритму RRT\*FN, впровадимо модифікації алгоритму застосувавши принцип динамічного оновлення та відновлення шляху. А саме під час кожної ітерації алгоритм оновлюватиме інформацію про середовище та виконуватиме оновлення планування на основі вихідних вузлів. Крім того, також проведемо оновлення інформації про розташування БАНЗ. Щоб зменшити розмір дерева під час процесу планування, зазначимо як непотрібні вузли і допоміжні гілки, через які проходить БАНЗ, використовуючи поточне розташування БАНЗ як новий кореневий вузол. Якщо запланований шлях знищено перешкодами, алгоритм відкине вузли на дереві, покриті перешкодами, і використає простір для перебудови дерева з повними вузлами і ефективного відновлення шляху, як показано на рисунку 2.

Етапи відновлення (перебудови) шляху є такими.

*Крок 1:* Коли шлях зруйновано перешкодою, від'єднаймо зруйнований вузол від інших вузлів, запишіть номер вузла та відкиньте ці вузли.

*Крок 2:* Виберіть відкинутий вузол, найдавший від кореневого вузла, з його дочірнім вузлом як центром кола, і повторно знайдіть потенційні батьківські вузли для нього в межах області з радіусом  $R$ . Потенційний батьківський вузол із найменшою вартістю шляху є новим батьківським вузлом. Виконайте повторне підключення вузла.

*Крок 3:* Продовжуйте використовувати інші дочірні вузли найдавший округленого вузла та повторюйте крок 2, доки всі відкинуті вузли, крім кореневого вузла, не знайдуть свої батьківські вузли. Відновлення шляху завершено.



**Рис. 2.** Схематична діаграма відновлення шляху:  
а – до переміщення перешкоди; б – після переміщення перешкоди

*Аналіз повноти алгоритму та вибір фіксованої кількості вузлів*

Перевіримо та доведемо імовірнісну повноту та асимптотичну оптимальність алгоритму RRT\*.

Припустимо, що простір станів  $X \subseteq R_n$ , множина з 2 дерев пошуку  $T_1, T_2 \subseteq X$  становить (5):

$$\begin{cases} \forall p \in \sigma, p_{rand}(x) = p, x \in (0, iter1), \\ \forall q \in \sigma, q_{rand}(x) = q, x \in (0, iter2) \\ \sigma \subseteq T_1 \cup T_2, p_{rand} \subseteq T_1, q_{rand} \subseteq T_2. \end{cases} \quad (5)$$

Тобто RRT\* алгоритм двонаправленого жадібного пошуку все ще має ймовірнісну повноту. Після знаходження рішення шляху  $\sigma$  два дерева об'єднуються, а асимптотична оптимальність подвійного деревного алгоритму така сама, як і у одnodеревного RRT\* алгоритму. Модифікований алгоритм передбачає максимальну кількість вузлів, якщо кількість фіксованих вузлів  $n \rightarrow \infty$ , імовірнісна повнота та асимптотична оптимальність вдосконаленого алгоритму узгоджуються з алгоритмом RRT\*. Якщо кількість фіксованих вузлів  $n$  більше числа вузлів у розв'язку шляху  $m$ , то алгоритм не має імовірнісної повноти та асимптотичної оптимальності. Розглянемо  $m \leq n$ , коли максимальна кількість вузлів  $n = m$  і рішення шляху  $\sigma$  все ще не знайдено. Алгоритм буде відкидати випадкові бездітні листові вузли й продовжувати вибірку та планування, а повторний вибір батьківського вузла та повторне підключення вузла є еквівалентними розподілу випадкових точок  $p_{rand}$ , які залишаються у всьому просторі станів. Після достатньої кількості ітерацій маємо (6):

$$\forall p \in \sigma, p_{rand}(x) = p, x \in (0, iter). \quad (6)$$

Якщо шлях існує, кінцевий шлях  $L$  має бути перестановкою та комбінацією елементів у наборі  $\sigma$ , тобто повнота ймовірності задовольняється. Так само, через повторний вибір вузла та повторне підключення батьківського вузла, якщо  $p \in \sigma$ ,  $p_{rand}(x) = p$ , і цю точку остаточно вибрати як об'єкт повторного з'єднання вузла, вартість шляху однозначно зменшиться. Коли кількість ітерацій достатньо велика, все ще буде вірно (7):

$$\begin{cases} L\{p_1, p_2, \dots, p_n\} = \sigma^*, \\ \forall p \in \sigma^*, p_{rand}(x) = p, x \in (0, iter). \end{cases} \quad (7)$$

Тобто покращений алгоритм має імовірнісну повноту та асимптотичну оптимальність. Хоча алгоритм має ймовірнісну повноту, у діапазоні  $m \leq n < 1$ , якщо кількість реперних вузлів встановлена надто малою, ймовірність отримання шляхового рішення майже дорівнює 0. Але якщо значення реперного вузла встановлено занадто великим, воно займатиме забагато місця в пам'яті. Зазвичай кількість реперних вузлів вибирається на основі емпіричних методів. Але для уникнення людського фактору, модифікований алгоритм автоматично перевіряє кілька груп за умови фіксованого простору, станів і розміру кроку.

Послідовність вибору кількості реперних вузлів:

- Отримаємо дані про середній час оптимального рішення.
- Виконаємо апроксимацію кривої 7 разів.
- Вибираємо кількість фіксованих вузлів у мінімальній точці підгонки інтервалу кривої як кількість фіксованих вузлів для експерименту.

Через випадковість точок вибірки, вибраних алгоритмом RRT, метод вибору фіксованої кількості вузлів може бути не оптимальним, але цей метод відбору є відносно розумним і дозволяє уникнути впливу неправильного вибору фіксованої кількості вузлів для експерименту.

*Реалізація алгоритму BD-RRT\*FT* полягає в наступному:

*Крок 1:* Ініціалізуємо карту, дерева пошуку (Дерево 1 та Дерево 2). Додаємо  $p_{start}$  до списку вузлів Дерево 1 і  $p_{end}$  до списку вузлів Дерево 2.

*Крок 2:* Використовуємо менше дерево з двох дерев як ціль зростання (якщо кількість вузлів у дереві однакова, вибираємо Дерево 1), випадковим чином вибираємо точку відбору

проб  $p_{rand}$  у просторі. Вибираємо найближчий вузол  $p_{nearest}$ , і починаємо рухатися до  $p_{rand}$ , зростаючи з певним кроком, і отримуємо  $p_{new}$ .

*Крок 3:* Виконуємо повторний вибір батьківського вузла та повторне підключення вузла.

*Крок 4:* З  $p_{new}$  як з батьківського вузла, продовжуємо рости до вузла  $p'_{nearest}$  дерева, доки він не досягне цієї точки або не зустрине перешкоду.

*Крок 5:* Після виконання процесу зростання оновлюємо карту. Встановлюємо вузол, де розташований БАНЗ як кореневий вузол. Видаляємо вузол та його гілки в останньому місці розташування БАНЗ, якщо  $P \cap X_{obs} \neq \emptyset, P \in \sigma$ , видалить вузли, що покриті перешкодами, а також вузли, лінії яких перетинаються з перешкодами. Від'єднайте ці точки від оточуючих вузлів і виконайте крок 3.

*Крок 6:* Порівняйте кількість вузлів у списках Дерево 1 і Дерево 2, виберіть менший з них як об'єкт зростання та виконайте кроки 2–5.

*Крок 7:* Якщо два дерева з'єдналися під час процесу зростання (відстань між двома вузлами в Дереві 1 і Дереві 2 менша за встановлене значення  $connectDis$ ), визначте вузли на з'єднанні Деревя 1 і Деревя 2 як  $p_{contree1}$  і  $p_{contree2}$  та використовуйте  $p_{contree1}$  як кореневий вузол. Обміняйтеся зв'язками «батько-нащадок» вузлів у Дереві 2 і використовуйте  $p_{contree1}$  як батьківський вузол  $p_{contree2}$  для об'єднання двох дерев у дерево злиття.

*Крок 8:* використовуючи  $p_{start}$  як початкову точку та  $p_{end}$  як цільову точку, виберіть найкоротший шлях у дереві злиття як рішення шляху.

*Крок 9:* виконайте асимптотичну оптимізацію шляху відповідно до кроків 1–3 алгоритму RRT\*FN. Після завершення кожного зростання/повторного підключення виконайте крок 5.

## 2. Експериментальна перевірка алгоритму.

Імітаційне моделювання було здійсненом завдяки розробленій програмі моделювання, з використанням мови програмування Python 3+ та бібліотек PyGame, NumPy. В якості системи обчислювання використовувалась система 2-х сокетона Workstation із системними параметрами Intel® Xeon® Processor E5-2689 v4 (25M Cache, 3.10 GHz) = 2/ 4\*64 Gb DDR4 2133/ SSD 250Gb/ VA Asus e GForce GTX 1650 GDDR6 4096Mb.

Для перевірити ефективності запропонованого алгоритму було проведено порівняння алгоритму BD-RRT\*FT з іншими алгоритмами за трьома картами з оцінюванням показників продуктивності. Щоб полегшити аналіз симуляції та врахувати раціональність, перешкоди на мапах, що використані як блоки піксельної графіки, БАНЗ розглядається як точка піксельного розміру 4x4, а інші нерелевантні змінні, окрім алгоритму, контролюються, щоб бути узгодженими. Оскільки алгоритм RRT базується на випадковій вибірці, у процесі моделювання є непередбачуваність, і кожен результат вимірювання може мати відмінності, щоб усунути вплив випадковості, під час експерименту проводилось 100 незалежних експериментів для кожної ситуації та формувалися результати для порівняльного аналізу.

*Перевірка роботи алгоритмів на карті 1 (карта зі статичними перешкодами).*

Використовуємо карту 1, розміром 800 px × 600 px, як звичайну карту перешкод (рис. 3, а), яка використовується для перевірки швидкості реакції та індексу шляху алгоритму в нормальному середовищі перешкод. На цій карті верхній лівий кут встановлюється як початок координат [0, 0], а карта розташована в 4-му квадранті, початкова та кінцева позиція БАНЗ [20, 580], [780, 20] позначена значками БАНЗ та надписами START, END відповідно.

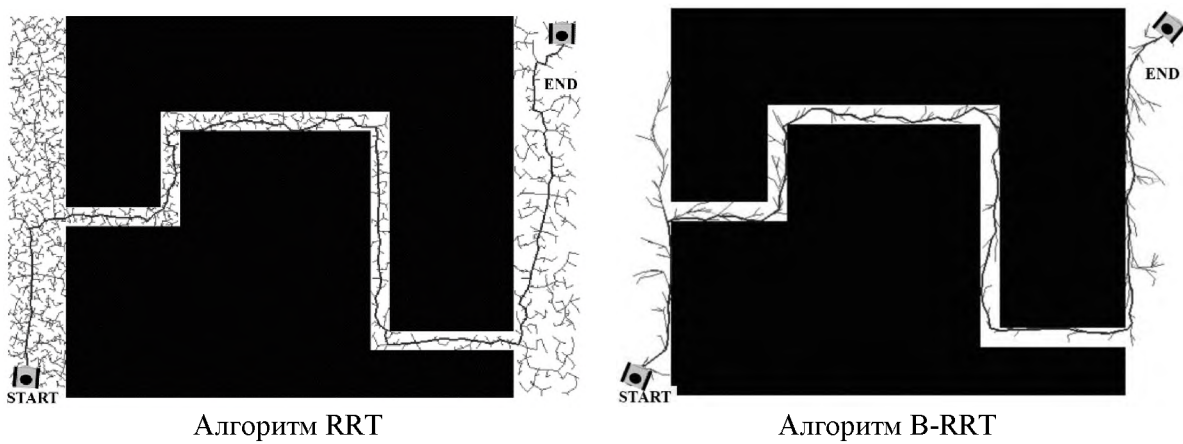
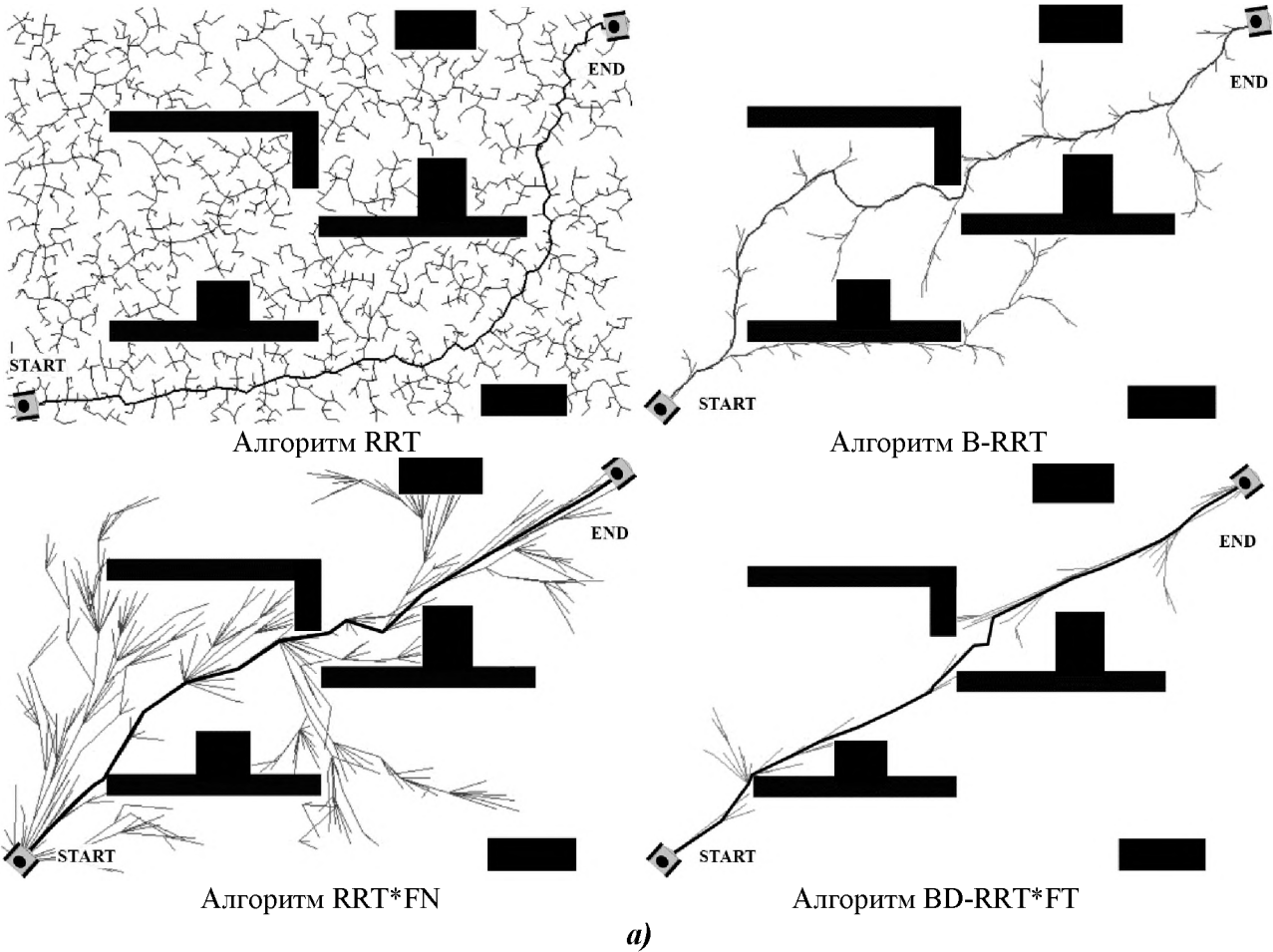
Перевіряються алгоритми RRT, B-RRT\*, RRT\*FN та BD-RRT\*FT. Результати планування шляху показані на рис. 3, а. Товста лінія позначає отримане рішення шляху. Інші дерева є ітераційними обчисленнями.

Бачимо, що односторонній алгоритм має занадто багато надлишкових точок вибірки в процесі планування, тоді як двосторонній алгоритм має більш очевидну спрямованість. Для інтуїтивного порівняння середня довжина шляху рішення, отримана зі 100 експериментів. Кількість ітерацій наведено в таблиці 1.

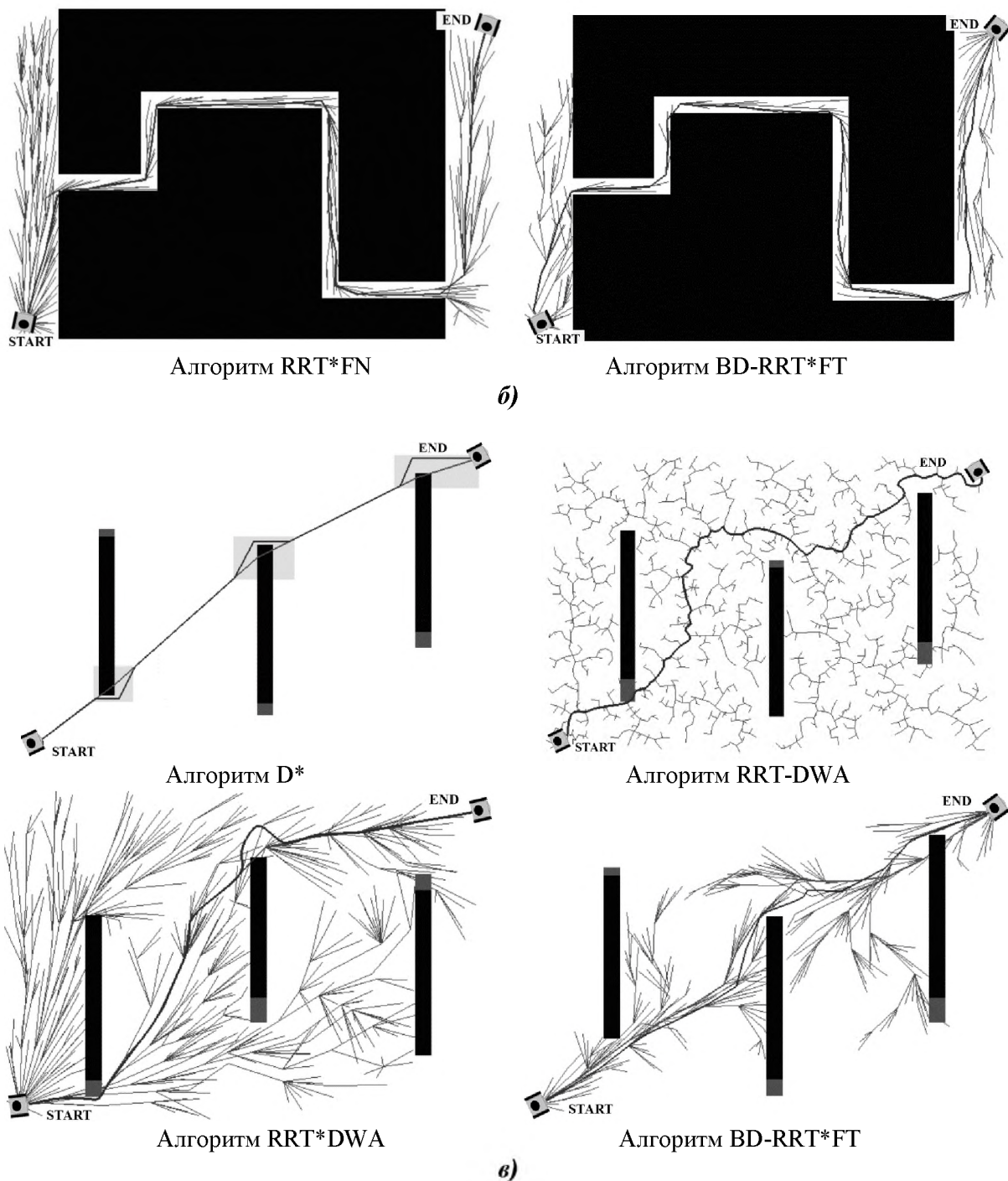
Таблиця 1

Дані порівняння продуктивності алгоритму на карті 1

Алгоритм	RRT	B-RRT*	RRT*FN	BD-RRT*FT
Середня довжина шляху (у. о.)	820,662	726,307	754,156	708,778
Середній час роботи, $\times 10^3$ (с)	41,596	0,624	2,188	0,1673
Споживана пам'ять (Мб)	329,78	285,52	282,63	246,51







**Рис. 3.** Візуалізація результату роботи алгоритмів. Планування шляху за трьома типами карт:  
*а* – карта 1: візуалізація результату роботи алгоритмів алгоритму;  
*б* – карта 2: візуалізація результату роботи алгоритмів; *в* – карта 3: візуалізація результату алгоритмів

Як видно з таблиці 1, двонаправлений алгоритм має певні переваги у швидкому пошуку рішення. Враховуючи, що вдосконалений алгоритм використовує стратегію двонаправленого жадібного пошуку, загальна вартість шляху ще більше зменшується. Оскільки алгоритм B-RRT\*, алгоритм RRT\*FN і алгоритм BD-RRT\*FT. Усі належать до алгоритму оптимального рішення. На рисунку 4, *а*, *б* показано графічний порівняльний аналіз продуктивності кожного алгоритму на карті 1.

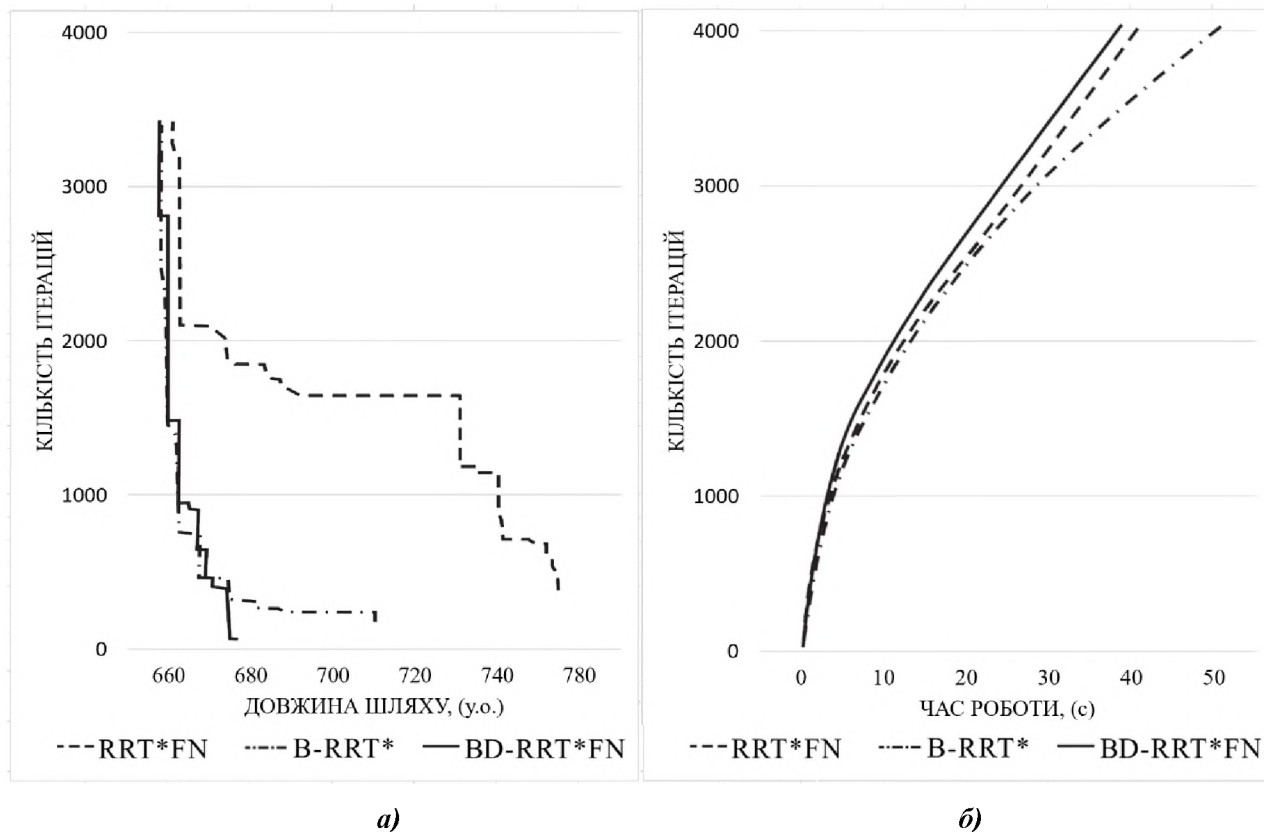


Рис. 4. Порівняльний аналіз продуктивності кожного алгоритму на карті 1:

*a* – зв'язок між кількістю ітерацій та довжиною шляху;

*б* – зв'язок між кількістю ітерацій та часом виконання

На рисунках 4, *a* і 4, *б* видно, що довжина рішення шляху та час пошуку алгоритму BD-RRT\*FN кращі, ніж у двох інших алгоритмів. Довжина алгоритму B-RRT\* після 500 ітерацій така сама, що й для BD-RRT\*FN. Розуміємо, що основа алгоритму в основному та сама, але оскільки він не має фіксованої кількості вузлів, час виконання демонструє увігнуту тенденцію до зростання зі збільшенням кількості ітерацій (рис. 4, *б*). Після 1500 ітерацій час роботи вдосконаленого алгоритму становить приблизно лінійну залежність, що пов'язано з кількістю ітерацій. При 3000 ітераціях алгоритму B-RRT\* необхідно 36,117 с, а BD-RRT\*FN – 29,221 с для виконання завдання зі знаходження шляху.

*Перевірка роботи алгоритмів на карті 2 (карта з вузьким проходом).*

Використовуємо карту 2 розміром 800 px × 600 px як карту з вузькими щілинами (рис. 3, *б*). За винятком конфігурації розташування перешкод на карті, решта налаштувань такі самі, як для карти 1. Результати планування шляху чотирьох алгоритмів показано на рисунку 3, *б*. Останні три є першими отриманими шляхами.

Для карт з вузьким каналом простору, через сліпоту зростання, односторонньому алгоритму важко отримати точки вибірки у вільному просторі в межах вузького каналу, в результаті чого кількість ітерацій і час виконання набагато вищі, ніж у двостороннього алгоритму пошуку шляху, а точки вибірки здебільшого зосереджені в лівому вільному просторі. В таблиці 2 показано отримані під час експерименту середня довжина рішення шляху та час виконання.

## Порівняння показників ефективності алгоритму на карті 2

Алгоритм	RRT	B-RRT*	RRT*FN	BD-RRT*FT
Середня довжина шляху (у. о.)	1383,031	1355,370	1239,629	1239,042
Середній час роботи, $\times 10^3$ (с)	145,188	2,4825	4,919	1,415
Споживана пам'ять (Мб)	320,98	281,12	280,67	245,72

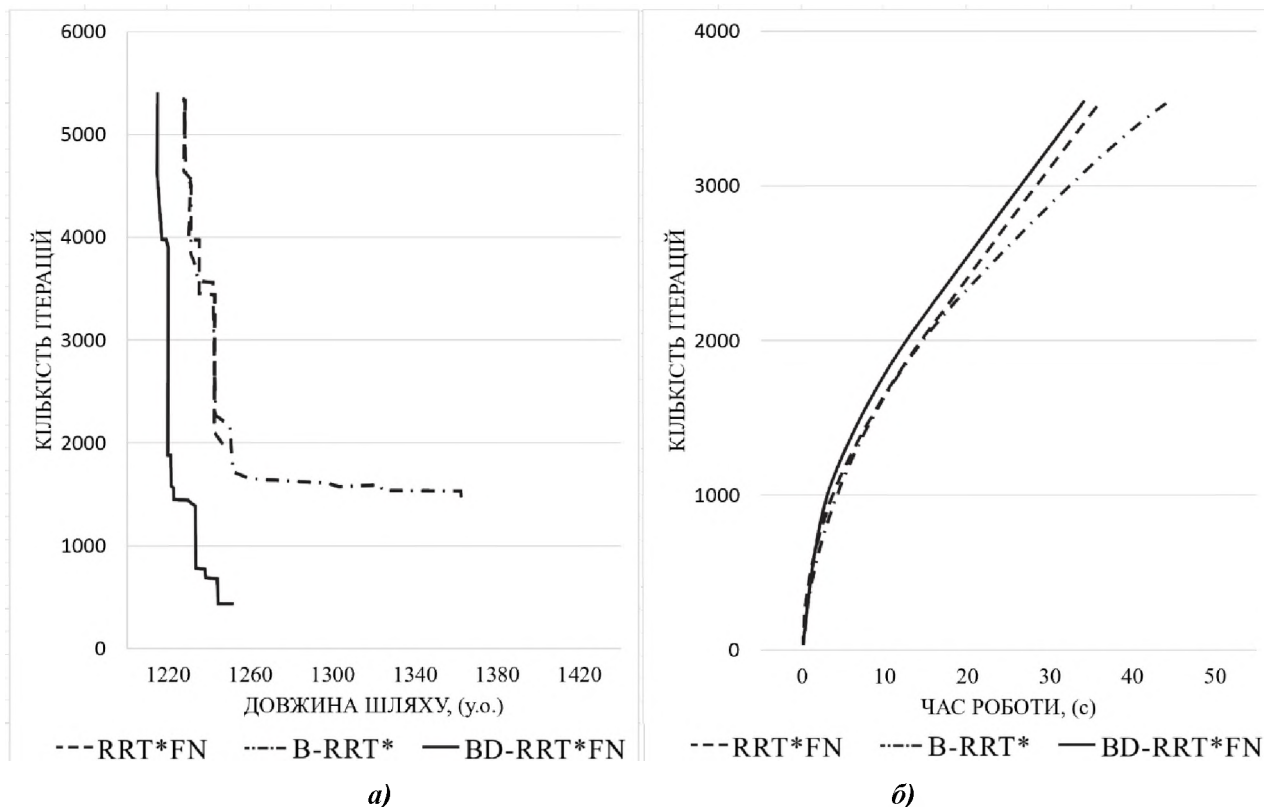


Рис. 5. Порівняльний аналіз продуктивності кожного алгоритму на карті 2:

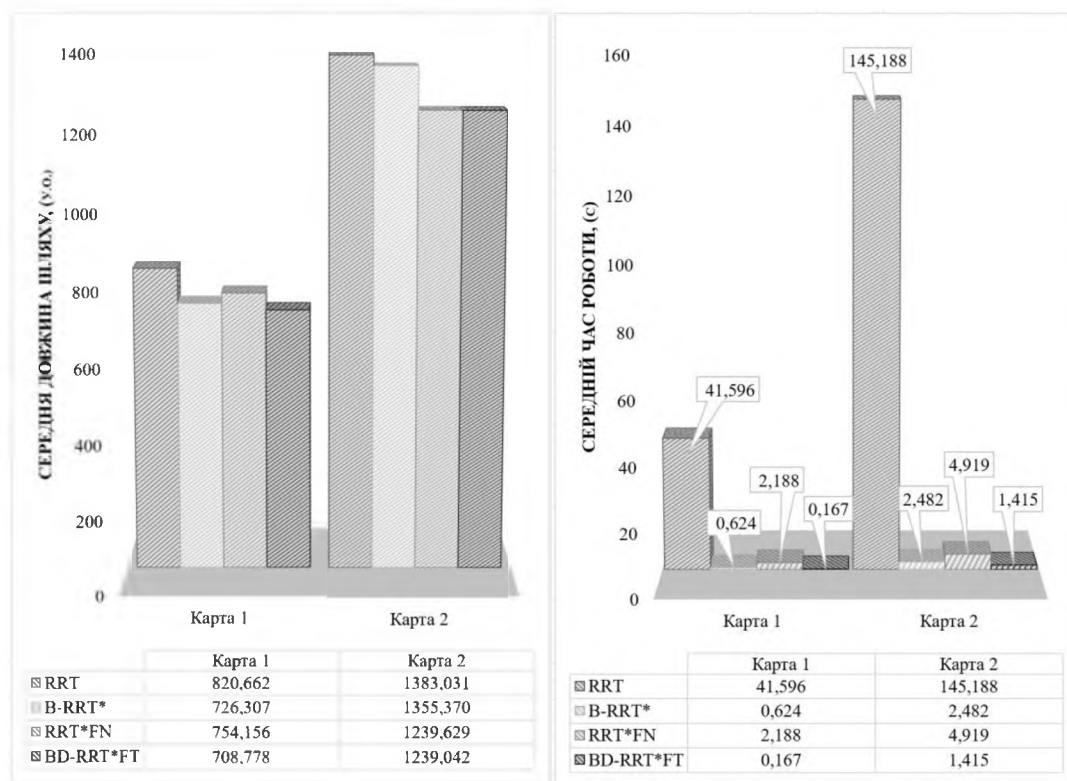
*а* – зв'язок між кількістю ітерацій та довжиною шляху;

*б* – зв'язок між кількістю ітерацій та часом виконання

Оскільки ймовірність вибору точок вибірки у вузькому каналі зменшується, загальна кількість точок вибірки збільшується. Час роботи алгоритму RRT перевищує 145 с, а кількість ітерацій перевищує 20 000, що створює велике навантаження на пам'ять, що досить сильно уповільнює процес розрахунку.

Порівняння продуктивності алгоритмів оптимального рішення та результати ітераційного процесу з додатковою оптимізацією в 3 алгоритмах показано на рисунку 5, *а*, *б*. З нього видно, що довжина та швидкість ітерації шляху, отриманого алгоритмом BD-RRT\*FN, кращі, ніж у алгоритмів B-RRT\* і RRT\*FN.

При перевірці з використанням карт 1 і 2 зі статично встановленими перешкодами, модифікований алгоритм BD-RRT\*FN показав високу продуктивність порівняно з іншими алгоритмами (рис. 6), тому для подальшої перевірки роботи алгоритму з динамічними об'єктами було прийнято рішення на заміну набору алгоритмів для карти 3.



**Рис. 6.** Порівняльні діаграми продуктивності алгоритмів на карті 1 і карті 2:  
 а – зв'язок між кількістю ітерацій та довжиною шляху;  
 б – зв'язок між кількістю ітерацій та часом виконання

*Перевірка роботи алгоритмів на карті 3 (карта з динамічними об'єктами).*

Для подальшого вивчення продуктивності алгоритму в динамічному середовищі, створено динамічну карту розміром 600 px × 800 px, що містить рухомі перешкоди. Динамічні перешкоди (чорна частина, розмір 40×200) рухаються вперед і назад уздовж осі Y, а діапазон руху становить Y = 20 – 580 px. В якості порівняльних алгоритмів представлено алгоритм D\* (Dynamics A\*), алгоритм RRT-DWA та алгоритм RRT\*DWA. Оскільки в динамічному середовищі довжина рішення шляху змінюється нерегулярно, то за для спрощення аналізу приймемо, що лише довжина шляху переміщення динамічної перешкоди буде впливати на глобальний шлях БАНЗ. Середні час виконання побудови шляху та довжина надані в таблиці 3, а результати планування шляху алгоритму показані на рисунку 3, в та рисунку 7.

Таблиця 3

**Порівняння показників ефективності алгоритму на карті 3**

Алгоритм	BD-RRT*FT	D*	RRT-DWA	RRT*DWA
Середня довжина шляху (у. о.)	759,658	691,375	989,506	766,310
Середній час роботи (с)	0,2844	41,303	36,9078	6,7424
Споживана пам'ять (Мб)	245,72	280,02	284,17	301,42

Як видно з рисунка 3, в, усі алгоритми мають можливість планування в реальному часі та можуть уникати динамічних (рухомих) перешкод. Середній шлях, запланований алгоритмом D\*, коротший, але оскільки алгоритм D\* є евристичним алгоритмом пошуку і базується на графах, його швидкість планування низька, а середній час планування на карті 3

перевищує 40 с. Алгоритми RRT-DWA і RRT\*DWA спочатку використовують алгоритми RRT і RRT\* для глобального планування шляху, а потім використовують алгоритм DWA під час руху БАНЗ. Локальне планування шляху використовується для досягнення динамічного уникнення перешкод, але через це легко впасти в локальну оптимальність, а середня довжина шляху та глобальний апіорний час планування шляху довший, ніж запропонований модифікований алгоритм BD-RRT\*FT. Фактично експеримент показав, що модифікований алгоритм BD-RRT\*FT має кращі можливості динамічного планування, але запланований шлях може бути тимчасово поганим через те, що деякі вузли вибірки відкидаються після того, як шлях знищено перешкодами. Ця ситуація покращується після кількох ітерацій, щоб переконатися, що шлях є цілісним.

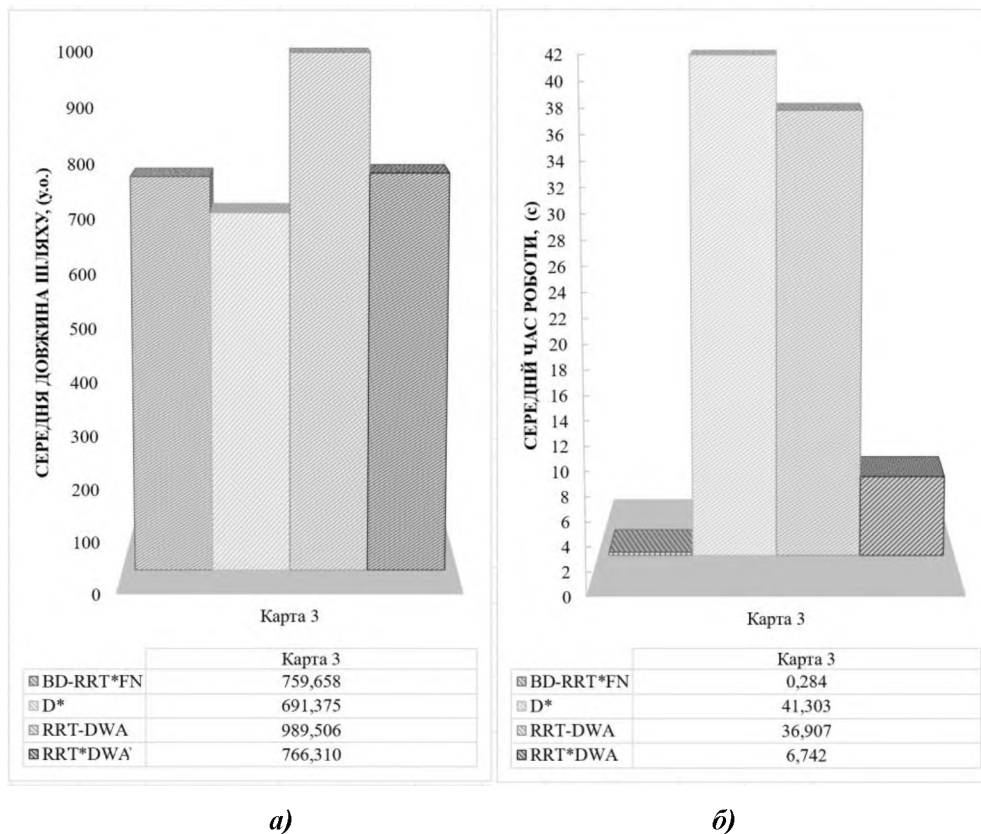


Рис. 7. Порівняльна діаграма продуктивності алгоритмів з динамічними об'єктами на карті 3:

а – зв'язок між кількістю ітерацій та довжиною шляху;

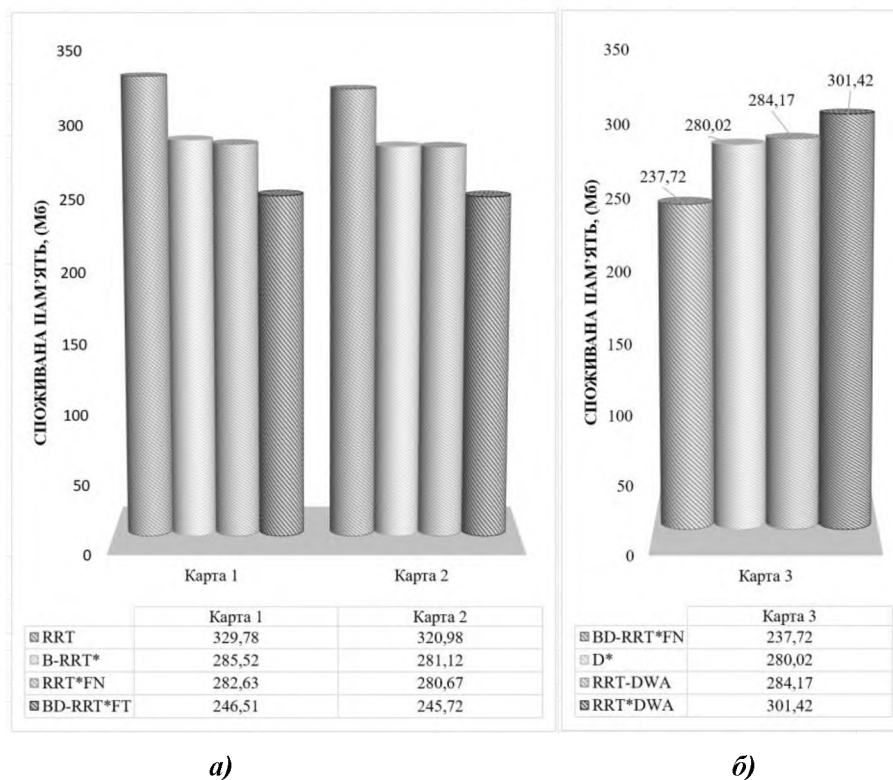
б – зв'язок між кількістю ітерацій та часом виконання

Під час проведення експериментальної частини на всіх етапах перевірки проводився контроль навантаження на пам'ять системи прийняття рішення.

Середні результати споживання при роботі всіх алгоритмів вказано в таблицях 1–3.

Також на рисунку 8 представлено порівняльні діаграми споживання об'єму пам'яті алгоритмами. Ми бачимо пряму залежність від складності та оптимальності виконання алгоритму та шляхів пошуку рішень.

Як і передбачалось, запропонований модифікований алгоритм BD-RRT\*FT показав гарну ефективність щодо завантаження пам'яті, внаслідок чого є можливість використання запропонованого алгоритму з менш потужними системами прийняття рішень.



**Рис. 8.** Порівняльна діаграма ефективності завантаження пам'яті системи прийняття рішень при виконанні пошуку шляху алгоритмами:  
*а* – робота алгоритмів на картах 1 і 2; *б* – робота алгоритмів на картах 3

### Висновки

З огляду на існуючу проблему планування шляху роботів у режимі реального часу, яка є центром досліджень у галузі інтелектуальних мобільних роботів, та розуміючи складність завдань під час проведення бойових дій в урбанізованому просторі щільної забудови міста з постійною зміною ландшафту, які покладаються на БАНЗ та мають тенденцію до постійного ускладнення, було запропоновано метод планування шляху БАНЗ з використанням модифікації динамічного двонаправленого RRT-алгоритму. Для чого проведено аналіз існуючих алгоритмів вирішення задачі пошуку шляху зі статичними перешкодами. На основі отриманої аналітики проведено модифікацію асимптотично оптимального алгоритму RRT\*FT та розроблено алгоритм BD-RRT\*FT, який можна застосовувати в динамічних середовищах, завдяки використанню двонаправленого жадібного пошуку для покращення часу планування алгоритму, довжини шляху та ефективності використання системних ресурсів пристрою прийняття рішення.

Під час досліджень з'ясовано, що для алгоритму RRT і його модифікацій існують різноманітні рішення, які побудовані з використанням сліпої вибірки, що ускладнює навігацію у вузьких ділянках. При цьому запропонований алгоритм завдяки оптимізації таких проблем не має і показав гарні результати.

Експериментально доведено ефективність алгоритму BD-RRT\*FT задля задоволення вимог планування шляху в реальному часі, дозволяючи БАНЗ швидко отримати оптимальний шлях без зіткнень у динамічних середовищах у режимі реального часу.

### Напрями подальших досліджень

Базуючись на виконаній роботі та отриманих в результаті даних, в подальшому планується створити для БАНЗ реальний прототип системи прийняття рішень, побудований з використанням запропонованого модифікованого алгоритму BD-RRT\*FT для подальшого вивчення поведінки алгоритму в реальних умовах в середовищі з динамічними перешкодами.



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Бернацький А. П., Панченко І. В., Восколович О. І. Розширена математична модель руху автономного наземного робота розвідника в умовах бойових дій в урбанізованому просторі // *Озброєння та військова техніка*. 2021. № 30 (2). С. 121–129.
2. Winnfield J. A. *Unmanned Systems Integrated Roadmap FY2011-2036* / Winnfield J. A. Jr., Kendall F.-Washington, DC: U. S. Department of Defense, March 9, 2012.
3. Бернацький А., Панченко І., Восколович О. *Основи робототехніки військового призначення: конспект лекцій*. Київ: ВІТІ, 2021.
4. Thomas H. Corman, Charles I. Leiserson, Ronald L. Rivest, Clifford Stein. *Algorithms: construction and analysis. Introduction to Algorithms*. Michigan U.: Williams, 2006. ISBN 978-0-262-53305-8.
5. Robert Schapire, Yoav Freund. *Boosting: Foundations and Algorithms*. MIT, 2012. ISBN 10: 0262526034; ISBN 13: 9780262526036.
6. Maw A. A., Tyan M., Nguyen T. A. et al. iADA\*-RL: Anytime graph-based path planning with deep reinforcement learning for an autonomous UAV // *Applied Sciences*. 2021. № 11 (9). P. 1–18. DOI: <https://doi.org/10.3390/app11093948>.
7. Kadry S., Alferov G., Fedorov V. D-Star Algorithm Modification // *International Journal of Online and Biomedical Engineering (iJOE)*. 2020. Vol. 16. No. 8. P. 108–113. DOI: <https://doi.org/10.3991/ijoe.v16i08.14243>.
8. Majeed A., Hwang SO. Path planning method for UAVs based on constrained polygonal space and an extremely sparse waypoint graph // *Applied Sciences*. 2021. № 11 (12). P. 5340. DOI: <https://doi.org/10.3390/app11125340>.
9. Kagan E. and Ben-Gal I. A Group-Testing Algorithm with Online Informational Learning. *IIE Transactions* // *Institute of Industrial Engineers*. № 46 (2). P. 164–184. DOI: <https://doi.org/10.1080/0740817X.2013.803639>.
10. Jeong I. B., Lee S. J., Kim J. H. Quick-RRT\*: Triangular inequality-based implementation of RRT\* with improved initial solution and convergence rate // *Expert Syst. Appl.* 2019. № 123. P. 82–90. DOI: <https://doi.org/10.1016/j.eswa.2019.01.032>.
11. Black, Paul E. Greedy algorithm. *Dictionary of Algorithms and Data Structures*, US National Institute of Standards and Technology\* PE Black. URL: <http://www.nist.gov/dads/HTML/greedyalgo.html>.
12. Gammell J. D., Srinivasa S. S., Barfoot T. D. Informed RRT\*: Optimal sampling-based path planning focused via direct sampling of an admissible ellipsoidal heuristic; *Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems*; Chicago, IL, USA. 14–18 September 2014. DOI: <https://doi.org/10.1109/IROS.2014.6942976>.
13. Taheri E., Ferdowsi M. H., Danesh M. Fuzzy greedy RRT path planning algorithm in a complex configuration space. *Int. J. Control. Autom. Syst.* 2018. № 16. P. 3026–3035. DOI: <https://doi.org/10.1007/s12555-018-0037-6>.
14. Adiyatov, Olzhas; Varol, Huseyin Atakan. A novel RRT-based algorithm for motion planning in Dynamic environments. In *Mechatronics and Automation (ICMA), 2017 IEEE International Conference on*, 2017. P. 1416–1421. DOI: <https://doi.org/10.1109/ICMA.2017.8016024>.
15. Spanogianopoulos, Sotirios and Sirlantzis, Konstantinos Non-holonomic Path Planning of Car-like Robot using RRT\*FN. In: *2015 12th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*. 2015. IEEE. P. 53–57. E-ISBN 978-1-4673-7971-7. DOI: <https://doi.org/10.1109/URAI.2015.7358927>.
16. Бідюк П. І., Тимошук О. Л. та ін. *Системи і методи підтримки прийняття рішень*. Київ: КПІ ім. Ігоря Сікорського, 2022.
17. Li B., Chen B. An Adaptive Rapidly-Exploring Random Tree, *Journal of Automatica Sinica*. 2021. IEEE. DOI: <https://doi.org/10.1109/JAS.2021.1004252>.
18. Klemm S., Oberländer J., Hermann A., Roennau A., Schamm T., Zollner J. M., Dillmann R. RT-Connect: Faster, asymptotically optimal motion planning / *Conference: 2015 IEEE International Conference on Robotics and Biomimetics (ROBIO 2015)*. At: Zhuhai, China Volume: 12. DOI: <https://doi.org/10.1109/ROBIO.2015.7419012>.

УДК 629.734

Данилюк І. А. ORCID: 0000-0003-0955-0108 (ВІТІ ім. Героїв Крут)  
Радченко М. М. ORCID: 0000-0002-8272-0727 (ВІТІ ім. Героїв Крут)  
Шаповал В. М. ORCID: 0000-0003-4637-9362 (ВІТІ ім. Героїв Крут)  
Сидоркін П. Г. ORCID: 0000-0003-2374-1402 (НДЦ ІСЗЗІ  
НТУ України «КПІ ім. Ігоря Сікорського»)

## МЕТОДИКА РАЦІОНАЛЬНОГО ВИБОРУ БЕЗПЛОТНОГО АВІАЦІЙНОГО КОМПЛЕКСУ ДЛЯ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ

Авіаційний ринок безпілотних авіаційних комплексів переповнений безпілотними апаратами, різноманітними за призначенням, класами, технічним рівнем і вартістю. Для вибору зразка безпілотного апарата, придатного для побудови телекомунікаційної аероплатформи, авторами запропонована методика, що вирішує завдання побудови телекомунікаційної аероплатформи як складової наземно-повітряної мережі систем радіозв'язку військового призначення з великою кількістю вагомих факторів.

З огляду на те, що при здійсненні вибору більшість дослідників у різних галузях схиляються до застосування методу аналізу ієрархій із залученням досвіду експертів у цих галузях, автори статті пропонують застосувати цей метод під час вибору варіанта безпілотного авіаційного комплексу для побудови зазначеної телекомунікаційної аероплатформи. В методиці виділені такі етапи аналізу ієрархій, як: визначення мети аналізу; визначення основних та варіантів; побудова дерева ієрархії від мети через параметри до варіантів; побудова матриць попарних порівнянь параметрів за метою та варіантів за параметрами; визначення ваг варіантів по системі ієрархії.

Наведені розрахунки здійснення вибору варіанта безпілотного авіаційного комплексу дозволили сформулювати наступні висновки: метод аналізу ієрархій відповідає потребі оперативного обґрунтування рішення щодо вибору варіанта безпілотного авіаційного комплексу для забезпечення виконання завдань телекомунікаційних аероплатформ при наявності групи експертів відповідної кваліфікації в галузі досліджень.

Напрямами подальших досліджень автори вважають можливість використання запропонованої методики для раціонального вибору обладнання (наприклад, безпілотного авіаційного комплексу) для розробки нових протоколів і алгоритмів функціонування самоорганізуючих радіомереж на основі безпілотних літальних апаратів.

**Ключові слова:** безпілотний авіаційний комплекс, метод аналізу ієрархій, телекомунікаційна аероплатформа, система зв'язку, управлінські рішення, вагові коефіцієнти.

### ***I. Danyliuk, M. Radchenko, V. Shapoval, P. Sidorkin Method of rational choice of unmanned aircraft for construction of telecommunication aeroplatforms.***

*The aviation market of unmanned aerial systems is saturated with unmanned vehicles, diverse in their purpose, classes, technical level, and cost. To select a suitable unmanned aerial vehicle for building a telecommunications air platform, the authors propose a methodology that addresses the task of constructing a telecommunications air platform as part of the ground-air network of military communication systems with a multitude of significant factors.*

*Given that when making a choice, most researchers in various fields tend to employ the Analytic Hierarchy Process (AHP) method with expert involvement, the authors of this article recommend applying this method when selecting an unmanned aviation complex variant for constructing the aforementioned telecommunications air platform. The methodology consists of the following AHP stages: defining the analysis objective, identifying key parameters and variants, constructing a hierarchy tree from the objective through the parameters to the variants, creating matrices of pairwise comparisons for parameters by objective and variants by parameters, determining the weights of variants within the hierarchy system.*

*The provided calculations for choosing an unmanned aviation complex variant have led to the following conclusions: the Analytic Hierarchy Process method aligns with the need for an expeditious justification of decisions regarding the selection of an unmanned aviation complex variant to fulfill the tasks of telecommunications air platforms in the presence of a group of experts with relevant qualifications in the research field.*

*The authors consider the possibility of using the proposed methodology for the rational selection of equipment (for example, unmanned aerial vehicle) for the development of new protocols and algorithms for the functioning of self-organizing radio networks based on unmanned aerial vehicles as directions for further research.*

**Keywords:** *unmanned aerial system, analytic hierarchy process, telecommunication aerial platform, communication system, management decisions, weighting factors.*



### **Постановка завдання у загальному вигляді**

Одним із сучасних напрямів розроблення систем озброєнь у збройних силах різних країн, згідно з оглядом трендів розвитку перспективних видів озброєння [1; 2], є використання робототехніки й автономних безпілотних апаратів. Військово-політичним керівництвом країни наряду із заходами щодо раціонального розподілу військово-технічної допомоги між учасниками сил оборони для відсічі повномасштабного вторгнення рф в Україну проводиться робота щодо синергії внутрішніх ресурсів і можливостей швидкого та безпечного виробництва безпілотних авіаційних комплексів (далі – БпАК) (під БпАК розуміється безпілотний літальний апарат та наземна станція керування ним) на потужностях різноманітних розробників.

Оснащення БпАК ретрансляторами радіосигналів перетворює їх в телекомунікаційні аероплатформи (далі – ТА). Застосування ТА в мережах зв'язку військового призначення дозволяє [3]:

- швидко (порівняно з наземними ретрансляторами) та незначними ресурсами (одиниці ТА) розширити зону функціонування мереж радіозв'язку військового призначення (територію виконання завдання бойовими підрозділами);

- покращити радіозв'язність між елементами мережі (радіозв'язок прямої видимості з більшою кількістю абонентів, можливість забезпечити зв'язність незв'язних компонент мережі, можливість забезпечити радіозв'язок між мобільними абонентами при їхньому значному віддаленні від основних сил або в умовах впливу РЕП противника тощо);

- значно покращити основні властивості (пропускну здатність, живучість, мобільність тощо) мережі зв'язку та характеристики процесу передачі інформації.

Отже, на сьогодні є актуальним наукове завдання щодо розробки методики раціонального вибору БпАК, необхідного для створення ТА з урахуванням багатьох варіантів вже розроблених БпАК, характеристик ретрансляторів радіосигналів, вимог до систем військового зв'язку та параметрів інформаційного обміну між органами управління та посадовими особами в сучасних бойових діях.

### **Аналіз останніх досліджень і публікацій**

Вибір варіанта БпАК для створення ТА пропонується здійснити з позицій системного підходу – шляхом дослідження об'єкта як цілісної множини елементів в сукупності відношень і взаємозв'язків між ними.

Під час синтезу раціонального варіанта ТА необхідно врахувати множину різних параметрів та факторів [4–7], таких як:

- технічні характеристики БпАК на відповідність вимогам бойового застосування підрозділів ЗСУ;

- технічні характеристики ретранслятора на їх відповідність вимогам інформаційного обміну системи військового зв'язку між мобільними абонентами (за пропускну здатністю, швидкістю передавання даних, типу трафіка тощо);

- необхідність забезпечення електромагнітної сумісності безпосередньо БпАК із обладнанням радіоретранслятора;

- необхідність оснащення ТА додатковим обладнанням (наприклад, антенами);

- конструктивні особливості щодо розміщення обладнання радіоретранслятора та додаткового обладнання тощо.

Крім того, вирішуючи завдання вибору БпАК для побудови ТА, необхідно врахувати велику кількість параметрів та різну їхню природу, тому пропонується використати методи експертної оцінки.

Завдання за обраною тематикою дослідження достатньо висвітлюються у публікаціях низкою авторів [8–11], як оціночні інструменти для багатокритеріальних задач із врахуванням

особливостей галузей застосування визнають доцільними саме експертні методи, де використовуються знання та досвід фахівців в обраній галузі.

Зважаючи на вищенаведене, авторами проаналізовано можливості використання експертних методів для вирішення поставленої задачі щодо раціонального вибору ТА на базі БпАК, які можна використовувати для отримання експертних оцінок [12; 13], а саме:

1. Метод Делфі. Цей метод використовується для отримання консенсусу серед групи експертів. Експерти надають свої оцінки певним питанням анонімно, а потім результати аналізуються і надсилаються їм для повторного розгляду. Процес повторюється до досягнення консенсусу.

2. Метод анкетування експертів. Експерти заповнюють анкети, де вони надають свої оцінки або ранжують альтернативи. Результати анкетування потім аналізуються для прийняття рішення.

3. Метод аналізу ієрархій (Analytic Hierarchy Process). Експерти порівнюють альтернативи попарно за допомогою шкали або оцінюють їх за певними критеріями. За допомогою математичних розрахунків визначається важливість кожної альтернативи.

4. Метод оцінки за допомогою експертних груп. Експерти збираються разом і обговорюють питання, що вимагають оцінки. Вони намагаються досягти консенсусу або приймають рішення на основі дискусії.

5. Метод вагових коефіцієнтів. Експерти надають числові вагові коефіцієнти кожному критерію або альтернативі відповідно до їхньої важливості. Потім проводяться обчислення для визначення сумарних оцінок.

6. Метод ранжування. Експерти ранжують альтернативи в порядку їхньої важливості або прийнятності.

7. Метод Борда. Експерти надають бали альтернативам відповідно до їхньої важливості, а потім сумують бали для кожної альтернативи.

8. Метод сценаріїв. Експерти розробляють різні сценарії розвитку подій та оцінюють їх вірогідність і наслідки.

9. Метод голосування. Експерти голосують за альтернативи або питання, і рішення приймається на основі голосів більшості.

10. Метод експертного судження. Експерти надають свої суб'єктивні оцінки на основі свого досвіду та знань.

Кожен із цих методів має свої переваги і недоліки та може бути застосованим залежно від конкретного контексту завдання. Важливо правильно підібрати метод експертних оцінок з урахуванням обставин і мети прийняття рішення.

Для вибору БпАК в якості ТА із перелічених методів експертної оцінки автори статті пропонують використати метод аналізу ієрархій (метод Сааті) [13], ґрунтуючись на наступних підставах:

1. Структурованість рішення. Метод ієрархій розкладає складне завдання вибору моделі БпАК на послідовні кроки та підзавдання. Це сприяє більш структурованому та системному підходу до прийняття рішення.

2. Узгодженість експертних оцінок. Цей метод дозволяє враховувати різні точки зору експертів і оцінки їхньої узгодженості, що допомагає уникнути суб'єктивних виборів і підвищує об'єктивність прийняття рішення.

3. Множинні критерії. Вибір моделі БпАК може бути визначений багатьма критеріями, такими як максимальна відстань, витрати, час роботи тощо. Метод Сааті дозволяє враховувати ці критерії та їхню важливість для кінцевого рішення.

4. Сприяє зростанню якості рішення. Враховуючи різні аспекти вибору та їхню важливість, метод Сааті допомагає зробити кращий вибір моделі БпАК, що відповідає специфікаціям проекту і потребам.

Автори вважають, що використанню методу Сааті властиві наступні недоліки:

1. Час та ресурси. Проведення аналізу ієрархій може вимагати значних зусиль, часу та ресурсів, особливо якщо задача дуже складна і велика кількість критеріїв та альтернатив. Даний недолік може бути вирішений завдяки достатнім розрахунковим можливостям сучасної комп'ютерної техніки, що нівелює цей недолік.

2. Суб'єктивність експертів. Результати методу Сааті можуть сильно залежати від обраної групи експертів. Якщо експерти недостатньо кваліфіковані або мають різний погляд, це може спричинити неточні результати. Цей недолік може бути усунений завдяки залученню досвідчених фахівців, які спеціалізуються саме на розробці БпАК в якості ТА.

3. Схильність до маніпуляцій. Можливість маніпуляції результатами аналізу ієрархій може виникнути, якщо деякі учасники намагаються вплинути на результати шляхом зміни їхніх оцінок або важливості критеріїв. Нівелюється шляхом сподівання на порядність залучених експертів.

4. Обмежена узгодженість. Деякі задачі можуть бути настільки складними, що досягнення узгодженості між оцінками може бути викликано важкістю порівняння різних альтернатив. Це нейтралізується завдяки порозумінню експертів у вибраних кількісних характеристиках моделей БпАК.

Публікацій за темою пошуку вибору шляхів підтримки управлінських рішень з використанням методу експертних оцінок, з огляду на важливість питання, існує достатня кількість.

Авторами [8] зазначено, що під час проектування і супроводження розподілених автоматизованих інформаційних систем потрібні інструменти комплексного оцінювання різних за своєю природою факторів якісного і кількісного характеру та врахування різних внутрішніх і зовнішніх зв'язків, а також виконано аналіз методів і процедур шкального оцінювання в задачах прийняття рішень. Комплексна оцінка представлена як узагальнена думка групи експертів про важливість (пріоритетність) конкретного об'єкта всередині деякої їхньої сукупності або про величину інтенсивності (концентрації) тієї чи іншої властивості об'єкта. Запропоновані числові шкали відношень Сааті дозволяють встановити відносні пріоритети важливості об'єктів – критеріїв і альтернатив рішень, що приймаються експертами. Ці шкали дозволяють експерту вибирати чисельні значення відношень переваги одного порівнюваного об'єкта перед іншим. Відмічено, що застосування методу аналізу ієрархій дає хороші результати при використанні дев'ятибальної шкали відношень у задачах прийняття рішень при проектуванні і супроводженні розподілених автоматизованих інформаційних систем.

У статті [9] наведено удосконалену методику вибору маршруту руху транспортного засобу для отримання максимального економічного ефекту під час доставки продукції від відправника до одержувача, а також описано застосування цієї методики на прикладі рішення практичної задачі. У процесі вдосконалення методики щодо вибору маршруту руху транспортного засобу для розвезення товару використовувався метод експертних оцінок, в якому 25 експертів визначали ранг кожного з критеріїв, що оцінювались. Зазначено, що метод експертних оцінок, який використано для раціонального вибору параметрів перевезення, суттєво зменшує витрати на транспортні послуги.

Автори статті [10] визначили шляхи розв'язання задачі раціонального вибору комплексу авторських засобів розробки курсів дистанційного навчання шляхом застосування методу аналізу ієрархій (далі – МАІ). Математична постановка задачі раціонального вибору комплексу передбачає побудову ієрархічної системи показників, що характеризують комплекс. А методика раціонального вибору авторських засобів згідно з методом аналізу ієрархій формує п'ять етапів розв'язання задачі вибору (порівняльної експертизи комплексу), а саме: з'ясування цілі дослідження, ієрархічну декомпозицію задачі, складання матриць

попарних порівнянь відносної важливості показників, формування локальних пріоритетів, експертизу. Зазначено, що розв'язання задачі множинного вибору за допомогою методу аналізу ієрархій є хоч і суб'єктивною процедурою особи, яка приймає рішення, але одночасно й відносно простим, доступним і ефективним для практичного використання методом щодо вибору комплексу авторських засобів розробки курсів дистанційного навчання.

В [11] наведено, що оцінка рівня кібербезпеки інформаційно-телекомунікаційного вузла (далі – ІТВ) відноситься до класу багатокритеріальних завдань і для її здійснення в умовах невизначеності, а також для аналізу та прогнозування ситуацій з великою кількістю вагомих факторів і для її здійснення найбільш доцільно застосовувати методи, в основі яких закладені судження експертів у галузі кібернетичного захисту. В методиці оцінки кібернетичної захищеності ІТВ автори запропонували застосувати метод анкетування, який є найвідомішим серед методів експертного оцінювання і дозволяє безпосередньо використовувати судження та інтуїцію експертів при оцінюванні захисту формалізованої структури ІТВ. Експертна оцінка попарних порівнянь вагових значень компонентів ІТВ, які захищаються, розраховують згідно з якісною шкалою Сааті. Отримання коефіцієнтів важливості компонентів ІТВ здійснюється з використанням методу рангових оцінок. Чим більше ранг, тим більша вага тієї чи іншої компоненти ІТВ для захисту, а сума всіх значень коефіцієнтів дорівнює одиниці. Запропонована методика надає посадовим особам, які відповідальні за кібернетичну безпеку ІТВ, можливість отримувати кількісний показник рівня кіберзахищеності, що дасть забезпечити якісне прийняття рішень щодо рівня кібернетичної захищеності ІТВ у цілому.

Тому автори статті пропонують розглянути метод аналізу ієрархій (метод Сааті) як інструменту для вибору моделі БпАК в якості ТА.

**Метою цієї статті** є розробка методики раціонального вибору БпАК для побудови ТА як складової наземно-повітряної мережі (далі – НПМ) систем транкінгового радіозв'язку військового призначення для вирішення наступних завдань [3]: поєднання незв'язних НПМ, резервування існуючої мережі радіозв'язку, збільшення зони покриття мережі радіозв'язку тощо.

#### **Виклад основного матеріалу**

Для вирішення завдання щодо вибору БпАК для ТА можливо використовувати кількісні та якісні методи прийняття управлінських рішень [12]. Кількісні методи застосовують, коли фактори, що впливають на вибір рішення, можна кількісно визначити та оцінити, а якісні методи використовують, коли фактори, що визначають прийняття рішення, не можна кількісно охарактеризувати або взагалі не піддаються кількісному виміру. До якісних методів належать переважно експертні методи. В рамках мети даної статті автори пропонують застосувати МАІ на основі вагових коефіцієнтів [13]. Як відомо, цей метод є загальним методом розв'язання широкого класу слабо структурованих задач прийняття рішень в умовах наявності багатьох критеріїв і дозволяє поєднати математичний апарат із досвідом та інтуїцією особи, що бере участь у підготовці рішення. Для оцінки відносної величини факторів за допомогою парних порівнянь використовується досвід окремих експертів. Кожен із респондентів повинен порівняти відносну важливість між двома пунктами відповідно до спеціально розробленої анкети МАІ, яка становить від 1 до 9 градацій оцінки [13].

Для вирішення поставленої мети роботи пропонується методика раціонального вибору БпАК під платформу ТА, яка складається з наступних етапів.

**Етап 1. Визначення вихідних даних.** Дано:

1) Варіанти ТА:

- ТА на базі БпАК літакового типу (ТА-Л);
- ТА на базі БпАК гвинтокрильного типу (ТА-Г);
- ТА на базі аеростатного типу (ТА-А).

2) Групи характеристик ТА для визначення критеріїв щодо прийняття рішень експертами:

- а) льотно-технічні характеристики ТА (далі – ЛТХ);
- б) коефіцієнт економічності силової установки (далі – КЕСУ);
- в) характеристики обладнання БпАК (далі – ХОТА);
- г) характеристики радіоретранслятора (далі – ХР);
- д) електромагнітна сумісність електротехнічних модулів БпАК з режимами роботи радіоретранслятора (далі – ЕМС);
- е) ринкова та експлуатаційна вартість ТА (далі – В).

Більш детально розглянемо кожен групу показників:

а) льотно-технічні характеристики ТА:

- максимальна дальність польоту (км), бойовий радіус дії (км);
- тип та режим зльоту та посадки;
- злітна маса (кг);
- економічна (крейсерська) швидкість (км/год);
- максимальна та мінімальна швидкість (км/год);
- статична стеля (м);
- маса корисного навантаження (кг);
- стартова потужність двигуна (Вт);
- ємність основного акумулятора (А\*год);
- номінальна напруга акумулятора (В);
- коефіцієнт допустимого розряду акумулятора;

б) коефіцієнт економічності силової установки – показник, який відображає ефективність перетворення вхідної енергії (наприклад, палива, електроенергії тощо) на корисну роботу, що виконується силовою установкою. Цей показник визначається співвідношенням між корисно витраченою енергією та загальною вхідною енергією, вираженою у відсотках і може бути від 0 % до 100 %. Корисна робота вказує на виконану корисну роботу, яка може бути механічною, електричною, тепловою або іншого типу, залежно від конкретного випадку. Вхідна енергія означає загальну енергію, витрачену на силову установку, наприклад, енергія палива, електроенергії тощо. Чим більший коефіцієнт ефективності, тим ефективніше силова установка використовує вхідну енергію для виконання корисної роботи та оцінюється експертами за шкалою від 1 до 9 градаций оцінки;

в) характеристики обладнання БпАК:

- характеристики систем навігації (GPS, ГЛОНАСС-NAVSTAR, інерціальна, гібридна);
- характеристики станції управління та контролю польоту (система повернення до міста базування, наявність програмного забезпечення для автоматизації рішення задач планування, розгортання та оперативного управління ТА тощо);
- характеристики каналу управління ТА з пункту управління (тип радіозасобу та параметри антени, діапазон частот, дальність дії, швидкість передачі даних, кількість закритих каналів, довжина ключів шифрування тощо);

г) характеристики радіоретранслятора:

- діапазон частот (МГц);
- кількість радіоканалів;
- вихідна потужність передавача (Вт);
- крок частотної сітки (кГц);
- напруга живлення (В);

- стабільність частоти (ррм);
- струм споживання при передачі (А);
- струм споживання при очікуванні (А);
- чутливість приймача (мкВ);
- протоколи інформаційного обміну;
- швидкості передачі при певних режимах роботи;
- характеристики антени (тип, розміри та ін.);
- габаритні розміри (мм × мм × мм);
- вага (г);

д) електромагнітна сумісність електротехнічних модулів БпАК із режимами роботи радіоретранслятора. Цей аналіз здійснюється експертами шляхом якісної оцінки впливу електромагнітних полів на електронні компоненти, антени, системи навігації та інші елементи БпАК для подальшого визначення способів забезпечення оптимальної роботи БпАК в якості ТА в умовах різних електромагнітних впливів;

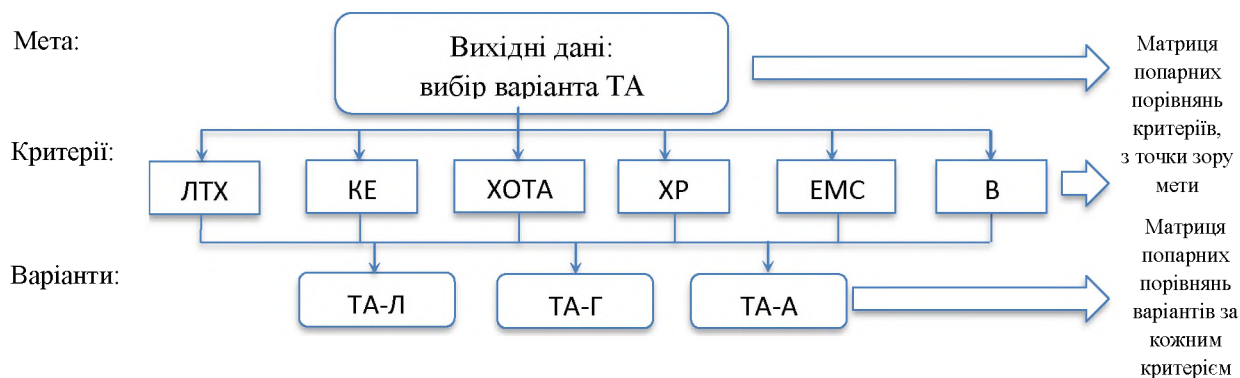
е) ринкова та експлуатаційна вартість ТА – це вартість придбання та експлуатації ТА.

3) Оперативно-тактичні та технічні вимоги до ТА для виконання завдань по зв'язку певної ланки управління ЗСУ (задання граничних значень показників ТА).

4) Цільові функції призначення ТА (наприклад, забезпечення зв'язності мобільних абонентів у зоні радіопокриття певного радіуса, забезпечення пропускну здатності певної кількості абонентів не менше заданого значення, забезпечення певного часу встановлення зв'язку на заданій відстані від точки старту тощо).

Експертами у процесі реалізації запропонованої методики були задіяні автори цієї публікації.

**Етап 2. Формування ієрархії ухвалення рішення (рис. 1).**



**Рис. 1.** Процес ухвалення рішення згідно з МАІ

**Етап 3. Побудова матриці попарних порівнянь критеріїв.**

3.1. Порівняння критеріїв за метою.

Експерти виконують попарне порівняння кожного з обраних критеріїв за якісною шкалою, з наступним перетворенням у бали:

- однаково, байдуже = 1;
- трохи краще (гірше) = 3 (1/3);
- краще (гірше) = 5 (1/5);
- значно краще (гірше) = 7 (1/7);
- принципово краще (гірше) = 9 (1/9).

При проміжній оцінці використовуються проміжні бали: 2, 4, 6, 8.

Складаємо матрицю, виходячи із умов:

$a_{ij}$  – відношення критерію  $i$  до критерію  $j$ .  $a_{ji} = 1/a_{ij}$ ,  $a_{ii} = 1$ .

Матриці за критеріями складаються так:

знаходимо суму елементів кожного стовпця за формулою:  $S_j = a_{1j} + a_{2j} + \dots + a_{nj}$ ;

ділимо всі елементи матриці на суму елементів відповідного стовпця:  $A_{ij} = \frac{a_{ij}}{S_j}$ .

Ці дві дії називаються нормуванням матриці.

Знаходимо середнє значення для кожного рядка: виконуємо нормування за кожним критерієм (визначаємо вагу в долях).

Наприклад, у таблиці 1 представлено парні порівняння груп критеріїв згідно з прийнятою вище шкалою (експертами виступали автори статті).

Отримані стовпчики нормування (вага в долях та вага у відсотках) визначають «ваги» критеріїв із точки зору заданої мети. Ці стовпчики називають вагомими стовпчиками параметрів за метою.

З точки зору задоволення мети щодо виконання оперативно-тактичних та технічних вимог до ТА для виконання завдань по зв'язку певної ланки управління ЗСУ (задання граничних значень показників ТА) та досягнення цільової функції призначення ТА (забезпечення зв'язності мобільних абонентів у зоні радіопокриття певного радіуса, забезпечення пропускну здатності певної кількості абонентів не менше заданого значення, забезпечення певного часу встановлення зв'язку на заданій відстані), найбільш вагомими є критерії: за льотно-технічними характеристиками ТА (42,63 %); електромагнітною сумісністю електротехнічних модулів БПАР з режимами роботи ретранслятора (19,9 %); характеристик радіоретранслятора (16,27 %). Коефіцієнт економічності ТА має найменший ваговий коефіцієнт, який складає загалом 2,94 %.

Таблиця 1

**Матриця попарних порівнянь критеріїв**

Критерій ТА	ЛТХ	КЕСУ	ХОТА	ХР	ЕМС	В	Нормування	Нормування
							(вага в долях)	(вага в %)
ЛТХ	1,00	7,00	5,00	3,00	7,00	5,00	0,43	42,63%
КЕСУ	0,14	1,00	0,17	0,20	0,20	0,17	0,03	2,94%
ХОТА	0,20	6,00	1,00	0,33	0,20	0,25	0,07	7,37%
ХР	0,33	5,00	3,00	1,00	0,50	4,00	0,16	16,27%
ЕМС	0,14	5,00	5,00	2,00	1,00	4,00	0,20	19,90%
В	0,20	6,00	4,00	0,25	0,25	1,00	0,11	10,88%

### 3.2. Порівняння варіантів за критеріями.

Складаємо аналогічні матриці порівняння варіантів ТА за кожним критерієм (рис. 2).

<b>Критерій ЛТХ</b>	ТА-Л	ТА-Г	ТА-А	<b>Критерій КЕСУ</b>	ТА-Л	ТА-Г	ТА-А
ТА-Л	1,00	0,33	7,00	ТА-Л	1,00	0,33	0,13
ТА-Г	3,00	1,00	5,00	ТА-Г	3,00	1,00	0,20
ТА-А	0,14	0,20	1,00	ТА-А	8,00	5,00	1,00
<b>Критерій ХОТА</b>	ТА-Л	ТА-Г	ТА-А	<b>Критерій ХР</b>	ТА-Л	ТА-Г	ТА-А
ТА-Л	1,00	0,33	0,14	ТА-Л	1,00	0,20	0,33
ТА-Г	3,00	1,00	5,00	ТА-Г	5,00	1,00	3,00
ТА-А	7,00	0,20	1,00	ТА-А	3,00	0,33	1,00
<b>Критерій ЕМС</b>	ТА-Л	ТА-Г	ТА-А	<b>Критерій В</b>	ТА-Л	ТА-Г	ТА-А
ТА-Л	1,00	0,33	0,14	ТА-Л	1,00	0,33	0,13
ТА-Г	3,00	1,00	0,20	ТА-Г	3,00	1,00	0,17
ТА-А	7,00	5,00	1,00	ТА-А	8,00	6,00	1,00

Рис. 2. Матриці порівняння варіантів ТА за кожним критерієм

Критерій ЛТХ	ТА-Л	ТА-Г	ТА-А	Нормування (вага в долях)	Нормування (вага в %)
ТА-Л	1,00	0,33	7,00	0,33	33%
ТА-Г	3,00	1,00	5,00	0,59	59%
ТА-А	0,14	0,00	0,00	0,08	8%

Критерій КЕСУ	ТА-Л	ТА-Г	ТА-А	Нормування (вага в долях)	Нормування (вага в %)
ТА-Л	1,00	0,33	0,13	0,09	9%
ТА-Г	3,00	1,00	0,20	0,20	20%
ТА-А	8,00	5,00	1,00	0,82	82%

Критерій ХОТА	ТА-Л	ТА-Г	ТА-А	Нормування (вага в долях)	Нормування (вага в %)
ТА-Л	1,00	0,33	0,14	0,11	11%
ТА-Г	3,00	1,00	5,00	0,58	58%
ТА-А	7,00	0,20	1,00	0,31	31%

Критерій ХР	ТА-Л	ТА-Г	ТА-А	Нормування (вага в долях)	Нормування (вага в %)
ТА-Л	1,00	0,20	0,33	0,11	11%
ТА-Г	5,00	1,00	3,00	0,63	63%
ТА-А	3,00	0,33	1,00	0,26	26%

Критерій ЕМС	ТА-Л	ТА-Г	ТА-А	Нормування (вага в долях)	Нормування (вага в %)
ТА-Л	1,00	0,33	0,14	0,08	8%
ТА-Г	3,00	1,00	0,20	0,19	19%
ТА-А	7,00	5,00	1,00	0,72	72%

Критерій В	ТА-Л	ТА-Г	ТА-А	Нормування (вага в долях)	Нормування (вага в %)
ТА-Л	1,00	0,33	0,13	0,08	8%
ТА-Г	3,00	1,00	0,17	0,17	17%
ТА-А	8,00	6,00	1,00	0,75	75%

Рис. 3. Нормовані матриці порівняння варіантів за кожним критерієм для різних варіантів ТА

Проводимо нормування кожної із матриць кожного критерію за варіантами ТА й в результаті одержуємо стовпці (вектори) вагових коефіцієнтів різних варіантів ТА порівняно з поглядом відповідності окремим критеріям (рис. 3).

Аналіз порівняння варіантів ТА за обраними критеріями представлено у таблиці 2.

Таблиця 2

**Порівняння варіантів ТА за обраними критеріями**

Критерій	Варіанти ТА за вагомістю		
	Найбільш	Середньо	Найменш
ЛТХ	ТА-Г 59%	ТА-Л 33%	ТА-А 8%
КЕСУ	ТА-А 82%	ТА-Г 20%	ТА-Л 9%
ХОТА	ТА-Г 58%	ТА-А 31%	ТА-Л 11%
ХР	ТА-Г 63%	ТА-А 26%	ТА-Л 11%
ЕМС	ТА-А 72%	ТА-Г 19%	ТА-Л 8%
В	ТА-А 75%	ТА-Г 17%	ТА-А 8%

З таблиці 2 можна зробити наступні висновки щодо вибору варіанту ТА за отриманими критеріями: за критерієм ЛТХ найбільш вагомим є ТА-Г; за критерієм КЕСУ найбільш вагомим є ТА-А; за критерієм ХОТА найбільш вагомим є ТА-Г; за критерієм ХР найбільш



вагомим є ТА-Г; за критерієм EMC найбільш вагомим є ТА-А; за критерієм В найбільш вагомим є ТА-А.

**Етап 4. Визначення ваг варіантів по системі ієрархії.**

Внаслідок попередніх розрахунків порівняння результатів за обраними критеріями були сформовані:

- вектор ваг параметрів;
- матриця ваг варіантів за кожним критерієм, що складається з отриманих вагових стовпців.

Таблиця 3

**Вектор ваг критеріїв за наступними характеристиками**

	Нормування (вага в долях)
ЛТХ	0,43
КЕСУ	0,03
ХОТА	0,07
ХР	0,16
EMC	0,20
В	0,11

Таблиця 4

**Матриця ваг варіантів за кожним критерієм**

Варіанти / Критерії	ЛТХ	КЕСУ	ХОТА	ХР	EMC	В
ТА-Л	0,33	0,09	0,11	0,11	0,08	0,08
ТА-Г	0,59	0,20	0,58	0,63	0,19	0,17
ТА-А	0,08	0,82	0,31	0,26	0,72	0,75

**Етап 6. Визначення ваг варіантів.**

Знаходячи добуток матриці ваг варіантів за кожним критерієм (табл. 2) та вектором ваг критеріїв (табл. 3), отримуємо ваги варіантів із погляду досягнення мети (рис. 4):

$$\begin{pmatrix} 0,33 & 0,09 & 0,11 & 0,11 & 0,08 & 0,08 \\ 0,59 & 0,20 & 0,58 & 0,63 & 0,19 & 0,17 \\ 0,08 & 0,82 & 0,31 & 0,26 & 0,72 & 0,75 \end{pmatrix} \times \begin{pmatrix} 0,43 \\ 0,03 \\ 0,07 \\ 0,16 \\ 0,20 \\ 0,11 \end{pmatrix} = \begin{pmatrix} 0,19 \\ 0,46 \\ 0,35 \end{pmatrix}$$

Рис. 4. Розрахунок вектору ваг щодо вибору варіантів БпАК

Внаслідок обчислень отримуємо ваги варіантів із точки зору досягнення визначеної мети (табл. 5).

Таблиця 5

**Таблиця вибору варіанту ТА за сукупністю обраних критеріїв (комплексного критерію)**

Варіанти ТА	Вага в долях	Вага у %
ТА-Л	0,19	19%
ТА-Г	0,46	46%
ТА-А	0,35	35%

Отже, згідно із запропонованою методикою та обраними критеріями кращим варіантом виявився ТА на базі БпАК гвинтокрильного типу (ТА-Г), а найгіршим варіантом – ТА на базі БпАК літакового типу (ТА-Л).

Використання цієї методики доцільно розглядати під час створення дослідних зразків ТА підприємствами: Товариство з обмеженою відповідальністю “Укрспецсистемс”; Товариство з обмеженою відповідальністю науково-виробниче підприємство “Spaitech”; Державне підприємство “Чугуївський авіаційний ремонтний завод”; Науково-виробничий центр безпілотної авіації “Віраж”; Державне підприємство “Антонов”.

Кожен із наведених виробників мають досвід розробки БпАК та у випадку отримання ними технічного завдання на виготовлення такого комплексу потенційно спроможні створити БпАК в якості телекомунікаційної аероплатформи, визначеною в постановці завдання у загальному вигляді із необхідними характеристиками та показниками [13].

### **Висновки**

Задача вибору варіанта БпАК для побудови ТА як повітряної складової системи зв'язку ЗС України відноситься до класу багатокритеріальних завдань, що здійснюються в умовах невизначеності з великою кількістю вагомих факторів. Тому, для досягнення мети вибору БпАК для побудови ТА запропоновано методику із застосуванням МАІ на основі вагових коефіцієнтів. Разом із перевагами (масштабованість як за кількістю критеріїв, так і за варіантами вибору, скорочення терміну між постановкою завдання і конкретним результатом) при застосуванні подібних методів варто назвати і недоліки, а саме: необхідно мати групу експертів відповідної кваліфікації в галузі досліджень та суб'єктивність оцінки, що зумовлена людським фактором особистості експерта.

Запропонована авторами методика може знайти своє застосування на підприємствах та в науково-дослідних організаціях, які вирішують завдання, пов'язані з розробкою ТА під задане функціональне призначення та з метою формування вимог та оцінки ефективності на етапі проектування, що може значно зменшити матеріальні та людські ресурси для виконання цього завдання.

**Напрямок подальших досліджень** автори вважають можливість використання запропонованої методики для раціонального вибору обладнання (наприклад, БпАК) для розробки нових протоколів і алгоритмів функціонування самоорганізуючих радіомереж на основі безпілотних літальних апаратів.

### **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Кваша Т. К. Світові наукові та технологічні тренди у сфері забезпечення національної безпеки. Київ: УкрІНТЕІ, 2019. 107 с. URL: <https://mon.gov.ua/storage/app/media/innovatsii-transfer-tehnologiy/2021/09/30/Svitovi.nauk.tekhn.trend.sfer.zabezp.nats.bezp-2019.30.09.pdf> (дата звернення: 27.06.2023).

2. Державний концерн «Укроборонпром» спільно з Генштабом Збройних сил України розробили програму розвитку безпілотних систем для Сил безпеки та оборони нашої держави (дата публікації: 26.08.2022) // Інтернет-портал концерну “Укроборонпром”. URL: <https://ukroboronprom.com.ua/news/ukroboronprom-spilno-z-genstabom-zsu-rozrobili-programu-rozvitku-bpla> (дата звернення: 27.06.2023).

3. Романюк В. А., Степаненко Є. О., Панченко І. В., Восколович О. І. Літаючі самоорганізуючі радіомережі // Збірник наукових праць ВІТІ. 2017. № 1. С. 104–114. URL: <https://journal.viti.edu.ua/index.php/cicst/romaniuk>.

4. Романюк В. А. Мережі MANET – основа побудови тактичних мереж зв'язку // IV науково-практичний семінар ВІТІ “Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”. Київ: ВІТІ НТУУ “КПІ”. 2007. С. 15–28. URL: <https://journal.viti.edu.ua/index.php/cicst/romaniuk>.

5. Бондар Д. В., Гурник А. В., Литовченко А. О., Хижняк В. В., Шевченко В. Л., Ядченко Д. М. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія. Київ, 2022. 312 с.
6. Илюшко В. М. Беспилотные летательные аппараты: методики приближенных расчетов основных параметров и характеристик // В. М. Илюшко, М. М. Митрахович, А. В. Самков и др.; под общ. ред. В. И. Силкова. Киев: ЦНИИ ВВТ ВС Украины, 2009. 302 с.
7. Катеринчук І. С., Балицький І. І. Інформаційна технологія обґрунтування раціональних значень параметрів застосування тактичних безпілотних літальних апаратів органу охорони державного кордону // Теорія та практика створення, розвитку і застосування високотехнологічних систем спеціального призначення з урахуванням досвіду антитерористичної операції: матеріали XXII Всеукраїнської науково-практичної конференції, м. Житомир, Житомирський військовий інститут ім. С. П. Корольова, 26 квітня 2018 р. С. 74–76.
8. Коломійцев О. В., Рябуха Ю. М., Калачова В. В., Третьяк В. Ф. Аналіз методів і процедур шкального оцінювання в задачах прийняття рішень при проектуванні і супроводженні розподілених автоматизованих інформаційних систем // International Forum: Problems and Scientific Solutions: матеріали 3-ї Міжнародної науково-практичної конференції, Австралія, м. Мельбурн, 26–28 квітня 2020 р. С. 250–259. URL: <https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/2309> (дата звернення: 27.06.2023).
9. Поляков А. П., Галушак О. О., Галушак Д. О., Грабенко М. Д. Методика вибору рухомого складу, маршруту і графіка перевезення вантажів. машинобудування та транспорт // Наукові праці Вінницького національного технічного університету. 2011. № 3. С. 1–10. URL: <https://praci.vntu.edu.ua/index.php/praci/article/view/288> (дата звернення: 27.06.2023).
10. Рябцев В. В., Тищенко М. Г. Методика рационального выбора комплекса авторских средств разработки курсов дистанционного обучения // Управляющие системы и машины. 2011. № 4. С. 72–77. URL: <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/82952/10-Riabtsev.pdf?sequence=1> (дата звернення: 27.06.2023).
11. Куцаев В. В., Радченко М. М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла // Збірник наукових праць ВІПІ. Київ, 2018. Вип. 2. С. 67–76. URL: [https://www.viti.edu.ua/index.php?view=coll\\_2018\\_2](https://www.viti.edu.ua/index.php?view=coll_2018_2) (дата звернення: 27.06.2023).
12. Гевко І. Б. Методи прийняття управлінських рішень: підручник. 2009. 186 с.
13. Томас Саати Т. Принятие решений – Метод анализа иерархий. М.: Радио и связь, 1993. 320 с.
14. Lav Gupta, Raj Jain, Gabor Vaszkun Survey of Important Issues in UAV Communication Networks, IEEE Communications Surveys and Tutorials, Volume PP, November 2015. DOI: 10.1109/COMST.2015.2495297.

УДК 004.932.2

Легкобит В. С. ORCID: 0000-0002-9118-4188 (ВІТІ ім. Героїв Крут)  
Стоцький І. В. ORCID: 0000-0002-5898-3228 (ВІТІ ім. Героїв Крут)  
Карпенко А. О. ORCID: 0000-0002-8372-6303 (ВІТІ ім. Героїв Крут)

## ПІДВИЩЕННЯ ТОЧНОСТІ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ НА МІСЦЕВОСТІ НА ОСНОВІ ПОЄДНАННЯ СЕНСОРНИХ МОДАЛЬНОСТЕЙ ІЗ ВИКОРИСТАННЯМ БІНАРНОЇ КРОСЕТРОПІЇ ЯК ФУНКЦІЇ ВТРАТ

У сучасних умовах ведення бойових дій надзвичайної важливості набуло програмне забезпечення, в основу якого покладено техніку машинного навчання для виявлення та класифікації об'єктів інфраструктури на місцевості. У зв'язку з цим актуальним постає завдання підвищення точності класифікації об'єктів на місцевості, оскільки застосування безпілотних літальних апаратів (далі – БпЛА) та космічних систем є життєво важливим для ведення розвідувальної діяльності. Враховуючи характер вхідних даних, а саме статичні зображення місцевості, отримані у вигляді супутникових знімків та знімків з камер БпЛА, для вирішення завдань класифікації доцільно застосовувати згорткові нейронні мережі. У більшості випадків супутникові знімки представлені у вигляді мультиспектральних та гіперспектральних зображень, тому для навчання моделі були використані загальнодоступні набори даних, що запропоновані спільнотою дослідників SpaceNet. Важливим етапом підготовки навчальної вибірки є орторектифікація зображень, а саме додавання інформації про 3D-поверхню до зображень, що надає моделі важливу геометричну інформацію для семантичних класів, таких як будівлі та інші споруди, виправляє геометричні спотворення та сприяє навчанню моделі розпізнавати об'єкти в узгодженому геопросторовому контексті. Під час експериментів було проведено навчання моделі SegNet із використанням *normalized Digital Surface Model (nDSM)* та без неї. Результати експериментів демонструють, що узагальнена точність класифікації для шести класів об'єктів на тестовому наборі даних зростає на 23,9%. А експерименти з обмеженням навчальної вибірки продемонстрували, що за потреби достатньо використати половину доступного тренувального набору даних для отримання лише на 4% нижчої точності класифікації та заощадження близько 10 годин навчання.

**Ключові слова:** згорткові нейронні мережі, класифікація, орторектифікація.

**V. Legkobyt, I. Stotskiy A. Karpenko Improving the accuracy of object classification on the ground based on a combination of sensory modalities using binary cross-tropism as a loss function.**

In today's warfare environment, software based on machine learning techniques for detecting and classifying infrastructure objects on the ground has become extremely important. In this regard, the task of improving the accuracy of classification of objects on the ground is becoming more urgent, as the use of UAVs and space systems is vital for intelligence activities. Given the nature of the input data, namely static terrain images obtained in the form of satellite images and UAV camera images, it is advisable to use convolutional neural networks to solve classification problems. In most cases, satellite images are presented in the form of multispectral and hyperspectral images, so publicly available datasets offered by the SpaceNet research community were used to train the model. An important step in preparing the training set is image orthorectification, namely adding 3D surface information to the images, which provides the model with important geometric information for semantic classes such as buildings and other structures, corrects geometric distortions, and helps the model to recognize objects in a consistent geospatial context. In the course of the experiments, the SegNet model was trained with and without the *normalized Digital Surface Model (nDSM)*. The experimental results show that the generalized classification accuracy for six classes of objects on the test dataset increases by 23.9%. And experiments with training set limitation demonstrate that, if necessary, it is enough to use half of the available training data set to obtain only 4% lower classification accuracy and save about 10 hours of training.

**Keywords:** convolutional neural networks, classification, orthorectification.

### Постановка завдання в загальному вигляді

Досвід застосування космічних систем та безпілотних авіаційних комплексів (далі – БпАК) в останніх конфліктах чітко вказує на трансформацію способів ведення війни, зокрема активне ведення інформаційної війни. Аналіз застосування засобів і систем різних видів розвідки у воєнних конфліктах останніх десятиліть показали, що близько 70% розвідувальної інформації про наземні об'єкти противника отримано за допомогою космічних апаратів та БпЛА з використанням великої кількості фотографічних, оптико-електронних, радіолокаційних тепловізійних приладів [1].

Отримані актуальні дані дозволятимуть відповідним аналітичним підрозділам Збройних Сил України (далі – ЗС України) за демаскуючими ознаками робити висновки щодо ймовірних локацій (об'єктів, районів, напрямків) інтересу противника та ймовірних цілей для систем і комплексів високоточного керованого ракетного озброєння. Використання зазначеної інформації у ЗС України дозволить знизити втрати з боку особового складу, зберегти озброєння та військову техніку, завчасно визначати наміри противника, тим самим, в цілому, здійснювати більш ефективну протидію атакам противника [2].

На точність класифікації цільових об'єктів суттєво впливають фактори, що природним чином виникають внаслідок різноманітності зовнішнього вигляду, кутів огляду, умов навколишнього середовища, широкий спектр часових та просторових варіацій тощо. Усунення негативного впливу вищезазначених факторів на точність класифікації у більшості випадків досягається шляхом:

залучення попередньо навчених моделей на великих наборах даних (наприклад, ImageNet [3]);

виокремлення релевантних особливостей необроблених даних перед завантаженням їх у модель;

застосування методів перехресної перевірки, але з точки зору технічної реалізації ці підходи потребують значних апаратних і часових ресурсів.

Отже, актуальним постає завдання аналізу впливу на точність класифікації таких підходів до машинного навчання, як розширення навчальної вибірки завдяки збільшенню кількості анованих слідів об'єктів для усунення дисбалансу класів, мультимодальне злиття даних із різних джерел, налаштування гіперпараметрів та адаптація до предметної області шляхом застосування синтетичних даних.

Оскільки не існує універсальної архітектури нейронної мережі для класифікації об'єктів на місцевості, увагу слід зосередити на пошуку адаптивних рішень на основі модифікації вхідних даних стосовно особливостей конкретних завдань класифікації, бажаної точності.

**Аналіз останніх публікацій.** Дослідженню підходів до машинного навчання з метою пошуку способів оптимізації параметрів моделей нейронних мереж для класифікації об'єктів на місцевості присвячена значна кількість робіт, аналіз основних із яких викладено нижче.

У роботі [4] проведено дослідження значення різних модальностей та їх поєднання для аналізу геопросторових даних низької просторової роздільної здатності. У роботі представлено математичну модель, що дозволяє збагачувати геопросторові дані додатковою семантикою на основі заданої інформації про колір, гіперспектральної інформації та інформації про форму. Для визначення векторів ознак та класифікації використовувався класифікатор випадкового лісу. Отримані результати демонструють, що сама собою інформація про форму має досить обмежену цінність для вилучення семантичної інформації, якщо просторова роздільна здатність є відносно низькою і якщо визначені користувачем класи виявляють подібну геометричну поведінку локальної структури.

У роботі [5] проведено дослідження щодо ідентифікації слідів будівель у програмах дистанційного зондування місцевості з використанням у якості джерел вхідних даних 3D-лідарів та комерційних супутників. У роботі описано результати змагань фахівців із машинного навчання, таких як USSOCOM Urban 3D, DSTL Satellite Imagery Feature Detection Challenge та ISPRS Test Project on Urban Classification, переможці яких у своїх рішеннях використовували архітектури нейронних мереж LinkNet та UNet із модифікованими кодерами ResNet18, 34, 50 та VGG16. Узагальнюючи особливості підходів до вирішення завдань класифікації в рамках вищезазначених змагань, варто зазначити наступне: для усунення упередженості моделі дані для тренування було обрано випадковим чином у різних пропорціях відносно загальної вибірки, фаза тренування проходила різну кількість епох та з різними швидкостями, застосування методів ортогональної та випадкової ініціалізації wag

нейронної мережі та експерименти з різними пороговими значеннями для алгоритму сегментації зображень. Але поза увагою залишилися більш доцільні методи ініціалізації ваг мережі, такі як ініціалізація Ксав'є-Глорота, що встановлює ваги на основі кількості вхідних та вихідних нейронів і масштабує випадкові ваги на коефіцієнт, який гарантує, що дисперсія активацій залишається приблизно однаковою між шарами та ініціалізація LeCun, яка часто використовується для активацій Leaky ReLU та Scaled Exponential Linear Units (SELU) і також встановлює ваги на основі кількості вхідних і вихідних нейронів із різним коефіцієнтом масштабування.

У роботі [6] розглядається глибока семантична сегментація аерофотознімків на основі мультимодальних даних з урахуванням відповідних цифрових моделей поверхні, створених на основі радіометричних та геометричних характеристик, які надаються окремо та в різних комбінаціях як вхідні дані для Depthwise Separable Convolutional Neural Network (DSCNN), модифікованої шляхом застосування функцій масштабування, отриманих із проміжних рівнів SCNN. Отримані результати демонструють, що масштабування та глибинна згортка сприяють покращенню продуктивності сегментації зображень, особливо для груп об'єктів, але не підвищують точність класифікації окремих об'єктів. Загалом, DSCNN забезпечують ефективний і дієвий спосіб побудови глибоких нейронних мереж для задач комп'ютерного зору, одночасно вирішуючи проблеми, пов'язані з розміром моделі та обчислювальними витратами. Вони знайшли застосування в мобільних і вбудованих системах, комп'ютерному зору в реальному часі та інших сценаріях, де ефективність використання ресурсів має вирішальне значення.

У роботі [7] Data Scientist компанії Capella Space, що є партнером SpaceNet LLC, Jake Shermeyer опублікував результати переможців змагань "SpaceNet 6 мультисенсорне всепогодне картографування". В рамках даного змагання учасникам у якості вхідних даних були запропоновані принципово нові сенсорні модальності у вигляді даних Synthetic Aperture Radar (SAR) та півметрових електрооптичних зображень із супутника Maxar WorldView 2. Метою змагання було автоматично отримувати сліди будівель за допомогою комп'ютерного зору та алгоритмів штучного інтелекту (ШІ), використовуючи комбінацію вищезазначених даних. Незважаючи на те, що результат переможця змагань стосовно точності розпізнавання слідів будівель становить лише 42,423 %, його можна вважати успішним, враховуючи, що дані SAR були зібрані з точки зору поза надіром із усередненням  $\sim 35^\circ$ , що є одним із найскладніших аспектів, присутніх у спостереженні Землі. Показники точності виявлення слідів будівель підкреслюють проблеми, пов'язані з входженням у нову модальність, і демонструють, що необхідні подальші дослідження для повного використання домену SAR. Стосовно архітектурних рішень та підходів учасників варто зазначити використання таких ансамблевих методів, як Bootstrap Aggregating, AdaBoost, Gradient Boosting та Dropout Regularization, виключення оптичних даних із набору даних для попереднього навчання, застосування багатоканальних масок для сегментації зображень. Ці підходи показують, що іноді навіть незначні етапи попередньої обробки можуть бути особливо цінними для покращення продуктивності та мінімізації деяких складнощів.

У роботі [8] представлено новий підхід до підвищення продуктивності нейромережевих класифікаторів. У традиційних нейромережевих класифікаторах центроїди (репрезентативні точки) фіксуються в просторі розбиття перед навчанням. Дані центроїди мають вирішальне значення для створення меж розбиття між класами. Однак такий фіксований підхід обмежує потенційні конфігурації нейронної мережі, оскільки він обмежує форму меж прийняття рішень. Запропонований авторами підхід поєднує класифікацію за методом найближчого сусіда з нейромережевим класифікатором. На відміну від традиційних методів із фіксованими центроїдами та сфероподібними розділами, використання найближчих сусідів дозволяє більш гнучко визначати межі рішень. Методи найближчих сусідів можуть адаптуватися до шаблонів

даних і створювати кордони довільної форми в просторі розбиття. Експериментальні результати показують, що цей новий підхід працює краще з погляду точності та середньої F-міри порівняно з існуючими методами. Іншими словами, поєднання класифікації за методом найближчого сусіда з нейронними мережами призводить до покращення результатів класифікації, особливо у випадках, коли потрібні складні та неоднорідні межі розбиття. Отже, у роботі представлено новий підхід до нейромережевої класифікації, який використовує гнучкість методу найближчого сусіда для створення більш ефективних меж прийняття рішень довільної форми. Експериментальні результати підтверджують ефективність цього підходу в підвищенні точності та достовірності класифікації.

У роботі [9] представлено метод нечітких плаваючих центроїдів (МНПЦ), який має на меті покращити продуктивність нейромережевого класифікатора. Традиційні нейромережеві класифікатори з плаваючими центроїдами часто мають фіксовані межі прийняття рішень, що може призводити до ексклюзивного розподілу класів, особливо для зашумлених або граничних точок, це призводить до неправильної класифікації і впливає на навчання нейронних мереж. Щоб вирішити цю проблему, МНПЦ вводить нечітку стратегію разом із плаваючими центроїдами для створення нечітких меж прийняття рішень. Нечіткі межі дозволяють точкам даних мати ступінь приналежності до декількох класів, що робить його більш гнучким і здатним обробляти зашумлені та граничні точки. Ця гнучкість збільшує ймовірність знаходження оптимальної конфігурації нейронної мережі під час оптимізації. Крім того, МНПЦ використовує зважену цільову функцію для обробки незбалансованих даних, надаючи більше значення класам меншин. Це допомагає покращити обробку незбалансованих наборів даних. Ефективність МНПЦ оцінено на 32 еталонних наборах даних за допомогою таких показників, як середня F-міра та точність узагальнення. Результати експерименту показують, що МНПЦ досягає заданої точності узагальнення на 17 наборах даних і оптимальної F-міри на 21 наборі даних, перевершуючи інші методи класифікації. МНПЦ особливо ефективний у балансуванні між точністю та запам'ятовуванням, що робить його підходящим вибором для таких завдань, як оцінка класів на основі мікроструктурних зображень. Отже, МНПЦ – це метод, який поєднує нечітку логіку і плаваючі центроїди для створення нечітких меж прийняття рішень в нейромережевій класифікації. Експериментальні результати демонструють його перевагу над іншими методами, особливо в обробці незбалансованих даних і балансуванні точності та запам'ятовуванні для конкретних застосувань.

У роботі [10] розглядаються дві проблеми: проблема дисбалансу в класифікації та обробка матричних образів без векторизації, для вирішення яких автори пропонують новий метод Entropy-based Matrix Learning Machine with MatMHS and Fuzzy Membership Evaluation (EMatMHS). Замість перетворення матричних шаблонів у вектори, автори пропонують використовувати в якості базового класифікатора Matrix-pattern-oriented Ho-Kashyap learning machine with regularization learning (MatMHS). Даний підхід є актуальним для ефективної обробки матричних шаблонів. Для вирішення проблеми дисбалансу автори представляють підхід до оцінки нечіткої приналежності на основі ентропії. Цей підхід використовує ентропію як міру визначеності класу для визначення нечіткої належності навчальних моделей. Шаблони з вищою ентропією можуть мати нижчу приналежність, що відображає невизначеність щодо їхнього класу. У роботі проведено оцінку запропонованого методу EMatMHS із використанням реальних незбалансованих наборів даних порівняно з такими підходами до попередньої обробки, як Synthetic Minority Over-sampling Technique (SMOTE), Adaptive Synthetic Sampling machine learning technique (ADASYN), Cluster Based Synthetic Oversampling (CBSO). Результати показують, що EMatMHS перевершує порівнювані підходи з точки зору точності класифікації, особливо для незбалансованих наборів даних. Отже, EMatMHS

представлено як рішення, яке може ефективно обробляти як незбалансовані дані, так і матричні патерни.

У роботі [11] представлено підхід для вирішення проблеми незбалансованих наборів даних у нейронних мережах, що полягає в інтеграції попередніх ймовірностей у функцію перехресної ентропійної помилки, чутливої до втрат. Щоб оцінити ефективність цього методу, дослідники провели експерименти на декількох встановлених еталонних наборах даних, використовуючи різні метрики оцінки, такі як G-середнє, площа під ROC-кривою (AUC), скориговане G-середнє, точність, істинно позитивна частота, істинно негативна частота і F1-бали. У дослідженні порівнювалися результати, отримані за допомогою цього нового підходу, з результатами відомих алгоритмів. Результати продемонстрували ефективність і стійкість запропонованого методу, особливо в сценаріях із незбалансованими наборами даних. Підхід виявився успішним у створенні добре збалансованих класифікаторів, вирішуючи проблеми, пов'язані з різним ступенем незбалансованості даних.

У роботі [12] Основною концепцією є представлення та пояснення SegNet архітектури, призначеної для семантичної попиксельної сегментації. Автор обговорює мотивацію створення SegNet, підкреслюючи необхідність точного зіставлення об'єктів низької роздільної здатності з вхідною роздільною здатністю для попиксельної класифікації. Її порівнюють з іншими архітектурами сегментації (FCN, DeepLab-LargeFOV та DeconvNet.), висвітлюючи компроміси між використанням пам'яті та точністю. У статті оцінюється продуктивність SegNet у задачах сегментації сцени і підкреслюються її можливості в реальному часі, особливо для автономного водіння. Отже, враховуючи переваги даної архітектури з точки зору продуктивності та практичного застосування у сценаріях реального часу, доцільно застосовувати її для класифікації об'єктів на місцевості.

Враховуючи потенційний успіх фахівців із машинного навчання у підвищенні точності класифікації об'єктів на місцевості, залишається ряд недоліків, які суттєво впливають на різницю між фактичними та очікуваними результатами щодо вирішення завдань класифікації об'єктів на місцевості. До них варто віднести дисбаланс класів, ініціалізацію ваг нейронної мережі, інтеграцію додаткових модальностей, забезпечення стійкості моделей до шуму та мінливості умов навколишнього середовища. Комбінування запропонованих в аналізі методів попередньої обробки даних та параметризації моделей нейронних мереж дозволить мінімізувати різницю між фактичними та очікуваними показниками точності класифікації об'єктів на місцевості.

**Метою статті** є підвищення точності класифікації об'єктів на місцевості на основі поєднання сенсорних модальностей із використанням бінарної кросентропії як функції втрат в умовах обмеженої навчальної вибірки.

Авторами статті пропонується синергетичний підхід, який базується на використанні архітектури SegNet, представленої на рисунку 1, розробленої для задач семантичної сегментації, оскільки ця архітектура передбачає віднесення кожного пікселя зображення до одного з декількох попередньо визначених класів об'єктів, забезпечуючи детальне розуміння сцени.

Серед структурних особливостей даної архітектури варто відзначити використання шару  $\text{softmax}$  у кінці декодера, щоб призначити ймовірності класів кожному пікселю, створюючи остаточну карту сегментації. Однією з відмінних рис архітектури SegNet є використання індексів під час об'єднання шарів у кодері. Замість того, щоб зберігати фактичні значення пікселів у цих індексах, SegNet зберігає індекси максимальних значень у кожній області об'єднання. Ця інформація має вирішальне значення для збільшення вибірки у декодері.



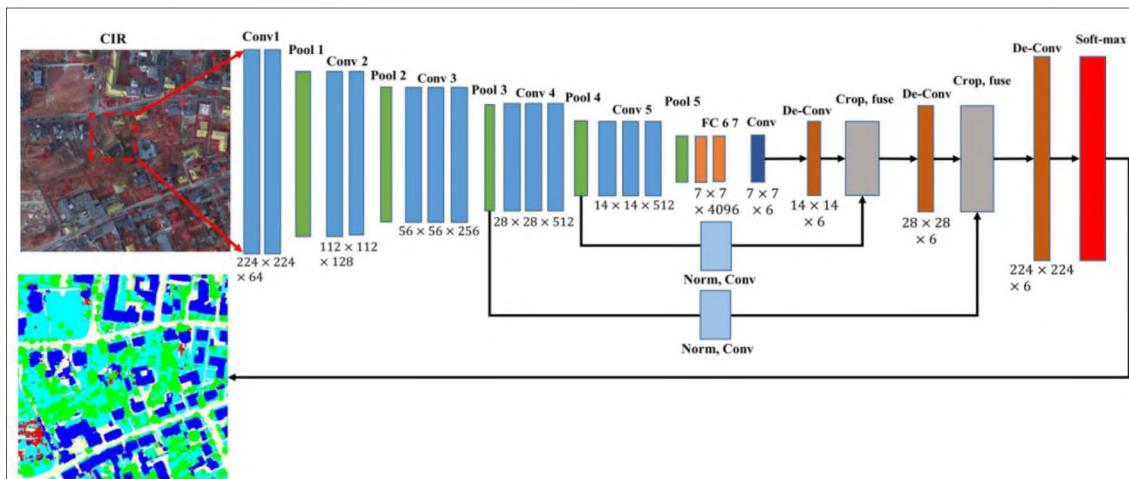


Рис. 1. Архітектура SegNet зі структурою кодер-декодер

Враховуючи попередню навченість моделі на наборі даних ImageNet, залишається необхідним донавчання моделі з метою адаптації під конкретні умови застосування. Набори даних для донавчання та тестування були отримані з репозиторію <https://registry.opendata.aws/spacenet>, вони містили багаторакурсні супутникові знімки високої роздільної здатності, що використовувались у рамках проекту USSOCOM Urban 3D Challenge та аерофотознімки, опубліковані Міжнародним товариством фотограмметрії (ISPRS). Кожен із 144 знімків місцевості містить приблизно 157 000 анотованих контурів будівель, має розмір 2048×2048 пікселів і займає площу приблизно 4 кв. км (рис. 2).

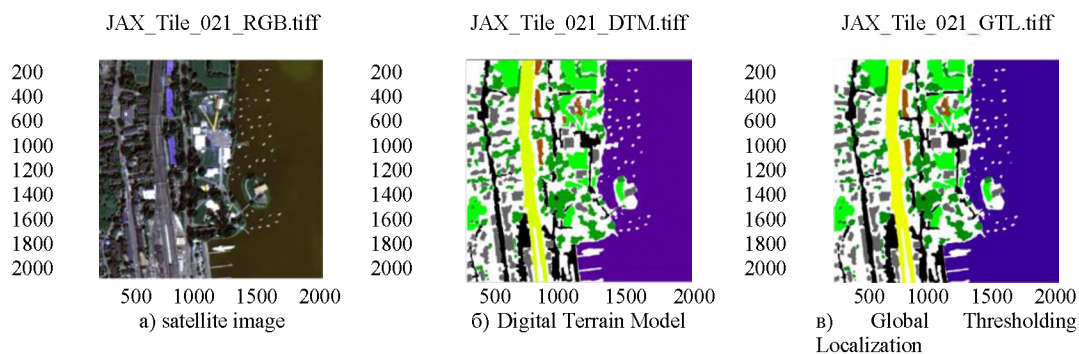


Рис. 2. Зразок зображення з USSOCOM Urban 3D Challenge dataset

Геометрична корекція зображень була здійснена шляхом виправлення геометричних спотворень, спричинених варіаціями рельєфу та кривизною Землі за допомогою ground control points (GCP). Інтеграція даних про висоту об'єктів необхідна з метою налаштування перспективи зображень відповідно до рельєфу місцевості, які в подальшому використовуються для генерації nDSM. Інформація nDSM створюється шляхом щільного зіставлення зображень за допомогою програмного забезпечення Trimble INPHO 5.3. 32-бітові рівні сірого використовуються для кодування висоти та зберігаються у файлі формату TIFF.

У підсумку було сформовано три навчальні вибірки з набору даних USSOCOM, до першої увійшли гіперспектральні орторектифіковані RGB зображення, до другої – nDSM, композитні зображення RGB + nDSM до третьої, та три навчальні вибірки з набору даних ISPRS, до першої увійшли мультиспектральні зображення IRRG, до другої – nDSM та композитні зображення IRRG + nDSM до третьої відповідно. Співвідношення розподілу

становило 70 % для навчання, 15 % для перевірки і 15 % для тестування від загального набору даних.

Налаштування моделі SegNet містить конфігурацію її архітектури, вхідних вимірів, вихідних класів, функції активації, функції втрат, оптимізатора, параметрів навчання, методів регуляризації, метрик оцінювання, а також проведення навчання і тестування. Враховуючи використання попередньо-навченої моделі на великому наборі даних ImageNet, що дозволило моделі вивчити корисні ієрархічні особливості, які можна використовувати для конкретних задач класифікації об'єктів, залишалось провести точне налаштування та оновлення вагових коефіцієнтів моделі відповідно до визначеного набору даних, а також застосувати функцію втрат на основі бінарної перехресної ентропії для попиксельної класифікації, у зв'язку з тим, що дана функція вимірює розбіжність між прогнозованими ймовірностями класів та істинними мітками. У налаштуваннях бінарного та багатокласового класифікатора однією з основних цілей оптимізації є мінімізація функції втрат на основі двовимірної бінарної перехресної ентропії (1).

$$\theta_b^* = \arg \min_{\theta \in \Theta} \left( - \sum_{i=1}^m \sum_{j=1}^n Y_{i,j} \log(P(X; \theta)_{i,j}) + (1 - Y_{i,j}) \log(1 - P(X; \theta)_{i,j}) \right), \quad (1)$$

де  $Y_{i,j} \in \{0, 1\}$  і  $P(X; \theta)_{i,j} \in [0, 1]$  позначають основні істинні та передбачені мітки відповідно у пікселі  $(i, j)$  для кожного фрагмента навчального зображення;  $X$  позначає вхідні функції (1-, 3- або 4-канальне зображення).  $X$  і  $Y$  індексуються як двовимірні масиви з (висотою, шириною), заданими як  $(m, n)$ .

Мультикласовий класифікатор зводить до мінімуму аналогічне завдання пошуку параметрів  $\Theta_m^*$  (2), за винятком того, що замість розгляду одного класу, наприклад, будівля, цей класифікатор робить попиксельні прогнози з кількох класів. Цей класифікатор навчається шляхом мінімізації наступної задачі, яка відповідає негативній попиксельній логарифмічній правдоподібності за  $N$  класами.

$$\theta_m^* = \arg \min_{\theta \in \Theta} \left( - \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^N Y_{i,j,k} \log(P(X; \theta)_{i,j,k}) \right), \quad (2)$$

де  $Y_{i,j,k} \in \{0, 1\}$  і  $P(X, \theta)_{i,j,k} \in [0, 1]$  позначають основні істинні та передбачені мітки відповідно в пікселі  $(i, j)$  для класу  $k \in \{0, 1, \dots, N\}$  для кожного навчального зображення  $X$ , яке індексується як двовимірний масив форми  $(m, n)$ . Щоб зробити оптимальні прогнози семантичної сегментації, використовується метод градієнтного спуску для ітеративного рішення для набору ваг  $\theta$ , які мінімізують цілі, представлені вище.

До того ж обчислення поелементної крос-ентропійної втрати для кожного пікселя зображення необхідно зважити кожен піксель, використовуючи його зворотну частоту класу, тобто якщо клас  $i$  зустрічається в наборі даних із часткою  $f_i \in (0, 1]$ , то вага визначається так:  $w_i = 1/f_i$ . Даний вираз визначення ваг використовується для виправлення дисбалансу класів у наборах даних та відповідає зваженій негативній логарифмічній правдоподібності або виваженій меті крос-ентропії. Використання виваженої функції вартості дозволяє вивчити класифікатор, не орієнтований на найбільш поширений клас. Отже виважена бінарна та багатокласова класифікація виглядатиме так (3), (4):

$$\theta_{b,w}^* = \arg \min_{\theta \in \Theta} \left( - \sum_{i=1}^m \sum_{j=1}^n w(Y_{i,j}) (Y_{i,j} \log(P(X; \theta)_{i,j}) + (1 - Y_{i,j}) \log(1 - P(X; \theta)_{i,j})) \right), \quad (3)$$

де  $w(Y_{i,j})$  позначає вагу, присвоєну пікселю  $(i, j)$  на основі його основного класу істинності  $Y_{i,j}$ . Слід зауважити, що  $Y_{i,j} \in \{0, 1\}$ .

$$\theta_{m,w}^* = \arg \min_{\theta \in \Theta} \left( - \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^N w(c_{i,j}) Y_{i,j,k} \log(P(X; \theta)_{i,j,k}) \right), \quad (4)$$

де  $w(c_{i,j})$  позначає вагу, присвоєну пікселю  $(i,j)$  на основі його основного класу істинності  $c_{i,j}$ . Відповідно для позначення класу використовується  $c_{i,j} \in \{0, 1, \dots, N\}$ , а не  $Y_{i,j,k} \in \{0, 1\}$ . Описаний вище математичний апарат представлено у [13].

Процес навчання, як правило, передбачає ітерації над усім навчальним набором даних протягом заданої кількості епох або до досягнення збіжності. Кожна епоха являє собою один повний прохід через набір даних, під час якого вхідні ділянки зображення подаються в модель SegNet, модель обчислює попиксельні карти ймовірностей класів, а втрати бінарної перехресної ентропії обчислюються шляхом порівняння прогнозованих ймовірностей класів із відповідними істинними мітками. Зворотне розповсюдження відбувається шляхом обчислення градієнтів відносно втрат, і ваги моделі відповідно оновлюються за допомогою зворотного оптимізатора, який підлаштовує ваги моделі для мінімізації функції втрат. Безперервна перевірка продуктивності моделі SegNet на валідаційному наборі даних під час навчання здійснюється з метою відстеження надмірного припасування і гарантує, що модель добре узагальнює раніше невидимі дані.

У рамках першого експерименту мережа була навчена з використанням пар ділянок вхідних зображень з набору ISPRS і відповідних базових карт міток, які містили шість анотованих класів об'єктів. Час навчання становив приблизно 20 годин. За результатами цього експерименту встановлено, що наявність додаткових модальностей в умовах узгодженого геопросторового контексту майже не впливає на продуктивність класифікації, підвищуючи показники точності для деяких класів об'єктів лише на 0,5 %. Але зовсім інша ситуація спостерігається під час класифікації об'єктів на раніше небаченій місцевості. Узагальнена точність класифікації поза вибіркою зростає на 23,9 % порівняно з випадком IRRG та на 17,1 % порівняно з випадком nDSM (табл. 1).

Таблиця 1

Результати дослідження для набору даних ISPRS

Класи об'єктів	segnet (isprs)					
	validation dataset			test dataset		
	ndsm	irrg	ndsm & irrg	ndsm	irrg	ndsm & irrg
Непроникні поверхні	0,8727	0,9520	<b>0,9531</b>	0,7127	0,7502	<b>0,8374</b>
Будинки	0,9549	0,9638	<b>0,9722</b>	0,6828	0,4571	<b>0,7886</b>
Низька рослинність	0,8486	0,9199	<b>0,9243</b>	0,7320	0,7829	<b>0,8589</b>
Дерева	0,9159	<b>0,9488</b>	0,9473	<b>0,8846</b>	0,8568	0,8643
Авто	0,9922	<b>0,9969</b>	0,9959	0,9865	0,9879	<b>0,9912</b>
Інші об'єкти	0,9995	0,9993	<b>0,9996</b>	0,9518	<b>0,9598</b>	0,9522
Разом	0,7919	<b>0,9003</b>	0,8962	0,4752	0,3974	<b>0,6463</b>

Другий експеримент проводився для набору даних USSOCOM із використанням кількісних метрик бінарної класифікації, таких як точність, прецизійність, повнота, а також частота хибнонегативних та хибнопозитивних результатів. Результати експерименту демонструють, що класифікатори, навчені за допомогою інформації RGB та nDSM, у середньому мають на 6 % вищу точність поза вибіркою, ніж класифікатори, навчені лише інформацією RGB. Ці результати підтверджують те, що інформація nDSM сприяє більшій узагальнюваності класифікатора порівняно з лише інформацією RGB для вирішення завдань класифікації (табл. 2).

Таблиця 2

## Результати дослідження для набору даних USSOCOM

Метрики класифікації	segnet (ussocom)					
	validation dataset			test dataset		
	ndsm	rgb	ndsm & rgb	ndsm	rgb	ndsm & rgb
Точність	0,9164	0,9298	<b>0,9367</b>	0,8690	0,8739	<b>0,9386</b>
Прецизійність	0,9245	0,9412	<b>0,9451</b>	0,9425	0,9416	<b>0,9512</b>
Повнота	0,9105	0,9245	<b>0,9341</b>	0,8122	<b>0,9307</b>	0,9298
Хибнонегативні	0,0895	0,0755	<b>0,0659</b>	0,1878	<b>0,0693</b>	0,0702
Хибнопозитивні	0,0829	0,0643	<b>0,0604</b>	0,0610	0,0626	<b>0,0518</b>

Враховуючи результати попередніх експериментів, очевидним є те, що RGB + nDSM забезпечує найкращу кореляцію з фактичною інформацією про місцевість. Це обумовлено тим, що інформація про висоту допомагає розрізняти об'єкти зі схожими спектральними характеристиками, але різною висотою, наприклад, будівлі або дерева, забезпечує зменшення надмірності даних. Покращена дискримінація nDSM допомагає розрізняти об'єкти, які мають однакову спектральну сигнатуру на стандартних знімках, наприклад, різні типи дахів, дорожніх покриттів або рослинного покриву на основі їхніх висотних профілів. Важливим аспектом проведення експериментів було тренування моделі з обмеженими наборами даних, адже не завжди є можливість використовувати достатню кількість даних з адекватним поданням і кутами огляду для всіх об'єктів, що цікавлять, особливо для завдань, в яких критичним ресурсом виступає час. У таблиці 3 показано результати навчання класифікаторів з 15 %, 25 %, 50 % та 100 % від загального тренувального набору даних (TDS) із проміжним контролем за допомогою зображень із валідаційного набору даних (VDS).

Таблиця 3

## Результати аналізу впливу обмеження вибірки на точність класифікації

Пропорції	Точність класифікації					
	In city				Out of city TDS	
	VDS		TDS		+ nDSM	- nDSM
	+ nDSM	- nDSM	+ nDSM	- nDSM		
15 %	0,9054	0,9003	0,8356	0,8263	<b>0,5336</b>	0,2258
25 %	0,9121	0,9174	0,8649	0,7982	0,4159	0,4367
50 %	0,9215	0,9211	0,8923	0,8815	0,4677	0,3917
100 %	<b>0,9367</b>	<b>0,9298</b>	<b>0,9386</b>	<b>0,9339</b>	0,5112	<b>0,4729</b>

Результати розпізнавання об'єктів на пересіченій місцевості показують, що існує помірна позитивна кореляція між часткою використаних даних і точністю. Це свідчить про те, що використання лише 50 % даних може бути достатнім для відносно точної класифікації. При оцінці точності в межах валідаційного набору даних для міських районів спостерігається негативна кореляція між розміром підмножини набору даних і точністю. Це означає, що зі зменшенням розміру підмножини даних точність у цій підмножині також має тенденцію до зниження. Це спостереження може бути пов'язане з тим, що нейронна мережа має менше зразків для навчання, що ускладнює її адаптацію до навчальної вибірки. Що стосується раніше небачених зображень, то тут також спостерігається негативна кореляція між точністю та часткою навчального набору даних, це свідчить про те, що використання лише RGB-даних може призвести до надмірного припасування, коли модель добре працює на навчальних даних, але не може узагальнити їх для нових міст чи районів.

**Висновки.** У статті вирішується завдання підвищення точності класифікації об'єктів на місцевості завдяки комбінуванню існуючих методів попередньої обробки даних та параметризації моделей нейронних мереж. Фахівці з машинного навчання здебільшого концентрують свої зусилля на вирішенні специфічних актуальних прикладних задач щодо покращення конкретних аспектів продуктивності нейронних мереж.

Проведено аналіз існуючих підходів до машинного навчання з метою пошуку способів оптимізації параметрів моделей нейронних мереж для класифікації об'єктів на місцевості, серед яких варто зазначити: вплив мультимодального поєднання даних (nDSM, SAR) на точність класифікації об'єктів на місцевості в умовах обмеженої навчальної вибірки; використання попередньо навчених моделей нейронних мереж (LinkNet, UNet, SegNet) та архітектур (DSCNN, EMatMHKS); використання класифікаторів нейронних мереж на основі методів найближчого сусіда та нечітких плаваючих центроїдів та двовимірної бінарної кросентропії.

Результати проведеного аналізу підходів до підвищення точності класифікації об'єктів на місцевості демонструють вплив модальності nDSM на точність класифікації, особливо в умовах обмеження навчальних даних, а класифікатор на основі бінарної кросентропії дозволяє усунути вплив дисбалансу класів на точність класифікації.

Запропоновано синергетичний підхід на основі моделі SegNet, навченої на попередньо орторектифікованих зображеннях, у поєднанні з nDSM для навчання моделі розпізнавати об'єкти в узгодженому геопросторовому контексті та використанні класифікаторів на основі двовимірної бінарної кросентропії, що дозволило усунути вплив дисбалансу класів на точність класифікації об'єктів на місцевості.

Результати експериментів, наведені у таблицях 1–3, демонструють, що узагальнена точність класифікації для шести класів об'єктів на тестовому наборі даних зростає на 23,9 % порівняно з випадком IRRG та на 17,1 % порівняно з випадком nDSM. Класифікатори, навчені за допомогою інформації RGB та nDSM, у середньому мають на 6 % вищу точність поза вибіркою, ніж класифікатори, навчені лише інформацією RGB. А експерименти з обмеженням навчальної вибірки продемонстрували, що за потреби достатньо використати половину доступного тренувального набору даних для отримання лише на 4 % нижчої точності класифікації та заощадження близько 10 годин навчання.

Отже, на великих і добре відомих наборах даних SegNet є конкурентоспроможною, досягаючи високих показників точності, особливо з використанням інформації про тривимірну поверхню та в умовах обмеженої навчальної вибірки.

**Напрямок подальших досліджень** є удосконалення існуючих методів впливу на метрику Каппа Коена, яка використовується для оцінки збігу між прогнозованою та фактичною класифікаціями, враховуючи при цьому збіг, який може виникнути випадково

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Козуб А. М., Шумейко В. О., Зуйко В. В., Ніколаєнко О. Є. Аналіз досвіду використання космічних систем та безпілотних авіаційних комплексів в сучасних локальних конфліктах та перспективи їх розвитку // НУОУ. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. № 3 (33).
2. Епішев В. П., Мотрунич І. І., Періг В. М., Кудак В. І., Найбауер І. Ф., Сухов П. П., Кашуба В. І., Сухов К. П., Варламов І. Д., Албул В. В., Москаленко С. С., Мисливий С. О. Можливості національних оптичних засобів спостереження за космічним простором щодо контролю геостационарної орбіти у інтересах збройних сил України // НУОУ. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. № 3 (33).
3. ImageNet: website. URL: <https://www.image-net.org/index.php>.
4. M. Weinmann and M. Weinmann. Geospatial computer vision based on multi-modal data. 2018. DOI: 10.3390/rs10010002.
5. Goldberg H., Brown M. and Wang S. A benchmark for building footprint classification using orthorectified rgb imagery and digital surface models from commercial satellites. Proceedings of IEEE applied imagery pattern recognition workshop. 2017. DOI: 10.1109/AIPR.2017.8457973.
6. Chen K., Weinmann M., Gao X., Yan M., Hinz S., Jutzi B. and Weinmann M. Residual shuffling convolutional neural networks for deep semantic image segmentation using multi-modal data. ISPRS annals

of photogrammetry, remote sensing & spatial information sciences. 2018. DOI: 10.5194/isprs-annals-IV-1-29-2018.

7. Medium: website. URL: <https://medium.com/the-downlinq/spacenet-6-announcing-the-winners-df817712b515>.

8. Wang L., Yang B., Chen Y., Zhang X., Orchard J. Improving neural-network classifiers using nearest neighbor partitioning. IEEE Trans NNL System. 2017. DOI: 10.1109/TNNLS.2016.2580570.

9. Shuangrong Liu, Lin Wang, Bo Yang, Jin Zhou, Zhenxiang Chen, Hui fen Dong. Improvement of Neural-Network Classifiers Using Fuzzy Floating Centroids. DOI: 10.1109/TCYB.2020.2987904.

10. Zhu C., Wang Z. Entropy-based matrix learning machine for imbalanced data sets. Pattern Recognit Lett. 2017. DOI: 10.1016/j.patrec.2017.01.014.

11. Aurelio, YS, de Almeida, GM, de Castro, CL and Braga, AP. Learning from imbalanced data sets with weighted cross-entropy function. 2019. DOI: 10.1007/s11063-018-09977-1.

12. Badrinarayanan V., Kendall A. and Cipolla R. Seg-Net: a deep convolutional encoder-decoder architecture for image segmentation. IEEE Trans. Pattern Analytic. Mach Intelligence. 2017. DOI: 10.1109/TPAMI.2016.2644615.

13. Daniel Voigt Godoy. Deep Learning with PyTorch Step-by-Step: A Beginner's Guide. Copyright 2020-2022.



УДК 355.41

канд. техн. наук Мельник Б. О. ORCID: 0000-0002-5635-0099 (ЦНДІ ОБТ ЗС України)

канд. військ. наук Овчаренко І. В. ORCID: 0000-0001-9066-0800 (НУОУ)

Новікова І. В. ORCID: 0000-0003-4854-0682 (НУОУ)

## ТЕХНІКО-ЕКОНОМІЧНА ОЦІНКА РЕМОНТУ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

*Аналіз застосування підрозділів та військових частин під час ведення бойових дій у російсько-українській війні дозволяє стверджувати, що одним із основних чинників, які впливають на успіх у виконанні завдань, є наявність працездатних зразків озброєння та військової техніки.*

*Водночас одним із основних джерел надходження в підрозділи (військові частини) працездатних зразків озброєння і військової техніки під час ведення бойових дій є повернення їх зі стаціонарних та рухомих ремонтно-відновлювальних військових частин (підрозділів) після виконання заходів з їхнього відновлення.*

*Відповідно під час відновлення пошкоджених зразків озброєння і військової техніки витрачаються запасні частини, вузли, агрегати, комплектуюче обладнання тощо, які необхідно закупляти у виробників, що призводить до фінансово-економічних витрат.*

*Тому в роботі запропоновано методичний підхід до оцінювання економічної ефективності ремонту зразків озброєння і військової техніки.*

*Цей підхід враховує два напрямки: фінансово-економічні витрати на ремонт озброєння і військової техніки в стаціонарних умовах та у рухомих ремонтно-відновлювальних військових частинах (підрозділах).*

*Під час ремонту озброєння і військової техніки в стаціонарних умовах основні фінансові витрати будуть спрямовані на основну заробітну плату спеціалістів-ремонтників, основні матеріали, запасні частини, цехові накладні витрати, загальні накладні витрати, витрати на освоєння нових видів продукції і спеціальні витрати.*

*А під час ремонту озброєння і військової техніки у ремонтно-відновлювальних військових частинах (підрозділах) основні витрати будуть спрямовані на закупівлю нових деталей, вузлів, агрегатів, вартість амортизації обладнання, вартість утримання особового складу спеціалістів-ремонтників, середню вартість експлуатаційного комплекту.*

**Ключові слова:** озброєння та військова техніка, ремонт, фінансові витрати, матеріальні ресурси, ремонтно-відновлювальні органи, система забезпечення, рівні ієрархії.

### ***B. Melnyk, I. Ovcharenko, I. Novikova Technical and economic assessment of the repair of weapons and military equipment's repair.***

*The analysis of divisions and military units' use in the course of hostilities during the Russian-Ukrainian war allows us to state that one of the main factors that affects the success in completing tasks is the availability of operational samples of weapons and military equipment. At the same time, one of the main sources of serviceable samples of weapons and military equipment being received by units (military units) in the course of hostilities is their return from stationary and mobile repair and restoration military units (units) after carrying out measures to restore them.*

*Accordingly, during the restoration of damaged samples of weapons and military equipment, spare parts, assemblies, aggregates, component equipment, etc. are consumed, that must be purchased from manufacturers, which led to financial and economic costs.*

*Therefore, the work proposes a methodical approach to evaluating the economic efficiency of repairing samples of weapons and military equipment.*

*This approach takes into account two directions: financial and economic costs for the repair of weapons and military equipment in stationary conditions and in mobile repair and restoration military units (subunits). During the repair of weapons and military equipment in stationary conditions, the main financial costs will be directed to: the basic salary of repair specialists, basic materials, spare parts, workshop overheads, general overheads, costs for the development of new types of products and special costs.*

*And during the repair of weapons and military equipment in repair and restoration military units (units), the main costs will be directed to the purchase of new parts, assemblies, units, the cost of depreciation of equipment, the cost of maintaining the personnel of repair specialists, the average cost of the operational kit.*

**Keywords:** weapons and military equipment, repair, financial costs, material resources, repair and restoration bodies, support system, hierarchy levels.

## **1. Постановка проблеми**

### **1.1. Новизна дослідження**

Досвід виконання завдань в операції Об'єднаних сил (далі – ООС) на території Донецької та Луганської областей та відбиття збройної агресії російської федерації (рф) підтверджує широке застосування збройними силами рф мінно-вибухових засобів ураження, які здатні уражати не лише днище, а й кормову та бокові проєкції зразків озброєння та військової техніки (далі – ОВТ). Окупаційними силами та проросійськими терористичними угрупованнями активно використовуються атаки на підрозділи Сил Оборони за допомогою саморобних вибухових пристроїв та мін-пасток, що призводить до суттєвих втрат серед особового складу та техніки. Найбільш часто російська армія використовує протипіхотні, протитанкові, протитранспортні міни, кумулятивні а також зосереджені заряди вибухових речовин, які були прийняті на озброєння Радянської армії за часів СРСР [1–3].

Характер пошкоджень зразків ОВТ, які мають місце під час ведення бойових дій, вказує на те, що найбільш уразливими елементами бойової броньованої машини (далі – ББМ) від саморобного вибухового пристрою (далі – СВП) є ходова частина, днище корпусу, бокова проєкція ББМ тощо. Серед кінетичних засобів ураження найбільш часто ББМ уражається артилерійськими боеприпасами, мінометними мінами та протитанковими гранатометами [4].

Аналіз втрат, що має місце у військових частинах, залучених до ведення бойових дій (операції), свідчить, що від підривання на вибухових пристроях та від кінетичних засобів ураження значна кількість ОВТ, які отримали пошкодження, потребують відновлення та повернення їх у підрозділи [5].

Відповідно для відновлення зразків ОВТ, які отримали бойові пошкодження різної складності, залучаються стаціонарні ремонтні підприємства (бази) і рухомі ремонтно-відновлювальні військові частин (підрозділи) різних рівнів ієрархії. Тобто, основним джерелом поповнення підрозділів і військових частин, які виконують завдання за призначенням, є відновлені зразки ОВТ, які зазнали бойових пошкоджень або вийшли з ладу з експлуатаційних причин. Відповідно для їх відновлення витрачаються запасні частини, вузли, агрегати, комплектуюче обладнання тощо, які необхідно закупляти у виробників. Усе це пов'язано з фінансовими витрати, що підтверджує актуальність даного дослідження.

### **1.2. Аналіз останніх досліджень та публікацій**

Дослідженню питань щодо оцінювання економічної ефективності відновлення зразків ОВТ, які вийшли з ладу внаслідок бойових пошкоджень та від експлуатаційних несправностей, присвячена ціла низка робіт, зокрема в роботі [6] запропоновано науково-методичні підходи щодо дослідження воєнно-технічних і техніко-економічних аспектів життєвого циклу зразків ОВТ. Так, у роботі [7] розглянуто питання оцінки техніко-економічної ефективності модернізації зразків ОВТ, вказано, що модернізація продовжує життєвий цикл зразка озброєння, але кожна конструкція зразків має обмеження щодо модернізації з погляду економічної доцільності, а у роботі [8] визначено економічний ефект від впровадження удосконаленої системи технічного обслуговування і ремонту для гусеничних машин, котрі знаходяться в безперервній експлуатації і для машин, знятих зі зберігання. У роботі [9] розглянуто основні підходи до організації бюджетного та оборонного планування в Міністерстві оборони України та Збройних сил України щодо розвитку ОВТ та вироблено рекомендації до формування техніко-економічних показників життєвого циклу ОВТ. В роботах [10–11] визначено, що для забезпечення ефективного використання фінансових ресурсів при обґрунтуванні вартісних показників заходів державної програми озброєння необхідно застосовувати комплексний підхід, що полягає в обліку бюджетних коштів на реалізацію стадій життєвого циклу зразка ОВТ, а також ефекту від його застосування в складі військового формування, а в роботі [12] на підставі аналізу застосування броньованих спеціалізованих машин і вимог до захищеності запропоновано методичний



підхід вибору способів зварювання корпусів панцирних автомобілів, який дозволяє визначити технологічну собівартість виконання зварювальних робіт за існуючою і пропонованою технологіями. В роботі [13] наводять приклади застосування контрактних моделей державно-приватного партнерства зі схемою оплати послуг виконавця за нормативними показниками кінцевого результату післяпродажного обслуговування техніки. В літературних джерелах [14] запропоновано метод, який ґрунтується на двох критеріях для оцінки надійності транспортного засобу. Перший критерій має технічний характер, а другий – економічний характер. Економічний критерій полягає в оцінюванні витрати на технічне обслуговування, які тісно пов'язані з рівнем надійності транспортного засобу і зазвичай являють собою значну частину загальної вартості кожного транспортного засобу, а у [15] запропоновано методику, яка містить показники справності зразків ОБТ а також показники для оцінювання витрат на їхню експлуатацію. В роботі [16] приведено підходи щодо раціоналізації матеріально-технічних витрат для забезпечення розподілу відповідно до способів їх одержання органом забезпечення, а у роботі [17] наведено організаційні та технічні умови, пов'язані з впровадженням системи доцільного ремонту озброєння та військової техніки та питання уніфікації й налагодження обладнання в процесі проектування та виробництва.

### 1.3. Постановка завдання

Тому, враховуючи складності пошкоджень, які отримані зразками ОБТ в сучасній війні проти РФ, необхідно розробити методичний підхід до оцінювання економічної ефективності ремонту зразків ОБТ, які ремонтуються стаціонарними та рухомими ремонтно-відновлювальними підрозділами за рахунок рухомих засобів відновлення на різних рівнях ієрархії, що і буде метою цієї статті. Цей методичний підхід дозволить оцінювати, у який ремонтний підрозділ направляти пошкоджений зразок ОБТ залежно від ступеня отриманого пошкодження та економічних витрат на його ремонт.

### 2. Виклад основного матеріалу

Ремонт ОБТ проводиться в стаціонарних або польових умовах. Для цієї мети створюються стаціонарні ремонтні підрозділи і рухомі ремонтно-відновлювальні військові частин (підрозділи) тактичного, оперативного та стратегічного рівнів ієрархії.

До стаціонарних ремонтних підрозділів відносяться ремонтні майстерні арсеналів, центральних баз і складів, призначені для ремонту ОБТ і складальних одиниць агрегатів, тощо. Відповідно до рухомих відносяться ремонтно-відновлювальні військові частини стратегічного та оперативного рівнів ієрархії, а також ремонтно-відновлювальні підрозділи військових частин [18].

Фінансово-економічні витрати на ремонт зразків ОБТ у стаціонарних ремонтних підрозділах можна згрупувати за такими елементами:

основна заробітна плата спеціалістів-ремонтників;

основні матеріали;

запасні частини;

цехові накладні витрати;

загальні накладні витрати;

витрати на освоєння нових видів продукції і спеціальні витрати.

До основної заробітної плати спеціалістів-ремонтників на стаціонарних ремонтних підрозділах (ремонтних цехах баз, арсеналів тощо) відносять виплати за роботу, проведену безпосередньо з ремонту ОБТ [19].

Основна заробітна плата  $P_0$  спеціалістів-ремонтників може бути орієнтовно підрахована за формулою (1):

$$P_0 = S_1 K_{at} R F_{wtf}, \quad (1)$$

де  $S$  – годинна ставка першого розряду, грн/год;

$K_{at}$  – середній тарифний коефіцієнт спеціалістів-ремонтників;

$R$  – кількість спеціалістів-ремонтників, люд.;

$F_{wtf}$  – річний дійсний фонд робочого часу одного робітника, люд.-год.

У додаткову заробітну плату входять оплата відпусток, доплати за роботу в нічний час, оплата понаднормових годин тощо.

Додаткова заробітна плата спеціалістів-ремонтників, основна і додаткова заробітна плата допоміжних робітників, зайнятих обслуговуванням виробництва, відносяться до накладних витрат.

Основні матеріали – це такі матеріали, які використовуються безпосередньо для зразка ОВТ, який ремонтується та збільшують його вагу. До основних матеріалів зазвичай відносять сталь, кольорові метали, електроди, фарби тощо.

До допоміжних матеріалів відносяться матеріали, які використовуються в процесі ремонту ОВТ, але не залишаються на них після ремонту (гас, розчинник, матеріали для протирання тощо).

Річна потреба в основних матеріалах визначається кількістю зразків ОВТ, які ремонтуються за встановленими нормами витрати матеріалів. Вартість основних матеріалів приймається за цінами постачальних організацій з нарахуванням транспортних витрат.

Допоміжні матеріали до цієї статті витрат не відносяться. Вони враховуються у витратах, пов'язаних з обслуговуванням виробництва. Якщо при витрачанні основних матеріалів їх відходи не використовуються, то вартість відходів повинна бути виключена з вартості основних матеріалів.

До витрат на запасні частини зазвичай відносять:

вартість запасних частин, які купуються, нормалей, вузлів, агрегатів, комплектуючого обладнання та інших виробів, що йдуть на укомплектування продукції, яка ремонтується;

вартість придатних запасних частин, отриманих від розбирання списаного ремонтного фонду;

вартість запасних частин, що залишилися після модернізації зразків ОВТ, які надійшли від заводів промисловості без оплати.

Вартість запасних частин визначається за надані послуги. Значну частку витрат складають витрати на обслуговування виробництва і управління. Ці витрати поділяються на цехові і загальні й відносяться до накладних витрат.

Цехові накладні витрати охоплюють:

витрати на енергію (стиснене повітря, вода, силова електроенергія тощо);

заробітну плату допоміжних робітників, молодшого обслуговуючого персоналу, лічильно-облікового персоналу, інженерно-технічних працівників;

утримання будівель і споруд (витрати на освітлювальну електроенергію, пар і воду для опалення та побутових потреб);

утримання обладнання;

витрати на допоміжні матеріали;

амортизаційні відрахування;

додаткову заробітну плату спеціалістів-робітників;

витрати на охорону праці, раціоналізаторські впровадження, винахідництво.

Цехові накладні витрати становлять приблизно 180–200 % основної заробітної плати спеціалістів-робітників.

Загальні накладні витрати містять ті самі групи витрат, що і цехові, але в масштабі ремонтних підрозділів баз, арсеналів тощо. Сюди відносять витрати на утримання котельні, компресорної, електропідстанції, будівель управління, їдальні, клубу, гаража, заробітна плата персоналу управління, поштово-телеграфні витрати, придбання літератури тощо.

Загальні накладні витрати складають близько 60–80 % основної заробітної плати спеціалістів-робітників.

До витрат з освоєння виробництва нових видів продукції відносять витрати з технічної, документальної і матеріальної підготовки виробництва, а також інші витрати, пов'язані з освоєнням ремонту нових типів виробів.

Спеціальні витрати охоплюють витрати на оплату відряджень, відрахування на преміювання працівників за розроблення і впровадження нової техніки, оплату штрафів, пені тощо [20].

У собівартості ремонту ОВТ в основному переважають витрати на придбання запасних частин. Тому основний резерв зниження собівартості при ремонті ОВТ це, перш за все, розширення номенклатури деталей, що підлягають ремонту без зниження їхньої якості і надійності, а також всебічне підвищення продуктивності праці.

Економічне значення зниження собівартості продукції велике і є найважливішою умовою зростання економічної ефективності, досягнення найвищих результатів при найменших затратах праці.

Розрахунок зниження собівартості продукції зазвичай проводиться за двома показниками:

зниження собівартості товарної продукції, яка порівнюється у відсотках до попереднього року, якщо зіставні види продукції переважають у загальному вигляді випуску продукції;

за витратами на одну грошову одиницю товарної продукції, якщо в загальному випуску продукції переважають непорівнянні з попереднім роком види продукції.

Завдання щодо зниження собівартості товарної продукції у відсотках до попереднього року розробляються в плані підвищення ефективності виробництва. При цьому частка порівнюваних виробів в собівартості залежить від річного випуску продукції, передбаченого на плановий рік.

Зниження собівартості продукції визначається за рівнем середньорічної собівартості цієї продукції за попередній рік.

Для визначення планового зниження собівартості продукції щодо минулого року порівняльна продукція, яку намічено до випуску, оцінюється за двома параметрами: собівартості в плановому році і за середньорічною собівартості її за минулий рік.

При вирішенні питань, пов'язаних зі зниженням собівартості продукції, підвищенням прибутку і рентабельності виробництва, необхідно розрізняти прибуток від реалізації продукції за планом і балансовий прибуток.

Прибуток від реалізації продукції за планом  $P_r$  визначається як різниця між сумою, яка отримана від реалізації продукції в діючих оптових цінах за планом, і собівартістю реалізованої продукції за планом згідно з виразом (2):

$$P_r = B_{sp} - C_p, \quad (2)$$

де  $B_{sp}$  – сума, отримана від реалізації продукції в діючих оптових цінах за планом, грн.;

$C_p$  – собівартість реалізованої продукції за планом, грн.

Балансовий прибуток являє собою суму, що складається з прибутку від реалізації продукції за планом і сальдо прибутків і збитків за балансовим кредитом, житлово-комунального відділу тощо. Балансовий прибуток  $P_b$  містить також премії інженерно-технічних працівників згідно з виразом (3):

$$P_b = P_r + C_{pb}, \quad (3)$$

де  $C_{pb}$  – сальдо прибутків і збитків за балансовим кредитом, житлово-комунального відділу тощо, або позареалізаційний прибуток.

Отриманий ремонтним підрозділом баз, арсеналів тощо прибуток характеризує кінцевий фінансовий результат роботи колективу спеціалістів-ремонтників, отже, значною мірою визначає внесок його в чистий дохід, який направляється на розширення матеріального відтворення, поліпшення трудових умов, зміцнення обороноздатності країни.

Але абсолютна величина прибутку не дозволяє ще об'єктивно оцінювати результати роботи ремонтного підрозділу баз, арсеналів тощо, тому що збільшення її маси може бути досягнуто не тільки шляхом мобілізації внутрішніх резервів, зниження витрат виробництва, підвищення продуктивності праці і кращого використання виробничих фондів, а й шляхом надмірного накопичення останніх через невиправдано великі капітальні вкладення, тобто зростання обсягу прибутку може супроводжуватися погіршенням використання виробничих фондів. Щоб дати об'єктивну оцінку роботи ремонтного підрозділу баз, арсеналів тощо, необхідно обчислити рівень його рентабельності [21].

Для визначення рівня рентабельності ремонтного підрозділу баз, арсеналів тощо в цілому прибуток за планом зіставляється з основними виробничими фондами, що враховуються за первісною (балансовою) вартістю. Тобто, без врахування зносу і нормованих оборотних коштів, що характеризує загальну рентабельність ремонтного підрозділу баз, арсеналів тощо. Вона показує величину прибутку на грошову одиницю виробничих фондів, і, отже, орієнтує працівників ремонтного підрозділу баз, арсеналів тощо на поліпшення використання виробничих фондів для отримання максимального прибутку.

Крім загальної рентабельності ремонтних підрозділів баз, арсеналів тощо розраховують також розрахункову рентабельність, яка визначається як відношення балансового прибутку за вирахуванням плати за виробничі фонди, фіксованих платежів і платежів за відсотками за банківський кредит до середньорічної вартості основних виробничих фондів і нормування оборотних коштів.

За рівнем розрахункової рентабельності оцінюється виконання плану, визначаються нормативи відрахувань до фондів економічного стимулювання, за якими утворюється основна частина заохочувальних фондів.

Викладене можна представити у вигляді формул (4), (5):

$$P_{gen} = \frac{P_{re}}{S} 100, \quad (4)$$

де  $P_{gen}$  – загальна рентабельність;

$P_{re}$  – прибуток від реалізації продукції за планом;

$S$  – середня вартість основних фондів і нормованих оборотних коштів для розрахунку рентабельності;

$$P_{ret} = \frac{P_b}{S} \frac{(P_s + P_{fp} + P_{il})}{(S_{pf} + S_{ep})} 100, \quad (5)$$

де  $P_{ret}$  – розрахункова рентабельність;

$P_b$  – балансовий прибуток;

$P_s$  – плата за фонди;

$P_{fp}$  – фіксовані платежі в бюджет;

$P_{il}$  – відсотки за кредит банку;

$S_{pf}$  – пільгові фонди;

$S_{ep}$  – фонди, які звільняються від платежів.

У сучасних умовах ведення бойових дій (операції) найважливішими напрямками підвищення рентабельності ремонтного підрозділу баз, арсеналів тощо, а отже, і ефективності ремонту ОВТ є технічний прогрес, використання резервів виробництва, зниження собівартості

і підвищення якості продукції, зростання накопичень і постійне поліпшення використання виробничих фондів.

Технічний прогрес дозволяє замінювати застарілі засоби з низькою ефективністю праці високопродуктивними зразками, за допомогою яких при економії людської праці можна виробляти більше продукції і кращої якості на одиницю матеріальних, трудових і фінансових витрат. Із технічним прогресом тісно пов'язані можливості поліпшення використання виробничих фондів, зниження собівартості, зростання накопичень і, отже, підвищення рентабельності ремонтного підрозділу баз, арсеналів тощо.

Зростання масштабів виробництва і якісні зрушення в економіці висувають нові вимоги до організації та управління ремонтом ОБТ, диктують необхідність подальшого вдосконалення методів планування і економічного стимулювання ремонтних підрозділів баз, арсеналів тощо.

Економічне стимулювання має, по-перше, спонукати ремонтні підрозділи приймати напружені плани, раціонально використовувати матеріальні, фінансові та трудові ресурси, а по-друге, стимулювати прискорення науково-технічного прогресу, продуктивності праці і підвищення якості продукції, яка випускається.

Нині у ремонтних підрозділах баз, арсеналів створюються три фонди економічного стимулювання: фонд матеріального заохочення, фонд соціально-культурних заходів і житлового будівництва й фонд розвитку виробництва.

Фонди економічного стимулювання, утворені завдяки відрахуванням від прибутку і безпосередньо пов'язані з основними показниками господарсько-фінансової діяльності підприємств, призначено для стимулювання високої ефективності виробництва, забезпечення гармонійного сполучення інтересів кожного працівника з інтересами виробничого колективу і суспільства в цілому.

Відповідно до прийнятого порядку фонд матеріального заохочення і фонд соціально-культурних заходів і житлового будівництва утворюються від прибутків за нормативами, встановленими у відсотках до фонду заробітної плати, а фонд розвитку виробництва – за нормативами, встановленими у відсотках до середньорічної вартості основних виробничих фондів.

Існують два види нормативів: один із них встановлюється для ремонтних стаціонарних ремонтних підрозділів за кожен відсоток рівня розрахункової рентабельності, а другий – за кожен відсоток зростання реалізації продукції.

При перевиконанні планових показників нормативи відрахувань знижуються, що економічно зацікавлює ремонтні підрозділи в прийнятті напружених планів з урахуванням мобілізації внутрішніх ресурсів.

Враховуючи аналіз ведення бойових дій (операції) проти РФ та досвід ООС (АТО) основу військового ремонту ОБТ складають поточний і середній ремонти зразків ОБТ, який виконується ремонтно-відновлювальними військовими частинами (підрозділами) [1–4].

Поточний ремонт виконується, як правило, в ремонтних підрозділах військових частин на готових деталях, вузлах, агрегатах.

Вартість поточного ремонту зразків ОБТ буде складатися з цілого ряду складових: вартості заново встановлювальних на зразок ОБТ покупних деталей, вузлів, агрегатів, вартості амортизації обладнання, вартості утримання особового складу спеціалістів-ремонтників, які беруть участь у відновленні ОБТ, середньої вартості експлуатаційного комплексу на один поточний ремонт тощо [22].

Вартість знову встановлювальних на зразок ОБТ покупних деталей вузлів, агрегатів зазвичай визначається за прейскурантами.

Дещо складніше визначити інші витрати, але і вони можуть бути отримані узагальненням або розрахунковим шляхом.

Визначення вартості амортизації обладнання за один поточний ремонт може бути визначено на підставі норм постачання виробничим і допоміжним обладнанням, пристроями та інструментом для ремонтно-відновлювальних військових частин (підрозділів) відповідно до наказів Міністра оборони з урахуванням результатів обробки і аналізу статистичних даних.

На підставі статистичних даних ремонтно-відновлювальний підрозділ військової частини проводить в рік близько 100 поточних ремонтів в мирний час, а в особливий період усе буде залежати від імовірного виходу ОБТ з ладу від бойових пошкоджень.

Визначити вартість експлуатаційного комплексу можна із розрахунку вартості експлуатаційного комплексу на один поточний ремонт кожної номенклатури ОБТ.

Отже, усі складові можуть бути визначені або узагальненням статистичних даних, або розрахунковим шляхом, що дає можливість визначити структуру вартості поточного ремонту.

Як правило, у вартості поточного ремонту ОБТ переважають витрати на покупку заново встановлених деталей, вузлів і агрегатів, а також витрати на придбання експлуатаційного комплексу.

Вартісні витрати на поточні ремонти зразків ОБТ можуть бути оцінені також питомими показниками різного роду. Так, наприклад, оцінка може бути здійснена витратами на поточні ремонти на 1000 км пробігу, за міжремонтний термін експлуатації або середньорічними вартісними витратами.

Для оцінки вартісних витрат на поточні ремонти зразків ОБТ на 1000 км пробігу прийнятий коефіцієнт  $K_{Q=1000}$ . Зазвичай його визначають зі співвідношення (6):

$$K_{Q=1000} = \frac{Q_{cr} \cdot n_{ncr}}{0,001 S_{irp}}, \quad (6)$$

де  $Q_{cr}$  – середня вартість одного поточного ремонту;

$n_{ncr}$  – кількість поточних ремонтів за цикл експлуатації;

$S_{irp}$  – міжремонтний термін за цикл експлуатації.

Середньорічні витрати оцінюються коефіцієнтом  $K_{Qr}$ . Він визначається зі співвідношення (7):

$$K_{Qr} = \frac{Q_{er} \cdot n_{ner}}{0,001 S_{irp}} K_y, \quad (7)$$

де  $K_y$  – коефіцієнт річної експлуатації.

Річні витрати матеріальних засобів залежать від норм річної експлуатації зразків ОБТ і конкретного штату військової частини.

З погляду витрат на поточні ремонти для різної номенклатури зразків ОБТ вони будуть відрізнятися. Це пов'язано з тим, що деталі, вузли і агрегати мають різну вартість, коефіцієнт річної експлуатації  $K_y$  для кожного зразка ОБТ різні, що також негативно позначається на витратах на поточний ремонт.

Вартість середнього ремонту ОБТ, так само як і поточного ремонту, складається з цілого ряду складових (покупні деталі, вузли, агрегати, амортизація обладнання тощо).

Порядок і послідовність визначення вартісних витрат аналогічні визначенням витрат на поточний ремонт.

Середній ремонт зразків ОБТ виконується в ремонтно-відновлювальних військових частинах оперативного і стратегічного рівнів, як правило, на готових агрегатах і вузлах [22].

Вартість заново встановлюваних на зразок ОБТ покупних деталей, вузлів, агрегатів визначається за цінами постачальників. Вартість амортизації обладнання визначається за тією самою методикою, що і для поточного ремонту. На підставі статистичних даних у мирний час ремонтно-відновлювальна військова частина проводить близько 40 середніх ремонтів на рік.

Отже вартість амортизації обладнання можна визначити з розрахунку вартості на один середній ремонт кожної номенклатури ОВТ.

Аналогічно визначаються й інші складові, що, в кінцевому рахунку, дає можливість визначити структуру вартості середнього ремонту.

У вартості середнього ремонту зразків ОВТ переважають в основному витрати на придбання покупних деталей, вузлів і агрегатів. Величина цих витрат становить 97–98 % загальної вартості середнього ремонту.

Вартісні витрати на середній ремонт в розрахунку на 1000 км пробігу за міжремонтний термін оцінюються також за допомогою коефіцієнта  $K_{Q=1000}$ , який визначається зі співвідношення (8):

$$K_{Q=1000} = \frac{\bar{Q}_{ar}}{0,001S_{irp}}, \quad (8)$$

де  $\bar{Q}_{ar}$  – вартість середніх ремонтів за цикл експлуатації.

Вартісні витрати на середній ремонт в розрахунку на рік експлуатації визначаються за допомогою коефіцієнта  $K_{Qar}$ , який визначається зі співвідношення (9):

$$K_{Qar} = \frac{\bar{Q}_{ar}}{0,001S_{irp}} K_y. \quad (9)$$

Зменшення величини розглянутих показників можливо завдяки пошуку шляхів скорочення витрат матеріальних засобів на плановий ремонт і підвищення якості ремонту з метою збільшення міжремонтних термінів.

Не менш важливою обставиною є зниження вартості покупних деталей, вузлів, агрегатів. Це повинно здійснюватися насамперед на заводах виробництва запасних частин оборонно-промислового комплексу в загальнодержавному масштабі. Велику роль при цьому мають відігравати також заводи з капітального ремонту ОВТ, які випускають агрегати для військових ремонтних засобів. Зниження вартості агрегатів дозволяє значною мірою скоротити витрати на військовий ремонт ОВТ.

### 3. Висновки і перспективи подальших досліджень

Отже, серед економічних важелів впливу на ремонтне виробництво важливе місце належить прибутку і рентабельності, які є основними показниками ремонту ОВТ, джерелом накопичень, зростання виробничих і заохочувальних фондів стаціонарних ремонтних підрозділів. При цьому економічні важелі діють не відокремлено один від одного, а в тісному зв'язку і взаємозумовленості, утворюючи єдину економічну систему.

Зменшення фінансово-економічних витрат для рухомих ремонтно-відновлювальних військових частин (підрозділів) буде залежати від скорочення витрат на матеріально-технічні засоби і завдяки підвищенню якості ремонту.

Отже, стаціонарна і рухома складові відновлення ОВТ забезпечують високу ефективність ремонту ОВТ в мирний час і в особливий період.

### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Головне управління доктрин та підготовки Генерального штабу спільно з зацікавленими структурними підрозділами науково-дослідних установ Збройних Сил України. Збірник № 4 “Матеріалів вивчення бойового досвіду російсько-української війни червень 2022 р.”. Київ: 2022. С. 204–205.
2. Дачковський В. О., Кондратюк І. В., Дядечко А. О., Сампір О. А., Павлов Д. П. Крос-темпоральний аналіз втрат озброєння та військової техніки Російської Федерації під час ведення війн на території інших держав протягом останніх 30 років // *Social Development and Security*. 2022. Vol. 12. № 3. С. 14–29.
3. Аналіз бойових дій в районі Іловайська після вторгнення російських військ 24–29 серпня 2014 року. URL: <http://www.mil.gov.ua/news/2015/10/19/analiz-illovausk--14354/>.

4. Аналіз бойових дій на сході України в ході зимової кампанії 2014–2015 років. URL: <http://www.mil.gov.ua/news/2015/12/23/analiz-bojovih-dij-na-shodi-ukraini-v-hodi-zimovoi-kampanii-2014-2015-rokiv--16785/>.
5. Аналіз Генерального штабу ЗС України щодо бойових дій на Дебальцевському плацдармі з 27 січня до 18 лютого 2015 року. URL: <http://www.mil.gov.ua/analitichni-materiali/analiz-generalnogo-shtabu-zsu-shhodo-bojovih-dij-na-debaltzevskomu-placzdarmi-z-27-sichnya-do-18-lyutogo-2015-roku.html>.
6. Dachkovskiy V., Kondratiuk I. Technical and economic assessment of the weapons and military equipment exploitation // *Political Science and Security Studies Journal*. 2021. № 2 (4). С. 42–50. DOI: <https://doi.org/10.5281/zenodo.5810146>.
7. Шишанов М. О., Чеченкова О. Л., Павловський І. В. Техніко-економічна оцінка модернізації бронетанкової техніки при її капітальному ремонті // *Озброєння та військова техніка*. 2018. № 1 (17). С. 62–65.
8. Зянько В. В., Поляков П. А. Техніко-економічна оцінка рекомендацій щодо підвищення ефективності функціонування системи технічного обслуговування і ремонту техніки на гусеничній базі. URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/16822/3139.pdf?sequence=3>.
9. Parkhomenko Pavlo, Lavruk Michael, Tkach Ivan. Analiz zdiysnennya byudzhethnoho ta oboronnoho planuvannya u systemi Ministerstva oborony Ukrayiny ta Zbroynykh Syl Ukrayiny v konteksti rozvytku ozbroynennya ta viys'kovoyi tekhniky // *Social development & Security*. 2019. № 9 (5). Р. 174–189. DOI: <http://doi.org/10.33445/sds.2019.9.5.12>.
10. Викулов С. Ф., Косенко А. А., Подольский А. Г. Методический подход к оценке контрактных цен на реализацию программных мероприятий по созданию вооружения и военной техники. URL: <http://viculov.ru/trudy/93.pdf>.
11. Бахарев Г. А. Боевая эффективность и затраты. URL: <https://cyberleninka.ru/article/n/boevaya-effektivnost-i-zatraty-1>.
12. Shishanov M. O., Datsenko I. P. Metodychni osnovy tekhniko-ekonomichnykh otsinok tekhnolohichnykh protsesiv vyhotovlennya ta modernizatsiyi korpusiv pankrealizatsiyi avtomobiliv // *Social development & Security*. 2018. № 1 (1). Р. 29–38. DOI: <http://doi.org/10.5281/zenodo.1412070>.
13. Asadullin M. R. Method for technical and economic evaluation of the effectiveness of reliability improvement of military aircraft gas-turbine engines in their aftersales support based on outcome performance measures // *Vestnik Permskogo universiteta. Seria Ekonomika = Perm University Herald. Economy*. 2016. № 3 (30). Р. 92–104. DOI: 10.17072/1994-9960-2016-3-92-104.
14. Vintr Zdenek, Holub Rudolf. A Method of technical and economic evaluation of vehicle reliability. Seoul 2000 FISITA World Automotive Congress June 12–15, 2000, Seoul, Korea. URL: [https://www.researchgate.net/publication/267845747\\_A\\_Method\\_of\\_Technical\\_and\\_Economic\\_Evaluation\\_of\\_Vehicle\\_Reliability](https://www.researchgate.net/publication/267845747_A_Method_of_Technical_and_Economic_Evaluation_of_Vehicle_Reliability).
15. Буравлев А. И. Методика оценки военно-технического уровня парка ВВТ в ходе реализации программных мероприятий по их закупке и ремонту // *Вооружение и экономика*. 2016. № 4 (37). С. 91–103.
16. Kotsiuruba V., Dachkovskiy V., Kurtseitov T. The model of the organizational and technical weapons and military equipment recovery system // *Social Development and Security*. 2021. № 11 (6). Р. 194–208. DOI: <https://doi.org/10.33445/sds.2021.11.6.15>.
17. Smal T., Furch J. Expedient repairs – analysis of possibilities and needs // *Advances in Military Technology*. 2011. Vol. 6. No. 2. Р. 69–82.
18. Дачковський В. О., Ярошенко О. В., Овчаренко І. В., Сампір О. М. Методика проектування ремонтно-відновлювальних органів // *Збірник наукових праць військової академії*. 2020. № 13 (1). Ч. 1. С. 210–222. DOI: 19.37129/2313-7509.2020.13.1.210-222.
19. Деменев О. М., Рихтюк В. Л., Мунтіян В. І., Ткач І. М. Маркетинг та логістика у Збройних Силах України: навч. посіб. / за ред. В. Л. Рихтюка. – К.: НУОУ ім. Івана Черняховського, 2016. 304 с.
20. Слободяник С. П. Фінансовий менеджмент. К.: НУОУ ім. Івана Черняховського, 2014. 301 с.
21. Дачковський В. О., Овчаренко І. В., Ярошенко О. В., Багдасарян Н. К. Оперативні розрахунки завдань технічного забезпечення (методика та приклади). К.: НУОУ ім. Івана Черняховського, 2018. 116 с.
22. Дачковський В., Левченко М. Напрямки розвитку рухомих засобів ремонту озброєння та військової техніки // *InterConf*. 2021. № 65. URL: <https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/13839>.



UDK 621.396.4

Doctor of Tech. Sciences Romaniuk Valery ORCID: 0000-0002-6218-2327 (MITIT)  
PhD Hrymud Andrii ORCID: 0000-0003-4012-5185 (MITIT)

## ANALYSIS OF THE RULES FOR CONSTRUCTING A FLIGHT TRAJECTORY OF A COMMUNICATION AERIAL PLATFORM FOR DATA COLLECTION FROM NODES OF A WIRELESS SENSOR NETWORK

*Романюк В. А., Гримуд А. Г. Аналіз правил побудови траєкторії польоту для збору даних комунікаційною аероплатформою з вузлів безпроводової сенсорної мережі.*

Для збору даних моніторингу з вузлів безпроводових сенсорних мереж із незв'язною топологією пропонується використовувати комунікаційну аероплатформу (далі – КА), яка побудована на базі безпілотного літального апарата. КА в процесі польоту формує тимчасові локальні радіомережі та виконує роль повітряного шлюзу для збору даних з окремих вузлів та головних вузлів у зв'язних фрагментах мережі. Ефективність процесу збору даних залежить від характеристик мережі, способів (правил) побудови траєкторії польоту КА, кількості та локації точок (інтервалів) обміну даними тощо. У статті проводиться оцінка ефективності застосування різних продукційних правил побудови траєкторії польоту КА для збору даних з вузлів мережі для досягнення певних цільових функцій: мінімізації часу збору даних, максимізації часу функціонування мережі.

У роботі сформульована задача пошуку траєкторії польоту та збору даних КА з вузлів як задача пошуку найкоротшої траєкторії переміщення зони покриття КА з початкової в кінцеву точки польоту, яка забезпечує покриття всіх вузлів (кластерів на площі) на мінімальній відстані обміну КА з вузлами. Для оцінки ефективності застосування правил побудови траєкторії польоту та збору даних розроблена відповідна імітаційна модель. Вхідними даними моделювання є характеристики мережі, вузлів та комунікаційної аероплатформи, способи (правила) управління процесом збору даних. Імітаційна модель надає можливість отримувати залежності показників ефективності (час збору даних, витрати енергії батарей, час функціонування мережі) на множині правил побудови траєкторії польоту та збору даних КА при різних вхідних даних.

Результати імітаційного моделювання застосування множини (базис) правил довели можливість зменшення часу збору даних до 20 % або підвищення часу функціонування мережі до 15 % порівняно з існуючими рішеннями.

**Ключові слова:** безпроводова сенсорна мережа, комунікаційна аероплатформа, траєкторія польоту, збір даних, база правил, моделювання.

*V. Romaniuk, A. Hrymud Analysis of the rules for constructing a flight trajectory of a communication aerial platform for data collection from nodes of a wireless sensor network.*

To collect monitoring data from the nodes of wireless sensor networks with a disconnected topology, it is proposed to use a communication aerial platform (CA), which is built on the basis of an unmanned aerial vehicle. During the flight, the CA forms temporary local networks and performs the role of an air gateway for collecting data from individual nodes and main nodes in connected network fragments. The efficiency of the data collection process depends on the characteristics of the network, the methods (rules) of constructing the trajectory of the CA, the number and location of points (intervals) of data exchange, etc. The article assesses the effectiveness of the application of various production rules for building the trajectory of a CA to collect data from network nodes to achieve certain target functions: minimizing the time of data collection, maximizing the time of network operation.

The paper formulates the task of finding a flight path and collecting CA data from nodes as the task of finding the shortest trajectory of the movement of the CA coverage area from the initial to the end point of the flight, which provides coverage of all nodes (clusters on the area) at the minimum distance of the CA exchange with the nodes. In order to evaluate the effectiveness of the application of the flight path construction rules and data collection, a corresponding simulation model was developed. The input data of the simulation are the characteristics of the network, nodes and communication aerial platform, methods (rules) of managing the data collection process. The simulation model provides an opportunity to obtain dependences of efficiency indicators (data collection time, battery energy consumption, network operation time) on a set of flight path construction rules and CA data collection with different input data.

The results of simulated modeling of the application of a set (base) of rules proved the possibility of reducing the time of data collection by up to 20% or increasing the time of network operation by up to 15% compared to existing solutions.

**Keywords:** wireless sensor network, communication aerial platform, flight path, data collection, rule base, modeling.

**1. Problem statement.** In recent years, the technology of wireless sensor networks (WSNs) has been rapidly developing as the transport basis of the Internet of Things to solve various problems for both civilian and military purposes [1–3]:

monitoring the parameters of objects (territories) for pollution (radiation, chemical, biological, etc.) and compliance with environmental standards;

monitoring the state of state borders, crop fields, forests, rivers, seas, food pipelines, power lines, bridges, etc;

assistance in search and rescue missions;

seismic monitoring, tracking the movement of wild animals, etc;

control of military operations and the battlefield (monitoring the status of their own and enemy troops, obtaining coordinates of movement of military equipment and personnel), etc.

The peculiarity of WSNs [1–3] is the limited resources of sensor nodes in terms of battery power, processor speed, memory capacity, transmitter power, etc. Modern WSNs can have hundreds or thousands of sensor nodes. The classical WSN architecture is a self-organizing radio network that transmits monitoring data along built-in routes from nodes to a radio gateway, which then transmits data to users via the communication infrastructure.

Certain areas of application of WSNs should consider the peculiarities of the nodes' location and the possibility of obtaining an unconnected network topology. For example, in remote areas affected by an emergency, with difficult terrain, occupied by the enemy, there is no possibility of using public communication infrastructure to organize communication with the gateway and it is impossible to build a connect topology of the entire network in conditions of a significant distance between nodes.

In these conditions, it is proposed to use a communication airborne platform (hereinafter referred to as the CA) as a mobile air gateway to collect data from network nodes [1–4]. In contrast to the classical architecture of data collection in sensor networks (an ad-hoc radio network with data collection along transmission routes between nodes to the gateway), this allows first, to organize the collection of monitoring data from unconnected network nodes; second, to obtain line-of-sight radio channels and shorter range, which reduces the level of energy consumption of nodes for data transmission (respectively, increases the network lifetime), etc.

This raises the urgent scientific task of analyzing the methods (rules) for constructing a trajectory for the overflight of the network nodes by the CA to collect data to achieve certain objective functions (hereinafter referred to as the "OF"): minimizing the time of data collection and/or minimizing the energy consumption of nodes (maximizing the network operation time) [3–5]. Solving this problem will allow optimizing the parameters of the data collection management system and improving its efficiency.

**2. Analysis of recent publications.** The use of CA for data collection in remote high-dimensional WSNs is a well-known solution and has been considered from different angles in many publications [1–16].

The first group of publications [5; 6] considers two ways of solving the problem of constructing a CA flight path:

flying over the entire territory of nodes [5] according to different models – horizontally, spiral, zigzag, Hilbert curve, etc.

most of the territory (number of nodes), considering the limitation on the maximum flight time of the CA (tractor, angular, circular, square flight models of the CA are proposed [6]).

The main disadvantage of the method of collecting data by flying over the territory is the significant time of data collection, but this method will be used during the initial flight of the network of CA to determine the actual parameters of the nodes (position coordinates, battery power level, amount of monitoring data).

The next group of publications [7–10] considers the construction of a CA flight path when collecting data from nodes only as a solution to the classical traveling salesman problem – finding the shortest route between the starting and ending points of the CA flight with a flight over nodes or data collection points (cluster centers). This problem belongs to the class of NP-hard problems. Obtaining an exact solution for a network of significant dimensionality is problematic. Therefore, heuristic algorithms for obtaining an approximate solution are proposed in practice, which have a low computational complexity: Lin-Kernighan traveling salesman heuristic (LKH) [8], Near Neighboring (NN) [9], Spiral Decomposition (SD) [10], Fast Path Planning with Rules (FPPWR) [11], Convex Hull Insertion Heuristic (CHIH) [12], ant algorithm [13], genetic algorithm [14], particle swarm algorithm [15], etc. However, such a problem statement calculates only the shortest flight route but does not consider the state of the nodes' parameters, nor does it optimize the energy consumption of the nodes. Therefore, the application of the shortest path search algorithm can be used for the initial (basic) solution for its further improvement.

The third group of publications defines [16–21] two main approaches to improve the efficiency of CA data collection from nodes of large-dimensional WSNs:

1. Collecting CA data directly from each node by creating virtual clusters at the actual location of the nodes.

2. Data collection only from the head nodes of real network clusters.

With the first approach (in the absence of connectivity between nodes), the network control center calculates temporary clusters (local radio networks: CA – nodes of the cluster) and forms them during the flight by the CA (air gateway). In the second case, if there is radio communication between certain sensor nodes, the network is self-organized and divided into real clusters with the identification of the main cluster nodes (according to well-known clustering algorithms LEACH, HEED, etc.) [16], which collect data from simple monitoring nodes. The CA flies around and collects data only from the main nodes of the clusters. In the following, we will take both approaches into account.

Publications [17–21] investigate the peculiarities of individual stages of the data collection process and ways to achieve the objective functions: minimum collection time, maximum area coverage (number of nodes), etc.

In [17], the problem of reducing the data collection time by sequentially adding potentially possible hang points is investigated. However, the search for variants of hang points leads to a significant computational complexity, so the proposed solutions can be used in a small-dimensional network.

In [18], several strategies for constructing data collection points from cluster nodes and the CA flight path in a temporary clustered WSN are investigated: through the center of the cluster, data collection on the flight path at the closest node-CA distance, flight through critical nodes in clusters, flight with hovering at one collection point that minimizes the total energy consumption of nodes, etc. However, the authors do not consider the possibility of building multiple data collection points in a cluster, optimizing exchange intervals, optimizing multiple objective functions.

In [19], rules (heuristics) for shortening the CA trajectory are considered by considering the direction of movement of the CA and the location of nodes in the cluster. Further improvement of these rules and evaluation of their effectiveness will be presented later in the article.

In [20], a deep neural network is used to find the 3D flight path of a CA considering the quality of the radio channel, but the set of performance indicators of the collection process is not considered.

In [21], it is proposed to achieve the objective function sequentially by hierarchy levels: network, cluster, CA, group of nodes, and individual node. At the network level, performance indicators are optimized by determining the number of clusters and their sizes, and building the shortest flight path. At the levels of a CA group of nodes and a CA node, the distance is determined, which allows optimizing the time of exchange between them and energy consumption (rules for

adjusting the points (intervals) of trajectory data collection are proposed). To reduce the number of options and reduce the time for finding a solution along the trajectory of overflying nodes and collecting data, an appropriate database of decision-making rules is proposed. However, no evaluation of the effectiveness of the rules and the weighting of their priority is given.

Thus, the unresolved task when considering the rules for constructing a CA flight path is to evaluate the effectiveness of their application and determine the order (priority) of application for constructing a data collection path for a particular WSN to achieve two main optimization criteria: minimizing the time of data acquisition and maximizing the network operation time.

**The aim of the article** is to analyze the effectiveness of applying the basic rules for building and correcting the flight path and collecting data from the nodes of the BSM by a communication air platform when achieving certain target functions.

**Presenting main material.** We consider a stationary wireless sensor network of considerable dimensionality (hundreds of sensor nodes) for special purposes. Each sensor node consists of the following basic elements: a battery, a certain set of sensors (e.g., vibration, magnetic, acoustic, etc.), a processor, memory, transceiver, antenna, positioning system, and control system.

During its operation, each sensor node collects and stores environmental parameters (objects of observation) of the monitoring zone assigned to it. The number of collection parameters is determined by the type of sensor modules, and the frequency and methods of data collection (by events, periodically, continuously) are determined by the ground-based network control center (NCC).

The WSN nodes are randomly located in a certain area and are unable to establish a unconnected topology for data transmission to the gateway for various reasons: a significant distance between them, specific terrain, lack of any public communication infrastructure, the need to periodically perform radio silence, economic inexpediency of installing and operating gateways, etc. In other words, under these conditions, the topology of a sensor network will consist of separate unconnected nodes and/or separate unconnected network fragments (clusters). Nodes in connected clusters (if they have an appropriate control system capable of implementing self-organization algorithms) can introduce a control hierarchy: form the head nodes of clusters that will collect and store data from other so-called simple cluster nodes [16].

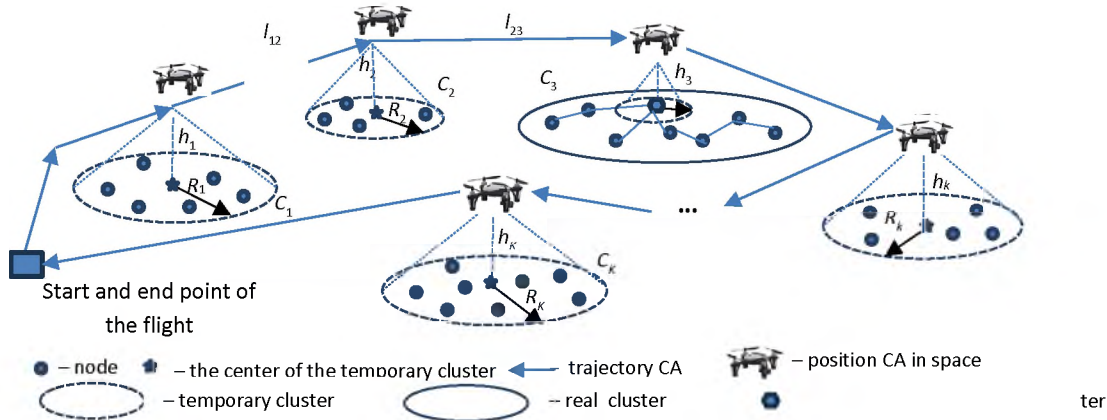
For WSNs with an unconnected topology, the role of a mobile gateway is played by an unmanned aerial vehicle (UAV) equipped with additional equipment to implement the process of collecting data from sensor nodes: processor, memory, transceiver, antenna, positioning system, and the corresponding control system.

At the planning stage, the NCC calculates the CA flight path and determines the preliminary points (segments) for collecting data from nodes in space. During the CA flight, thanks to a directional antenna at an altitude of  $h_k(t)$  forms temporary clusters (coverage and radio communication areas)  $C_k(t)$ ,  $k = 1 \dots K$  nodes with a radius of  $R_k(t)$ , that is, it creates temporary local radio networks with an air access point (CA). If during the flight of the CA some nodes (head nodes of real clusters of network fragments) fall into the current radio communication zone, then it: establishes radio communication with them (according to the MAC protocol), determines the exchange schedule and determines (or corrects) the point (interval) of the exchange trajectory. When the CA approaches the point (interval) of data collection on the trajectory, the node-CA data exchange process takes place (Fig. 1).

*Given:*

1. Characteristics of the wireless sensor network:
  - the area of the WSN ( $S$ ) and the type of its geometric shape (for example, rectangular, strip, circle, arbitrary, etc.)
  - the number of network nodes (unconnected and/or head nodes of real clusters), coordinates of their location on the ground  $(x_i, y_i)$ ,  $i = 1 \dots N$ ;
  - density of node placement  $\alpha = \bigcup_{k=1}^K \pi R_k^2 / S$  nodes (where  $R_k$  – radius  $k$ -th coverage area of the CA,  $k = 1 \dots K$ ) and the type of their placement (homogeneous, grouped, etc.);

– the amount of monitoring data collected by each  $i$ -th node –  $V_{dmi}$ .



**Fig. 1.** An example of a CA overflight of clusters and data collection from cluster nodes

2. Characteristics of the node:

- technical characteristics of the node – number and types of sensors, battery power level, energy consumption for monitoring environmental parameters for each type of sensor, etc.;
- communication characteristics of the node – parameters of the antenna, transmitter, energy consumption per bit of reception and transmission for the selected MAC protocol and type of equipment, etc.

3. Characteristics of the communication aeroplatform:

- flight characteristics – speed, altitude, flight time, battery energy, ability to hover and move in space at a constant or variable speed, etc.;
- communication characteristics – MAC protocol, antenna and transceiver parameters, etc.

4. Objective control functions (1)–(4) of data collection implemented by the NCC [21]:

- minimize data collection time  $T_{col}$

$$T_{col} = \frac{L}{v} = \sum_{m=1}^M \frac{l_m}{v_m} \rightarrow \min \quad (1)$$

ensuring a given network operation time  $T_{fun} \geq T_{fungiv}$ ,

$l_m, v_m, m = 1 \dots M$  – trajectory intervals between data collection points and flight speed;

- maximize network operation time  $T_{fun}$  by reducing (redistributing) the energy consumption of nodes  $e_{coni}$

$$T_{fun} \rightarrow \max \quad (E_{con} = \sum_{i=1}^N e_{coni} \rightarrow \min) \quad (2)$$

ensuring the specified data collection time  $T_{col} \leq T_{colgiv}$ ;

$$\text{– optimization of both criteria} \quad \begin{cases} T_{col} \rightarrow \min \\ T_{fun} \rightarrow \max \end{cases} \quad (3)$$

- obtaining an acceptable solution

$$T_{col} \leq T_{colgiv} \text{ and/or } T_{fun} \geq T_{fungiv}, \quad (4)$$

with restrictions  $\Omega$ :

– type of CA (rotary); speed  $v=[v_{min}, v_{max}]$ , altitude  $h=[h_{min}, h_{max}]$ , time  $t_{fly} \leq t_{flymax}$  and the range of its flight  $L \leq L_{max}$ ;

– number of clusters in the network –  $1 \leq k \leq K$ ;

– initial energy of the node batteries  $e_i \leq e_{max}$  and KA  $e_{KA} \leq e_{KAmax}$ ;

– the amount of monitoring data for each  $i$ -th node –  $V_{dmi} \leq V_{dmmax}$ ;

– radio communication range between node and CA –  $d_{i-TA} \leq d_{max}$  – the propagation of radio waves in line-of-sight conditions is considered;

– radius of the CA coverage area (cluster) –  $R_{min} \leq R \leq R_{max}$ .

Network operation time  $T_{fun}$  can be determined by the following indicators:

a) The period of stable operation of the network  $T_{pso}$  (5) – network operation time (monitoring and data transmission in each round of the CA flight) until the first node fails due to battery depletion

$$T_{pso} = \min_{i \in N} t_{funi}(Nround), \quad (5)$$

where  $t_{funi}$  – is the time of operation of the  $i$ -th node before its failure, which is determined by the number of rounds of circling ( $Nround$ ).

б) Percentage of nodes that failed (6) relative to the number of CA rounds

$$T_{fun} = \frac{N_{fail}(Nround)}{N} \text{ as a percentage}, \quad (6)$$

where  $N_{fail}(Nround)$  – the number of nodes where the battery energy is less than the permissible level on the  $Nround$  round.

5. A set of methods (rules) for constructing a flight path and collecting CA data from the WSN nodes.

*Restrictions and requirements:*

– the CA flight area has no prohibited zones, its flight trajectory is formed in the form of certain coordinates of points in space, modeling of the CA flight process is not considered;

– information on node status parameters (location coordinates, battery energy level, amount of monitoring data) is collected during the initial overflight of the CA network, and then the information on the node status is updated during each round of overflight;

– the CA has the ability to collect data both during hovering and during flight;

– The CA and sensor nodes have radio facilities with the same MAC protocol, which allows to change the data transmission rate depending on the state of the radio channel (signal-to-noise ratio) and to regulate the transmission power (energy consumption for transmission), for example, IEEE 802.11;

– memory capacity of sensor nodes and CA is sufficient to store monitoring data;

– the energy value of the CA battery is sufficient for a round of network overflight;

– algorithms for controlling the data collection process, which are implemented by the control systems of nodes and CA, should have a low computational complexity due to the need to implement autonomous flight and ensure the data collection process in real time.

***It is necessary to:*** to analyze the effectiveness of applying various rules for constructing and correcting the CA flight path to collect data from the WSN nodes while achieving certain objective functions.

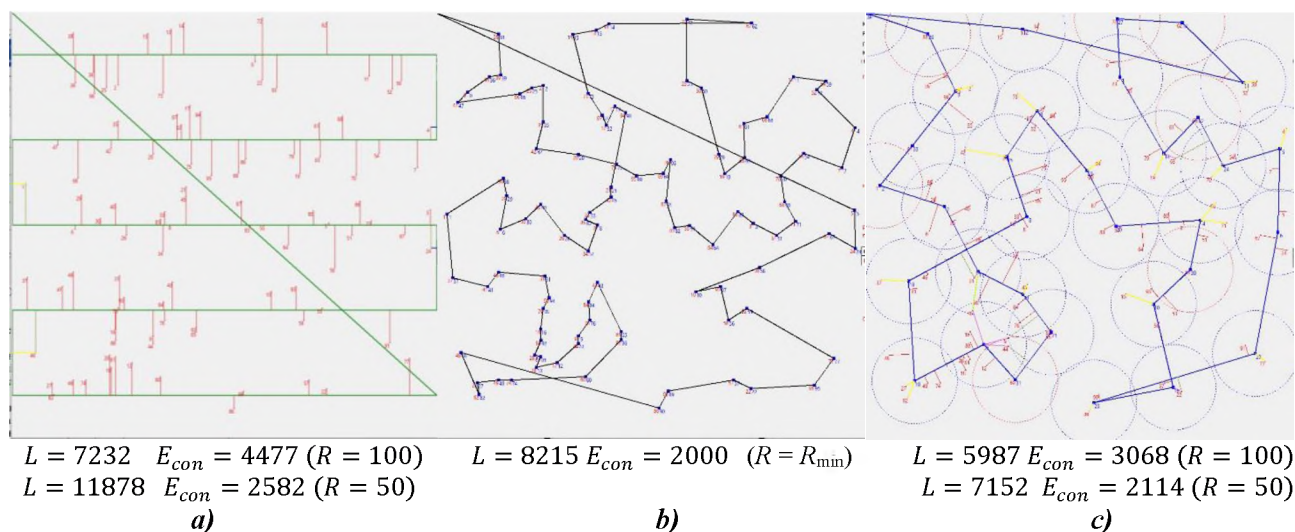
***Solution.***

The set of solutions for achieving the defined objective functions (1)–(4) lies between two limiting methods: flying over the entire area of the WSN and flying over each node of the network.

**1. CA overflight of the entire territory (area) occupied by the WSN nodes**, with simultaneous collection of monitoring data from network nodes. Thus, studies [5; 6] analyzed various options for flying over the entire area and collecting data from the main nodes of real clusters: by lanes (Fig. 2, *a*), by angle, by square, by circle. The aim of the study is to find overflight options that allow to reduce the length of the overflight route or maximize the number of serviced (covered) nodes for a limited time of the CA flight. It is shown that there is no single optimal overflight option: the "strip" option is effective for maximizing the coverage area of the CA, the "circle" option is more efficient in terms of overflight time. However, the length of the route and the flying time over the entire area of the CA remains very long. For example, according to the results of the authors' simulation modeling for a network of 100 nodes, the length of the CA trajectory when flying over the entire area horizontally at  $R=100$  is  $L=7500$  at the total energy consumption of the nodes  $E_{con} = 4477$ . When the coverage radius is reduced by half  $R=50$  the length of the trajectory is already  $L=11878$  with a halving of energy consumption to the value of  $E_{con} = 2115$  (Fig. 2, *a*), which imposes additional requirements on the flight characteristics of the CA. The overflight of the entire



network will usually be used during the initial overflight of the network to collect initial information about the parameters of the network nodes (position coordinates, amount of monitoring data, battery energy level, etc.).



**Fig. 2.** Ways to fly CA around the WSN nodes:

*a* – the entire area of the WSN ("by lanes"); *b* – of each node; *c* – temporary clustering

**2. Flying around each node at the minimum flight altitude of the CA.** As a result of the simulation of this method, we obtain the minimum energy consumption of nodes for data exchange  $E_{con} = 2000$  (due to  $R \leq R_{min}$ ) and a significant length of the route  $L = 8215$  (Fig. 2, *b*). It is advisable to use this method to minimize energy consumption – objective function (2), but it is not guaranteed that the flight time (data collection) limit will be met  $L \leq L_{max}$ . Different types of algorithms can be used to solve the problem of finding the shortest route to fly around each of the nodes: full search (for WSNs of small dimensionality), heuristic (NN – Fig. 2, *b*, FPPWR, CHIH, etc.), genetic, etc. Each of them shows different results depending on the network parameters and implementation features (see below in Section 3).

The results of modeling the performance evaluation indicators of the first two methods are borderline and are used for comparison with the results of applying other methods.

**3. Between the above two limiting ways of flying over the CA (the entire area and each node) is a hybrid variant of flying over (temporary clustering of the network) – flying over only certain zones (clusters) of the WSN area (for example, through the centers of the clusters, Fig. 2, *c*), in which groups of nodes or individual nodes are actually located.**

That is, the classical salesman problem is transformed into **the problem of finding the shortest route (or rather trajectory) to move the CA coverage area from the starting to the end point of the flight, which ensures coverage of all nodes (points on the area) at the minimum distance of exchange between the CA and the nodes.**

Achievement of the objective functions (1)–(2) has the opposite dependence. Reducing the length of the CA trajectory leads to an increase in the distance between the CA and the nodes and, accordingly, an increase in the energy consumption of the nodes for data transmission and vice versa. Therefore, it is proposed to use the lexicographic method to solve the two-criteria optimization problem (3). To do this, before the CA flight, the ground-based NCC determines the priority of the objective functions in accordance with the current operational situation. It is proposed to search for the optimal solution according to the hierarchy according to the priority of the objective functions in the following steps [21]:

virtual clustering of the network is carried out according to a certain cluster analysis algorithm - it is proposed to use the iterative cluster analysis algorithm FOREL (FORMal Element), which has certain advantages over others – low computational complexity, correspondence of the cluster concept to the physical content of the CA coverage area, etc;

the shortest (or permissible length) route for flying around the data collection points is built according to a certain algorithm for solving the salesman problem;

the data collection points (intervals) of CA monitoring in clusters are determined according to the adopted cluster overflight strategy and the priority of the objective functions (in the simplest case, the center of the cluster is determined as the data collection point).

It should be noted that the effectiveness of the final optimization solution and the speed of its obtaining (computational complexity) is largely determined by the initial clustering solution (depending on the choice of the starting point of the area and radius of coverage of the satellite), the algorithm for finding the shortest flight path, the strategy of flying around the nodes in the cluster, etc.

So data collection time  $T_{col}$  of CA from the network nodes depends on the following parameters (5):

$$T_{col} = f(N, K, TR(St_k), v, V_{dmi}, Q_k, INT_i, s_{i-CA}(d_{i-CA}, MAC), h_k, \Omega) \quad (5)$$

– number of nodes  $i = 1 \dots N$  and the coordinates of their location on the ground  $(x_i, y_i)$ ;

– quantities  $k = 1 \dots K$  clusters, their area, the number of nodes in a cluster  $n_k$ , and their relative position;

– trajectories  $TR$  of the CAs flight in the network defined by the strategy  $St_k$  overflight and data collection from the nodes of each  $k$ -th cluster (data collection during the flight and/or when the CA is hovering, one or more hovering points in the cluster, etc;)

– speeds  $v = \{v_m\}$  CA flight on each of the trajectory segments  $l_m, m = 1 \dots M$ ;

– the amount of monitoring data  $V_{dmi}$  in network nodes;

– number of data collection points  $Q_k$  with coordinates in space  $(x, y, h)_k$  in each  $k$ -th cluster when the CA hangs up;

– locations in the space and time of intervals  $INT_i = \{(x, y, h)_{begin}, (x, y, h)_{finish}, t_{begin}, t_{finish}\}_i$  CA flight trajectories, which are defined for data collection (exchange) in motion with the  $i$ -th node;

– transmission speed of the MAC protocol  $s_{i-CA}(d_{i-CA}, MAC)$ , which depends on the distance  $d_{i-CA}$  and parameters of the radio channel (signal-to-noise ratio), transmitter, receiver, antennas, etc;

– flight altitude  $h_k$ , limitations  $\Omega$  resources of nodes and CA, etc.

Increase in network operation time  $T_{fun}$  can be achieved:

reducing the energy consumption of nodes for data reception and transmission (reducing the transmission power of the node) by reducing the distance between the CA and the node

$$d_{i-CA} = g(K(R_k), n_k, TR_k, Q_k, INT_i),$$

which is achieved by optimizing the number of clusters  $K$  (the size of the coverage area  $R_k$ ), is the number of nodes in the  $k$ -th cluster  $n_k$ , trajectories  $TR_k$ , position of the points  $Q_k$  (intervals  $INT_i$ ) exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster exchange in the cluster;

redistribution of energy consumption between nodes competing for transmission (if a node has a higher battery energy level, then it must consume more energy).

In addition, when determining the trajectory of the cluster nodes and data exchange, it is necessary to take into account:

– relative location of nodes relative to the trajectory (it is desirable to exchange data in the nearest intervals of the CA flight trajectory from the node);

– critical energy level of the node's battery (plan to fly over "exhausted" nodes at a minimum distance);

– the amount of node monitoring data – selecting the point (interval) of trajectory collection that is closer to this node.



A simulation model was developed to evaluate the effectiveness of the proposed different methods (algorithms, rules) of collecting data from WSN nodes by CA. It is written in Python, has a user-friendly interactive interface, and allows visual tracking of all stages of the process of collecting CA data from network nodes.

The input data for the modeling are as follows.

1. Characteristics of the network, nodes, CA (according to the problem statement):  $S=1000 \times 1000$  conventional units;  $N = 50 \dots 200$ ; node placement (homogeneous, with grouping), the initial energy of the nodes and the amount of monitoring data  $e_i$ ; energy consumption of the node for transmission (calculated by a simplified formula  $e_{con} = c * d_{i-CA}^2$ , where  $c = \text{const}$ ,  $d$  – distance between the node and the CA); coverage radius  $R$ ; radio communication range between node and CA –  $d_{i-CA}$ ; number of overflight rounds  $N_{round}$  etc.
2. Methods (from the whole area, from each node, by clusters), methods (directly from each node, from the head nodes of clusters) of data collection.
3. Algorithms for temporary network clustering (FOREL,  $k$ -averages, etc.).
4. Algorithms for finding the shortest route: heuristic (nearest neighbor, FPPWR, CHIH, etc.).
5. Clustering rules, determination of data collection points (intervals) on the CA flight path rules, cluster overflight rules, rules for building the CA path, etc. (Table 1) [21].

Table 1

**Decision-making hierarchy for collecting CA data from the WSN nodes**

The stage decision	Managed parameter	Action (rule)	
		Objective function $\min T_{col}$	Objective function $\min E_{con}$
1. Virtual clustering of the WSN (network level)	Number and size of homogeneous clusters $R^*$ , starting point of clustering, number of nodes in clusters, size of each cluster $R_k$	Reduce the number of clusters: increase $R$ , determine the starting point of clustering in the places of grouping nodes, redistribution of nodes between clusters	Increase the number of clusters: reduce $R$ while maintaining connectivity between cluster nodes and CA
2. Search for the initial flight trajectory of the CA (network level)	An algorithm for finding the shortest route (trajectory) to fly around the centers of clusters (collection points) of the WSN	Selection of the best heuristic algorithm from the set, optimization of the algorithms' own parameters	–
3. Adjustment of data collection points in each cluster (cluster level)	Position of the data collection point (interval) relative to the CA trajectory and location of the cluster nodes	Rules for trajectory shortening in a cluster when ensuring radio communication CA - the farthest node	–
4. Determination of the data collection strategy in the cluster (cluster level)	Location of the trajectory relative to the position of the nodes in the cluster, number and position of data collection points	Rules for reducing the distance of a CA node that has a significant amount of data (reducing the exchange time)	Rules for reducing the node-CA distance for battery power consumption
5. Correction of collection points (intervals), calculation of the CA-node exchange schedule (CA node level)	Number of points (length of intervals) of data collection on the CA trajectory segments, CA flight speed	Redistribution of collection points along the CA trajectory segments, selection of the maximum flight speed while meeting the exchange time	Rules for the priority of exchange of node-CA with a lower (low) battery energy level

The simulation model provides an opportunity:

to obtain dependencies of performance indicators (data collection time (trajectory length), battery power consumption, network operation time) on a set of control parameters (rules) for

building a flight path and collecting CA data under different input data (network dimension, type of node location, number of overflight rounds, etc;)

explore the optimization parameters – the number and size of clusters, the number and location of data collection points (intervals) on the flight path, cluster flying strategies; algorithms for finding the shortest route, etc.

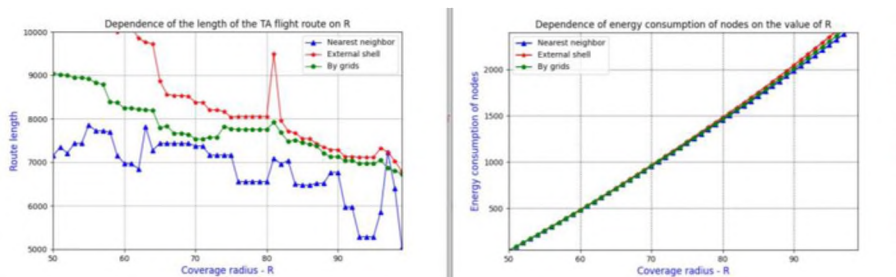
Let's model and evaluate the effectiveness of each stage of solving the problem of collecting CA data from the WSN nodes and the corresponding rules for their implementation

**1. Finding a solution for network clustering – optimization of CA coverage areas.**

Reducing the number of clusters  $k$  in the network potentially reduces the length of the CA flight route (and thus the data collection time), but leads to an increase in sensor node energy consumption (due to the increase in the node-CA distance) and an increase in node-CA communication time (decreases the MAC protocol transmission rate). And vice versa: an increase in the number of clusters leads to an increase in the length of the CA flight route, but reduces the node-CA distance and, accordingly, reduces their exchange time and node energy consumption. In other words, there is a certain optimum of the number of clusters  $k^*$ , their size  $R^*$ , and the location of points in them  $Q_k$  and intervals  $INT_i$  CA data collection, which determines a compromise decision regarding the TF. Therefore, the following basic rules apply [21].

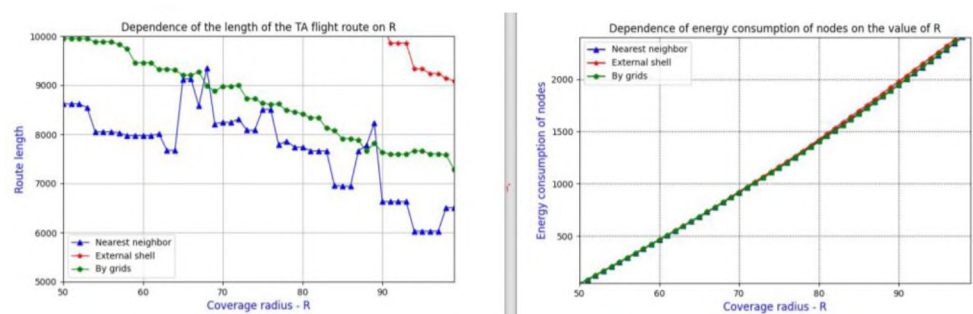
*The rule for determining the number of clusters in the network:* IF the priority of the objective function  $T_{col} \rightarrow \min$  ( $T_{fun} \rightarrow \max$ ), THEN increase (decrease) the size and number of clusters.

The results of the study of the proposed rule when applying various heuristic algorithms for finding the shortest path (nearest neighbor, FPPWR, CHIH) through the centers of clusters are shown in Fig. 3 and Fig. 4 ( $N = 100$ , nodes have the coordinates shown in Fig. 2). Cluster size is optimized  $R^*$  within the values of  $R = 50 \dots 100$  for each of the algorithms. According to the FOREL clustering algorithm, the number of clusters is determined  $k = 69 \dots 33$ . We observe that for each shortest path search algorithm there is an optimal value of  $R^*$  ( $R_{NN}^* = 94, R_{FPPWR}^* = 100, R_{CHIH}^* = 100$ ), which allows to significantly (more than 20%) reduce the primary length of the CA flight path.



**Fig. 3.** Estimation of the trajectory length and energy consumption of nodes as a function of the coverage area size  $R$  with homogeneous node placement under different shortest route search algorithms

For a network with grouped nodes, the simulation results are shown in Fig. 4.



**Fig. 4.** Estimation of the trajectory length and energy consumption of nodes as a function of the coverage area size  $R$  when nodes are placed in groups

The application of other network rules (Table 1) affects the number of clusters and, accordingly, the length of the route, the energy consumption for the exchange of CA data with nodes.

*The rule for selecting the initial clustering point:* to select the initial clustering point of the network, select the point with the maximum number of nodes in the cluster (the goal is to reduce the number of clusters).

*The rule for redistributing nodes between clusters:* IF there is a small number of nodes in a cluster, then redistribute the nodes of this cluster to other clusters if possible (i.e. reduce the number of clusters).

*The rule for adapting the size of each cluster:* IF objective function (2) THEN reduce  $R$  by reducing the flight altitude of the CA while maintaining the connectivity of the CA nodes in the cluster.

The benefit of applying these rules can reach 5–7 %.

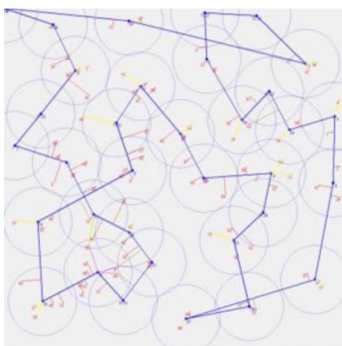
That is, optimization of the coverage area radius, application of the rules (selection of the initial clustering point at the planning stage, redistribution of nodes between clusters, adaptation of cluster sizes) has a significant impact on the efficiency of the data collection process during network operation..

## 2. Rules for finding the shortest route (trajectory) for flying over CA clusters.

To solve the problem of finding the shortest route to fly around each cluster, various known algorithms can also be used: full search (for a small number of clusters), heuristic, genetic, etc. Each of them shows different results depending on the parameters of the network, nodes, and CA. Figures 5–8 show the performance indicators ( $L$ ,  $E_{con}$ ,  $T_{fun}$ ) when using three heuristic algorithms for finding the shortest path (NN, FPPWR, CHIH) with homogeneous and group placement of nodes, the size of the coverage area ( $R = 50, 100$ ), network dimensions ( $N = 100$ ).

The modeling results demonstrated a significant dependence of the performance indicators on the nature of the location of universities in the area (homogeneous, grouped) and the adopted algorithm for finding the shortest route to fly around the clusters. In our case, in most cases, the nearest neighbor algorithm has the advantage of the three defined algorithms with the best performance indicators.

In addition, for each of the algorithms, there is an additional possibility of optimization by the internal parameters of the shortest path search algorithms themselves. For example, the nearest neighbor algorithm can be used to select the number of steps to the next cluster (one, two, three, etc.), by squares (optimizing the size of a lattice square), convex hull (optimizing the size of each hull). At the same time, for specific network parameters (area, placement, node parameters, CA, etc.), each of them may have an advantage.



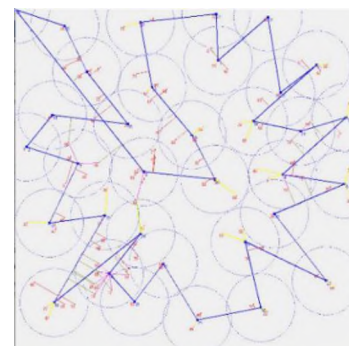
$L = 5987$   $E_{con} = 3068$  ( $R = 100$ )

a)



$L = 6596$   $E_{con} = 3157$  ( $R = 100$ )

b)

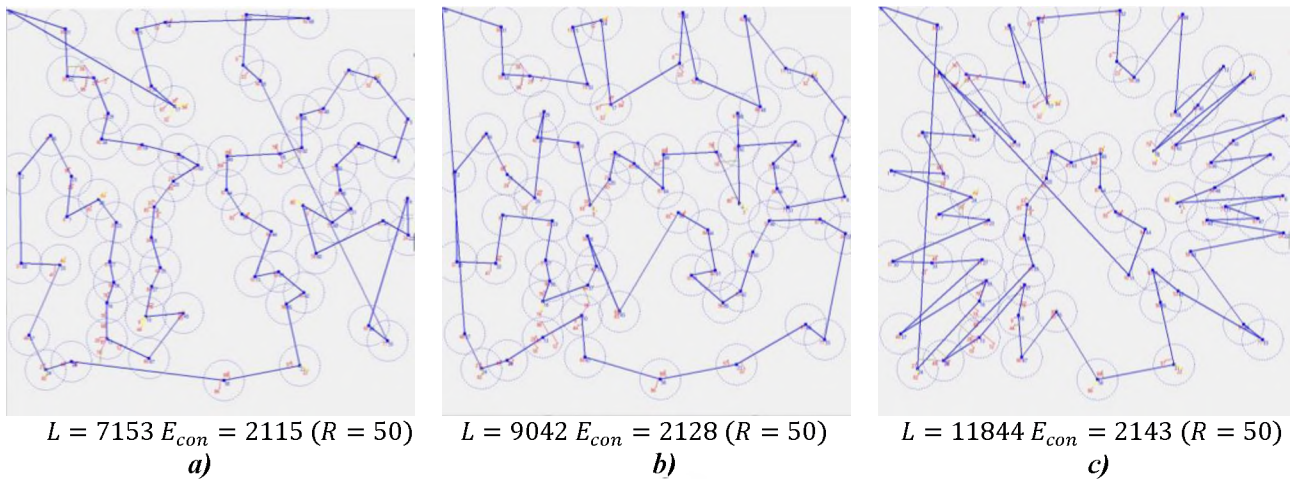


$L = 6899$   $E_{con} = 3290$  ( $R = 100$ )

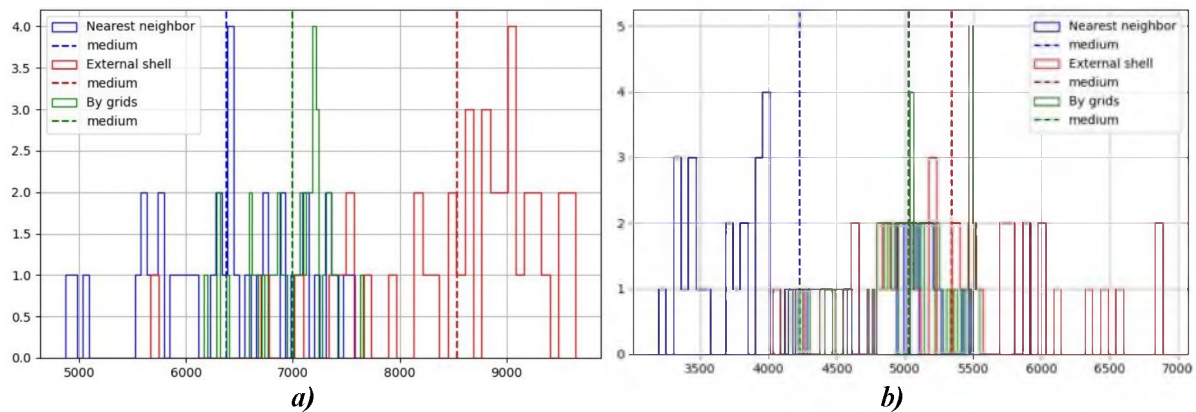
c)

**Fig. 5.** Results of modeling the trajectory of a CA flight in a clustered network with uniformly distributed nodes in the WSN using different shortest route search algorithms ( $N=100$ ,  $R=100$ ):

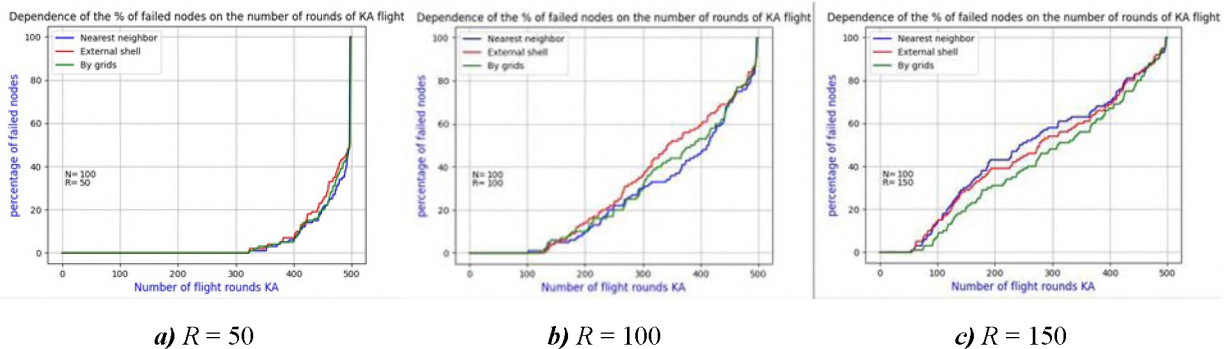
a – the nearest neighbor; b – FPPWR; c – CHIH with 2-layer shell



**Fig. 6.** The result of modeling the trajectory of a CA over a clustered WSN by grouping nodes using different shortest route search algorithms ( $N=100, R=50$ ):  
*a* – the nearest neighbor; *b* – FPPWR; *c* – CHIH 2-layer shell



**Fig. 7.** The result of modeling and estimating the length of the CA flight route of uniformly distributed and grouped nodes in the WSN using different algorithms for finding the shortest route ( $R=100$ , a sample of 100 random locations of nodes on the area):  
*a* – uniform placement of nodes; *b* – grouping of nodes



**Fig. 8.** Dependence of network operation time on the number of CA rounds and coverage radius ( $N = 100$  at  $R = 50, 100, 150$ )

### 3. Rules for calculating (adjusting) data collection points in a cluster with a reduction in route length to improve the basic solution (through cluster centers).

The task of finding the shortest route for a CA flight differs from the classical traveling salesman problem. In our formulation of the problem, it is enough for a node to fall within the



coverage area of the CA. Therefore, let us consider heuristic rules for shortening the route relative to the initial solution (see sections 1, 2) (Fig. 9) [19; 21].

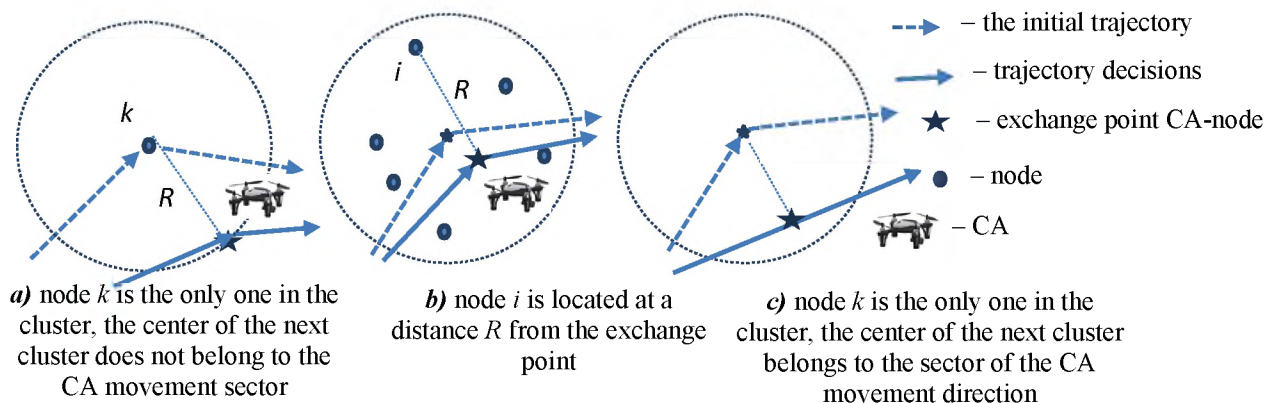


Fig. 9. Illustration of rules for reducing flight path length and CA data collection

*Rules for reducing the length of the CA flight path in a cluster (Fig. 9).*

IF the priority objective function  $T_{col} \rightarrow \min$ , the initial cluster flight route passes through the center of the cluster with one node  $k$ , and the next cluster center does not fall in the sector of the CA movement direction, THEN determine the point on the tangent line at a distance  $R$  from the new route in the CA movement direction as the data collection point (Fig. 9, a).

IF the priority objective function  $T_{col} \rightarrow \min$ , the initial route of the cluster overflight passes through the center of the cluster, the  $i$ -th node is at the greatest distance from the CA flight path, THEN determine the point that is at a distance  $R$  from the new route in the direction of the CA movement as the data collection point (Fig. 9, b).

IF the priority objective function  $T_{col} \rightarrow \min$ , the initial route of the cluster flight passes through the center of the cluster with one node  $k$ , and the next center of the cluster falls in the sector of the direction of movement of the CA, THEN the trajectory of movement is built directly to the next center of the cluster. determine the point on the trajectory closest to the center of the cluster as the data collection point (Fig. 9, c).

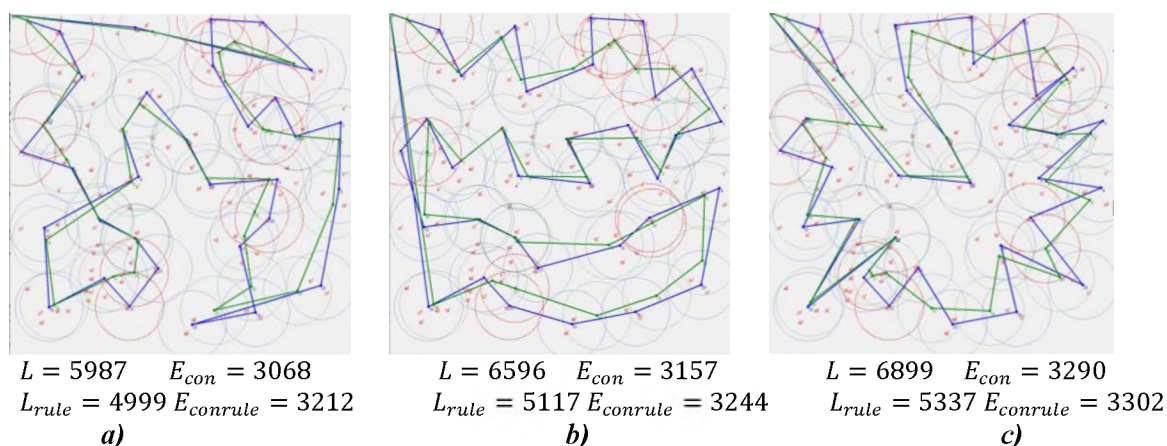


Fig. 10. Results of modeling the application of route shortening rules ( $N=100, R=100$ ):  
 a – the nearest neighbor; b – FPPWR; c – CHIH 2-layer shell

Based on the results of the simulation of the rules for shortening the route length, we can conclude that the trajectory length is reduced by up to 20 %, while energy consumption increases by

up to 10 %. According to the simulation results (Fig. 10), the heuristic with the nearest neighbor algorithm wins again, but with other network parameters, any algorithm for finding the shortest route can show the best performance.

#### 4. Rules for selecting points (intervals) of CA data collection in clusters (overflight strategies).

At the cluster level, the number and coordinates of the points (intervals) of data collection of the CA (cluster overflight strategy) are determined. Possible variants of point selection rules are shown in Fig. 11 [18; 21]:

a – selection of exchange points closer to the CA trajectory (through the center or center of mass of the cluster);

b – data collection only when the CA hovers in the center (center of mass) of the cluster;

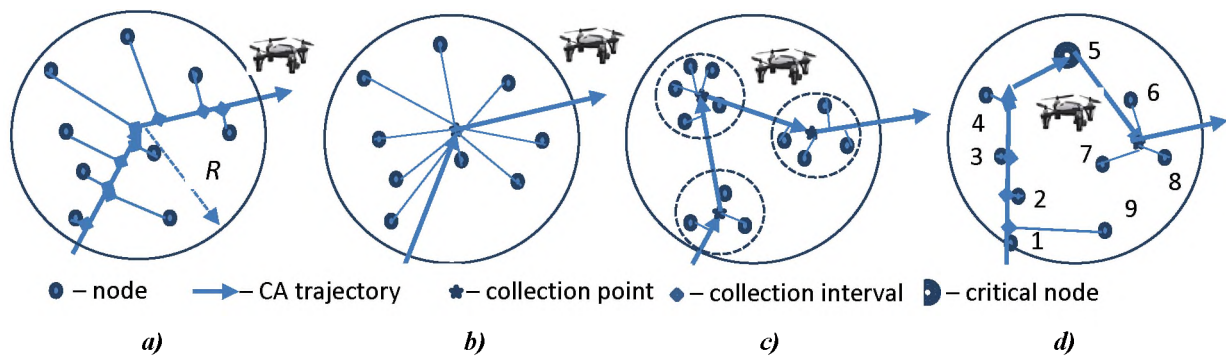
c – in-flight data collection with additional clustering if there are groups of nodes;

d – in-flight data collection taking into account the low battery energy level of individual nodes.

The result of each strategy in the  $k$ -th cluster is evaluated by a set of parameters:

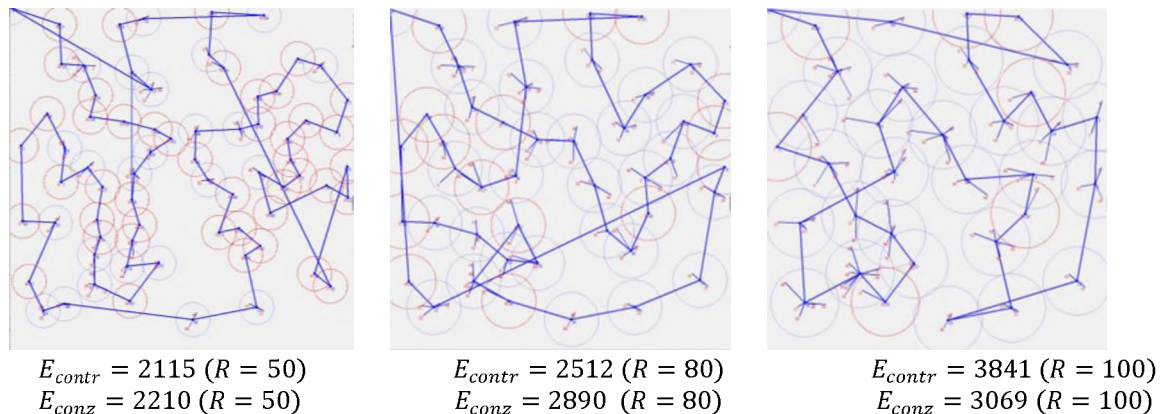
– is the energy consumption of each cluster node for data collection (transmission and reception)  $e_{coni}$ , the total energy consumption of cluster nodes  $E_{con}^k = \sum_{i \in \kappa} e_{coni}$ ;

– time of data collection in the cluster  $t_{con}^k$ , which is determined by the flight time and hover time of the CA.



**Fig. 11.** Basic rules for determining points (intervals) of CA data collection in a cluster:  $a$  – in the flight;  $b$  – only in the center of the cluster;  $c$  – with additional clustering;  $d$  – through critical nodes

The simulation results showed a reduction in node energy consumption when using the in-flight data collection strategy (Fig. 11,  $a$ )  $E_{contr}$  compared to collecting data only in the center of the cluster  $E_{conz}$  (Fig. 11,  $b$ ) – up to 20% reduction in node energy consumption for reception and transmission (Fig. 12).



**Fig. 12.** Results of modeling two strategies for flying around clusters (along the trajectory and only in the center)

If there is a grouping of nodes in the cluster, it is advisable to carry out their additional clustering in order to reduce energy consumption and reduce the exchange time (with a significant amount of monitoring data in the nodes) – Fig. 11, *c*.

*The rule for determining the hover points for data collection:* IF there is a cluster of nodes in the cluster (loaded or with low battery energy), THEN determine the hover point for collecting data from these nodes in the cluster that minimizes the communication time or energy consumption of these nodes.

*Rule for correcting the CA flight path:* IF it is necessary to reduce the transmission time in the node-CA radio channel and/or reduce the energy consumption of the node, THEN it is necessary to place (move) the exchange points on the satellite path closer to the node.

*Rule for reducing and equalizing transmission energy costs:* IF multiple nodes compete for exchange intervals with the CA, THEN determine the closest exchange interval *INT* on the CA flight path of a node with a lower battery energy.

*Rules for determining the number and location of hover points, exchange intervals, overflight and exchange strategies in the cluster:*

IF objective function  $T_{col} \rightarrow \min$ , the number of nodes in the cluster is small (average) and the amount of data is insignificant, THEN determine the basic strategy (flight of the CA through the center of the cluster with the determination of exchange intervals on the flight path) (Fig. 11, *a*);

IF objective function  $T_{fun} \rightarrow \max$ , a large number of nodes in the cluster, their data volume is significant, THEN cluster the cluster with the definition of additional hang points (Fig. 11, *d*).

#### **5. Rule with redistribution of nodes in different intervals of the constructed CA trajectory.**

Each constructed CA flight trajectory consists of segments between collection points, which can be estimated by the length of the segment  $l_m$  and the number of exchange points. If there are trajectory intervals with a significant (very small) number of collection points, then we try to add (remove) nodes to (from) it and re-cluster without taking into account the added (removed) nodes. The goal is to shorten the length of the trajectory or reduce the energy consumption of the nodes.

*Rule for redistribution of data collection points:* IF a trajectory segment has a significant (small) number of collection points, THEN fix this trajectory segment, delete (redistribute) nodes according to the objective function and re-cluster the network to achieve a certain objective function.

The results of modeling the application of the proposed rule demonstrated the possibility of obtaining a gain in efficiency of up to 8 %.

The interval of exchange between a node and a CA is determined by the following considerations: the node's flight time should be at least as long as the exchange time [21].

Since each rule is focused on achieving a certain objective function, it has a different result of its achievement, therefore, their hierarchy in the form of meta-rules is proposed. For example [21].

**Meta rule 1:** IF objective function  $T_{col} \rightarrow \min$ , THEN (single-criteria optimization) to find:

- the maximum (specified) number of network clusters;
- set the basic trajectory of the CA through the center of the clusters, find the shortest path (use one algorithm from the set to find the shortest path) to fly around the centers;
- apply the rules for reducing the route length, determine possible additional collection points (hovering) of the CA in accordance with the position and amount of data in the cluster nodes (grouping of nodes with a significant amount of data);
- determine the strategy of flying around the cluster nodes;
- set the maximum speed of CA movement in the cluster that meets the requirements for data exchange between CA and cluster nodes;
- calculate the intervals and schedule of node transmissions during the CA flight, taking into account the state of the nodes, using rules that are focused on increasing the transmission rate in the radio channel.

**Meta rule 2:** IF objective function  $T_{col} \rightarrow \min$  and  $T_{fun} \rightarrow \max$ , the first objective function takes precedence over the second, THEN (lexicographic optimization method):

- find the maximum (defined) number of network clusters;
- determine the collection points (hovering) of the CA in accordance with the priority of the objective function;
- determine the strategy of flying around the cluster nodes;
- calculate the trajectory of the CA through the collection points;
- calculate the intervals and schedule of node transmissions during a flight at a minimum distance using rules that take into account the available energy of the nodes.

Evaluation of the effectiveness of the application of meta-rules showed the possibility of reducing up to 20% of the data collection time and increasing up to 15% of the network operation time compared to previously proposed solutions. It is important to note that the proposed situational management model [21] can be used in special software of the data collection management system of the NCC and CA. The low computational complexity of the model allows the use of CA in an autonomous mode and making (correcting) decisions in real time.

**Conclusions.** The only solution for collecting data from WSN nodes with an unconnected topology is the use of communication aerial platforms. In this case, the task of building a CA flight path with the determination of data collection points (intervals) to ensure the main objective functions: minimum data collection time and/or maximum network operation time.

A specific WSN will differ in many parameters: area size and shape; number, coordinates and density of nodes, their relative positioning; battery power level, amount of monitoring data; characteristics and limitations of nodes and CA parameters, etc. The developed simulation model was used to study the dependence of data collection efficiency indicators on the application of various rules for constructing a CA flight path with certain network, node, and CA parameters. It is proved that there is no single method (set of rules) for finding a CA flight path that provides an optimal solution for all variants of the WSN and possible situations on the network.

To optimize the decision on the flight trajectory and data collection, a rule base is proposed that implements a hierarchy of rules for achieving the objective functions. The research made it possible to determine the priority and order of application of the rules in the database, i.e., the development of meta-rules. The results of simulation modeling have shown that the use of the rule base can reduce the data collection time by up to 20 % or increase the network operation time by up to 15 % compared to existing solutions.

**The direction of further research** is to improve the rule base for building a flight path and collecting CA data from the WSN nodes for other objective control functions.

## REFERENCES

1. Amodu O.A., Nordin R., Jarra C., Bukar U.A., Raja Mahmood R.A., Othma, M.A. (2023). Survey on the Design Aspects and Opportunities in Age-Aware UAV-Aided Data Collection for Sensor Networks and Internet of Things Applications. *Drones*, 7, 260. DOI: <https://doi.org/10.3390/drones7040260>.
2. Minh T. Nguyen, Cuong V. Nguyen, Hai T. Do, Hoang T. Hua, Thang A. Tran, An D. Nguyen, Guido Ala, and Fabio Viola. (2021). UAV-Assisted Data Collection in Wireless Sensor Networks: A Comprehensive Survey. *Electronics*. 10, 2603. DOI: [10.3390/electronics10212603](https://doi.org/10.3390/electronics10212603).
3. Imad Jawhar, Nader Mohamed, Jameela Al-Jarood (2015). UAV-based data communication in wireless sensor networks: Models and Strategies. *International Conference on Unmanned Aircraft Systems (ICUAS)*. DOI: [10.1109/ICUAS.2015.7152351](https://doi.org/10.1109/ICUAS.2015.7152351).
4. V. Romaniuk, O. Lysenko, A. Romaniuk, O. Zhuk (2020). Increasing the efficiency of data gathering in clustered wireless sensor networks using UAV. *Information and Telecommunication Sciences*, 11 (1), 102–107. DOI: [10.20535/2411-2976.12020.102-107](https://doi.org/10.20535/2411-2976.12020.102-107).



5. Zhiqing Wei, Mingyue Zhu, Ning Zhang, Lin Wang (2022). Zhiyong Feng UAV Assisted Data Collection for Internet of Things: A Survey. *IEEE Internet of Things Journal* 9(17):1-1, DOI:10.1109/IJOT.2022.3176903.
6. Sarmad Rashedand Mujdat Soy Turk (2017). Analyzing the Effects of UAV Mobility Patterns on Data Collection in Wireless Sensor Networks *Sensors*. 17, 413. DOI: 10.3390/s17020413.
7. Weihuang Huang, Jeffrey Xu Yu. (2017). Investigating TSP Heuristics for Location-Based Services *Data Sci. Eng.* 2: 71–93. DOI: 10.1007/s41019-016-0030-0.
8. Helsgaun K. (2017). An Extension of the Lin-Kernighan-Helsgaun TSP Solver for Constrained Traveling Salesman and Vehicle Routing Problems; Roskilde University: Roskilde, Denmark. DOI:10.13140/RG.2.2.25569.40807.
9. Hahsler M., Hornik, K. (2007). TSP – Infrastructure for the traveling salesperson problem. *J. Stat. Softw.*, 23, 1–21.
10. Wu Yue, Zhu Jiang (2018). Path Planning for UAV to Collect Sensors Data Based on Spiral Decomposition. *Procedia Computer Science* 131, 873–879. DOI: 10.1016/j.procs.2018.04.29.
11. Chengliang W, Jun-hui Y (2015). Path Planning for UAV to Collect Sensor Data in Large-Scale WSNs. *Transaction of Beijing Institute of Technology*; 35: 1044–1049. DOI: 10.1016/j.procs.2018.04.291.
12. Kumar Nitesh, Prasanta K. Jana (2019). Convex hull based trajectory design for mobile sink in wireless sensor networks/*International Journal of Ad Hoc and Ubiquitous Computing* 30(1):26 DOI: 10.1504/IJAHUC.2019.097092.
13. Q F., Yu W., Xiao K., Liu C., Liu W. (2022). Trajectory generation and optimization using the mutual learning and adaptive colony algorithm in uneven environments. *Appl. Sci.*, 12, 4629. DOI: <https://doi.org/10.3390/app12094629>.
14. Katoch S., Chauhan S.S., Kumar V. (2021). A review on genetic algorithm: past, present, and future. *Multimed. Tools Appl.*, 80, 8091–8126. DOI: 10.1007/s11042-020-10139-6.
15. Emambocus B.A.S., Jasser M.B., Hamzah M., Mustapha A., Amphawan A. (2021). An enhanced swap sequence-based particle swarm optimization algorithm to Solve TSP. *IEEE Access*, 9, 164820–164836. DOI: 10.1109/ACCESS.2021.3133493.
16. Haider S.K., Jiang A., Almogren A., Rehman A.U., Ahmed A., Khan W.U., Hamam H. (2021). Energy Efficient UAV Flight Path Model for Cluster Head Selection in Next-Generation Wireless Sensor Networks. *Sensors*, 21, 8445. DOI: <https://doi.org/10.3390/s21248445>.
17. Josiane da Costa Vieira Rezende, Roneílido da Silva, Marcone Jamilson Freitas Souza. (2020). Gathering Big Data in Wireless Sensor Networks by Drone. *Sensors*, 20, 6954. DOI: 10.3390/s20236954.
18. Dac-Tu Ho, EstenIngar Grotli, and Tor Arne Johansen (2013). Heuristic Algorithm and Cooperative Relay for Energy Efficient Data Collection with a UAV and WSN. *International Conference Computing, Management and Telecommunications (ComManTel)*. DOI: 10.1109/ComManTel.2013.6482418.
19. Cariou, C., Moiroux-Arvis, L., Pinet, F., Chanet, J.-P. (2023). Evolutionary Algorithm with Geometrical Heuristics for Solving the Close Enough Traveling Salesman Problem: Application to the Trajectory Planning of an Unmanned Aerial Vehicle. *Algorithms*, 16, 44. DOI: <https://doi.org/10.3390/a16010044>.
20. Nguyen, K. K., Duong, T. Q., Do-Duy, T., Claussen, H., & Hanzo, L. (2022). 3D UAV Trajectory and Data Collection Optimization via Deep Reinforcement Learning. *IEEE Transactions on Communications*. DOI: 10.1109/TCOMM.2022.3148364
21. Hrymud A., Romaniuk V. (2023). A model of situational control of the telecommunication aerial platform flight trajectory to collect data from nodes of a wireless sensor network. *Communication, informatization and cyber-security systems and technologies*, № 3. p. 88–100. DOI: 10.58254/viti.3.2023.12.101.

УДК 004.056(53+57)

д-р техн. наук Субач І. Ю. ORCID: 0000-0002-9344-713X (ІСЗЗІ «КПІ ім. Ігоря Сікорського»)  
Власенко О. В. ORCID: 0000-0001-6671-870X (ВІТІ ім. Героїв Крут)

## АРХІТЕКТУРА ІНТЕЛЕКТУАЛЬНОЇ SIEM-СИСТЕМИ ДЛЯ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ У БАЗАХ ДАНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

У статті розглянуто актуальні завдання кіберзахисту баз даних інформаційно-комунікаційних систем. Проаналізовано ефективність поточних заходів щодо захисту баз даних і зроблено висновок, що існуючі системи не враховують багаторівневості захисту, що є критичним аспектом у сфері кібербезпеки. Запропоновано забезпечення кіберзахисту баз даних із використанням інтелектуальних можливостей SIEM-системи. Пропонується новий підхід до архітектури SIEM-системи, який враховує різні рівні контуру захисту інформаційно-комунікаційної системи. Розроблена архітектура надає можливість ефективно виявляти та реагувати на кібератаки на всіх рівнях захисту: від операційної системи до баз даних. Основним аспектом цієї архітектури є багаторівневий захист бази даних, що дозволяє ефективно виявляти та реагувати на кібератаки. Запропонований підхід включає додавання джерел даних із застосунків різних рівнів контуру захисту інформаційно-комунікаційної системи, модуля аналізу даних про події в базі даних, який функціонує на основі застосування методів теорії нечітких множин та нечіткого логічного виводу та модуля кореляції правил для покращення виявлення кіберінцидентів. А також інтеграцію OLAP-технологій для отримання глибокого і аналітичного погляду на стан безпеки бази даних. Запропонована архітектура для виявлення кіберінцидентів дозволяє підвищити ефективність за показником точності виявлення кіберінцидентів, пов'язаних із функціонуванням бази даних інформаційно-комунікаційної системи. Результатом дослідження є покращення можливостей SIEM-системи у виявленні та реагуванні на кіберінциденти у сфері бази даних інформаційної системи військового призначення. Подальшим напрямком досліджень є побудова моделі функціонування системи кіберзахисту бази даних інформаційно-комунікаційної системи.

**Ключові слова:** база даних, інформаційно-комунікаційна система, кіберзахист, кіберінцидент, SIEM-система, теорія нечітких множин, нечіткі правила, архітектура SIEM.

### *I. Subach, O. Vlasenko Architecture of intelligent SIEM for detecting cyber incidents in databases of military information and communication systems.*

The article looks at the current supply of cyber defense to the databases of information and communication systems. The effectiveness of continuous visits to databases is analyzed. The analysis indicates that existing systems are not immune to security, which is a critical aspect in the field of cybersecurity. A new approach to the architecture of the SIEM system is being introduced, which is aimed at different parts of the protection circuit of the information and communication system. The fragmented architecture makes it possible to effectively detect and respond to cyber attacks at all levels of protection, from the operating system to databases. A new approach is being introduced to ensure cyber security of databases with the benefit of the intelligent capabilities of the SIEM system. The main aspect of this architecture is rich database protection, which allows you to effectively detect and respond to cyber attacks. The registration approach includes the addition of data from different levels to the security circuit of the information and communication system, the module for analyzing data about categories in the database, which operates on the basis of The use of fuzzy multiplicity theory methods, fuzzy logic inference and rule correlation module to improve the detection of cyber incidents. And also the integration of OLAP technologies to provide a deep and analytical view of the database security system. The architecture for identifying cyber incidents has been designed to improve the efficiency of identifying cyber incidents related to the functioning of the database of information and communication systems and. The result of the investigation is a reduction in the capabilities of the SIEM system in identifying and responding to cyber identities in the database of the military information system. Further, we directly monitor the operational model of the cybersecurity system of the information and communication system database.

**Keywords:** database, information and communication system, cyber protection, cyber incident, SIEM system, fuzzy set theory, fuzzy rules, SIEM architecture.

**Постановка завдання.** Існуючі умови ведення кібервійни заставляють державні інститути все більше і більше приділяти увагу кіберзахисту своїх інформаційно-комунікаційних систем (далі – ІКС). Дотримання безпечного функціонування ІКС є однією з головних задач будь-якого підрозділу кіберзахисту. Переважна більшість конфіденційної та

цінної інформації, яка функціонує в ІКС, зберігається в базах даних (далі – БД), тому ядром будь-якої ІКС можна сміливо вважати БД. У БД переважно зберігається службова чи конфіденційна інформація, що робить їх основною цілью для зловмисників. Кіберзахист БД постійно викликає занепокоєння через витоки даних з ІКС різного походження, які в подальшому набувають широко розголошення. Вторгнення (кібератаки) в БД стали більш складними та перетворилися у форму внутрішніх і зовнішніх вторгнень в комбінованому вигляді, що ускладнює їх виявлення. Зловмисники постійно змінюють тактику кібератак на БД, тому захист даних в ІКС є одним із пріоритетних напрямів кіберзахисту ІКС у цілому.

Отже, вирішення задачі кіберзахисту баз даних стає пріоритетом для будь-якого підрозділу, який оперує значущим обсягом конфіденційної інформації та є актуальною науковою задачею.

**Аналіз наукових публікацій.** Більшість публікацій розглядають кіберзахист БД виключно додаванням механізмів усунення ризиків безпеки БД до стандартних функцій захисту систем керування базами даних (далі – СКБД), таких як: покращена автентифікація; підзвітність та аудит; контроль доступу; шифрування даних та використання політики висновків [1; 2]. Але в деяких випадках тільки цих механізмів усунення ризиків не достатньо для надійного захисту БД ІКС.

Типова БД може мати 15–20 тисяч підключень на секунду й їх потрібно відслідковувати. Тому для надійної системи кіберзахисту потрібний додатковий елемент, який зможе відслідковувати всі дії, які відбуваються з БД у режимі реального часу, чи наближеного до нього і реагувати на них.

У [3; 4] для покращення кіберзахисту БД запропоновано додавати систему виявлення вторгнень (далі – СВВ) до звичайних механізмів усунення ризиків. СВВ можна вважати однією з найважливіших частин будь-якої добре захищеної системи, оскільки вона має можливість виявляти кібератаки в режимі наближеного до реального часу.

СВВ до БД (далі – СВВБД) – це спеціалізовані програмні або програмно-апаратні рішення, які автоматизують процес моніторингу та аналізу дій, які відбуваються під час роботи з БД за допомогою різних методів інтелектуального аналізу даних. Нині існують два основні підходи до побудови СВВ, а саме: побудова СВВ на основі застосування сигнатурних методів та побудова СВВ на основі методів виявлення аномалій. Відповідно, у проектуванні архітектури СВВБД дослідники віддають перевагу системам на основі аномалій тому, що вони дозволяють виявляти раніше невідомі види вторгнень (кібератак). Їхня робота, в основному, полягає у створенні на основі шаблонів поведінкового профілю суб'єктів БД, так званих моделей вторгнення. СВВБД визначають, чи є набір певних дій вторгненням шляхом застосування однієї або кількох моделей вторгнень. Модель класифікує послідовність дій як «позитивні» (немає вторгнення) або «негативні» (можливі вторгнення). Даний спосіб захисту БД, у деяких випадках, є більш ефективним ніж застосування сигнатурних методів виявлення вторгнень (кібератак), особливо під час виявлення атак нульового дня, але не завжди дозволяє захистити БД повністю.

Кібератаки, що відбуваються на прикладному рівні, набагато складніше виявляти, оскільки вони дуже часто виглядають як законні запити до БД. Наприклад, виконання складного або складеного запиту. Зловмисники знаходять доступний найбільш ресурсоємний процес і відправляють кілька десятків запитів. Кібератака даного типу спрямована на виснаження ресурсів БД, націлена на надмірне споживання оперативної пам'яті, обчислювальної потужності системи або в деяких випадках – потоку вводу-виводу. СВВБД буде розцінювати дані запити як коректні, тому що вони нічого неправомірного у своїй структурі не містять, і, як наслідок, не зможе виявити кібератаку.

Унаслідок цього, діапазон кібератак на БД є дуже великим і різнобічним. Наприклад, якщо обмежити невдалі спроби аутентифікації, зловмисники можуть заблокувати облікові

записи введенням великої кількості неправильних паролів. В іншому випадку, якщо впроваджувати сервіси автоматичного масштабування для обробки пакетів запитів, зловмисники можуть генерувати фіктивні запити для збільшення масштабу БД, доки вона не зруйнується під “власною вагою”, або в хмарному середовищі із вимірюванням досягне порогової суми і, як наслідок цього, відповідна служба буде закрита. Отже, не існує єдиного стандартного вектора кібератаки на БД, а в розпорядженні зловмисників знаходиться цілий арсенал різних технік, тактик і практик порушення штатного функціонування ІКС під час роботи з БД.

Зловмисники можуть використовувати дефекти, націлюючись на певну слабкість систем кіберзахисту ІКС або помилки в конфігуруванні БД (людський фактор). Аналіз літератури та досвід експлуатації ІКС дозволяє зробити висновок про те, що за останні двадцять років спостерігається постійна ретроспективна циклічність виникнення помилок, які дозволяють зловмисникам часто дистанційно та без доступу до облікових даних проводити кібератаки на БД [5; 6].

Відповідно до аналізу щомісячного рейтингу DB-Engines [7] одними з передових СКБД є:

- багатомодельна СКБД Oracle Database, розроблена компанією Oracle[8], яка доступна для локальної роботи, а також роботи у звичайній або гібридній хмарі;
- СКБД Microsoft SQL Server – реляційна СКБД, розроблена компанією Microsoft [9], яка призначена для забезпечення інформаційних потреб різних категорій користувачів (для робочих навантажень, починаючи від невеликих застосунків до великих Інтернет-платформ із багатьма одночасними підключеннями);
- IBM DB2 – це хмарна СКБД, створена для забезпечення транзакцій із низькою затримкою та масштабною аналітикою в реальному часі від компанії IBM[10].

Проведений аналіз показує, що переповнення буфера протягом тривалого часу було основною вразливістю всіх наведених СКБД. Так, десятки атак на переповнення буфера в СКБД Oracle Database виводили БД з ладу, іноді навіть без облікових записів користувача, використовуючи привілеї PUBLIC. СКБД MS SQL Server має власну історію подібних проблем, включаючи вразливість іменованих каналів. Свого часу була зламана СКБД DB2 внаслідок відправки пакетів протоколу UDP.

Якщо розглядати рішення, побудоване на базі багаторівневого підходу до кіберзахисту БД ІКС у рамках СВБД, то дана система повинна працювати з усіма рівнями захисту БД та відслідковувати всі дії, які відбуваються в екосистемі БД, і збирати дані для аналізу з різних джерел. Але більшість робіт, які присвячені розробці СВБД [3; 4], зосереджені тільки на аналізі SQL-запитів чи прав доступу користувачів. Самі архітектури запропонованих раніше СВБД не передбачають роботу з різними різнорідними даними і не розглядають проблему кіберзахисту БД ІКС комплексно. Аналіз літератури [11; 12] показує, що для обробки різнорідних даних, які отримують з багатьох джерел для кіберзахисту будь-якої системи ІКС, краще використовувати технологію, яка ґрунтується на застосуванні SIEM-систем (Security Information and Event Management).

Для покращення і вдосконалення кіберзахисту БД, як важливого елементу ІКС, у роботі [12] запропоновано розглядати систему кіберзахисту БД у контексті багаторівневої архітектури захисту ІКС із вбудованими до неї додатковими структурно-функціональними елементами. Вона повинна базуватись на різних рівнях безпеки, запропонованих у [12]: рівні СКБД та БД, рівні операційної системи та рівні мережі. Консолідація інформації, отриманої з цих рівнів, робить захист БД більш досконалим і ефективним. Цей підхід дозволяє створити багаторівневу систему кіберзахисту БД, де кожен рівень відповідає за конкретні аспекти безпеки БД.

Отже, інформаційна технологія для кіберзахисту БД ІКС, основою якої має бути інтелектуальна SIEM-система, дозволяє збирати дані від різних джерел, аналізувати їх

в реальному часі, виявляти аномальні дії та надавати офіцерам безпеки інформацію, необхідну для здійснення відповідних заходів із кіберзахисту.

Слід зауважити, що системам керування інформацією та подіями безпеки (SIEM-системам) нині приділяється дуже велика увага. У багатьох наукових публікаціях пропонуються покращені механізми роботи SIEM-систем. Дана технологія є дуже актуальною в сучасних наукових дослідженнях.

У [11–15] представлено систематичний огляд поточного стану технології SIEM, а також майбутніх етапів їхнього розвитку. Зроблено висновок, що парадигма технології повільно змінюється від покращення моніторингу/попередження до переведення на міжнародні стандарти, яким мають відповідати всі інструменти безпеки під час кожного внутрішнього чи зовнішнього аудиту, схилиючись до безпеки як послуги, а не до локальних рішень і вдосконаленням механізмів виявлення. Автори пропонують нову структуру, сумісну із загальним регламентом про захист даних (General Data Protection Regulation), використовуючи кілька технологій: блокчейн, шифрування, контейнери та ін.

У [16] наведено виклики та напрямки щодо застосування SIEM-системи у контексті критично важливої системи від компанії в області контролю повітряного руху. Дана система для аналізу видає величезні обсяги неструктурованих текстових журналів. Представлено проблеми, пов'язані з обробкою таких журналів, поточну роботу над інтеграцією SIEM-системи з відкритим кодом і напрямки моделювання базових сценаріїв поведінки системи для визначення індикаторів компромісу.

У [17] зроблено висновок про те, що використання, встановлення та обслуговування SIEM-систем є дуже витратними процесами. Як наслідок, такі системи досі не використовуються на малих і середніх підприємствах (МСП). Запропоновано систему в проєкті SIMU, яка базується на сценаріях застосування для кіберзахисту МСП і націлена на простішу стратегію впровадження. Використання протоколу IF-MAP дозволяє інтегрувати різну інформацію з багатьох компонентів безпеки в одному форматі даних. Вже реалізовані клієнти та відкрита архітектура полегшують включення типових мережевих пристроїв і служб, зменшуючи витрати на управління та інвестиції. Це додатково підтверджується загальною орієнтацією на рішеннях із відкритим кодом.

Використовувати СВВ, інтегровану з SIEM-системою, для створення методів аналізу подій за допомогою машинного навчання пропонують у [18]. У дослідженні для аналізу, виявлення та моніторингу кібератак запропоновано створити систему з використанням найпоширеніших програмних рішень з відкритим кодом. Для створення системи використовується комбінація програмних застосунків Elastic (ELK) Stack, Slips і Zeek IDS. Для підтвердження, що вибрані компоненти правильні та надійні, проведено дослідження, яке зосереджено на вимірюванні продуктивності споживання ресурсів (центрального процесора й оперативної пам'яті).

Так, аналіз публікацій і готових рішень показав, що вектор досліджень в сфері розробки та застосування технології SIEM-систем спрямований на покращення системи в цілому. Моніторинг подій в БД перекладається на відповідні СВВ та інтерфейсні модулі для отримання інформації з них. Висновок про неефективність використання тільки СВВ для захисту БД було зроблено в [12]. Для ефективного опрацювання подій безпеки потрібна покращена архітектури SIEM-системи з урахування багаторівневої системи захисту БД.

**Метою статті** є розробка архітектури інтелектуальної системи управління інформацією та подіями безпеки для виявлення кіберінцидентів в БД інформаційної системи військового призначення.

**Виклад основного матеріалу дослідження.** Внаслідок аналізу бойових дій у кіберпросторі під час першої в світі кібервійни та враховуючи існування різноманітних кіберзагроз, кількість яких постійно збільшується, виникає гостра потреба побудови

ефективної системи кіберзахисту ІКС шляхом розробки та вдосконалення існуючої архітектури SIEM-системи, яка стає важливим фактором захисту ІКС. У цілому, SIEM-система являє собою широкий спектр послуг для одночасного керування інформацією про події безпеки. SIEM-система також забезпечує своєчасний аналіз сповіщень безпеки. Сучасна архітектура системи повинна забезпечувати можливості представлення, аналізу та збору інформації з різнорідних джерел даних [11].

Архітектуру перспективної проактивної SIEM-системи представлено у [11]. Вона є багаторівневою та містить наступні рівні: рівень збору даних (COL), рівень управління даними (CON) та рівень аналізу даних (ANL), а також четвертий рівень (DEC) – рівень прийняття та реалізації рішень.

На відповідних рівнях архітектури важливо мати належні засоби, алгоритми та механізми, які допомагають ефективно виконувати завдання кожного рівня. Аналізуючи основні складові елементи запропонованої архітектури, можна зробити висновок про те, що кіберзахист у цій системі відносно БД не забезпечений повністю, а точніше, вона не відповідає концепції багаторівневого захисту БД відповідно до рівнів та середовища її функціонування [9]. Тому основні структурні рівні даної архітектури потребують вдосконалення.

Основними шляхами удосконалення можуть бути:

- інтеграція SIEM-системи з конкретними зразками СКБД. Дана інтеграція дозволить отримувати дані з журналів роботи СКБД, забезпечуючи при цьому більш глибокий рівень моніторингу подій безпеки;

- розширення можливостей SIEM-системи завдяки імплементації в її архітектуру модулів контекстного аналізу SQL-запитів, що виконуються СКБД та їхнє співставлення з шаблонами злочинної поведінки та відомими вразливостями;

- розробка поведінкових моделей БД для виявлення шаблонів штатної та позаштатної активності. Застосовуючи при цьому технології машинного навчання, можна виявляти аномальну поведінку в БД, наприклад, аномальні або непередбачені запити до неї;

- інтеграція з технологіями інтелектуального аналізу подій, наприклад, UEBA – User and Entity Behavior Analytics, для виявлення аномальної поведінки користувачів, що мають доступ до БД. Це дозволить оперативно виявляти підозрілі дії користувачів, такі як спроби несанкціонованого доступу або несанкціоноване отримання привілеїв;

- інтеграція з технологіями оперативного аналізу даних (OLAP – Online Analytical Processing), що дозволить розширити аналітичні можливості SIEM-системи щодо виявлення та запобігання кіберінцидентам, пов'язаним з БД, що дозволить:

1. Здійснювати розширений аналіз даних. OLAP-технології надають можливість аналізувати великі обсяги даних, накопичених SIEM-системою з різних джерел. У свою чергу, це дозволить здійснювати більш глибокий аналіз подій безпеки, пов'язаних із БД ІКС і виявляти приховані патерни та зв'язки між різними подіями. Це може допомогти у виявленні складних загроз та аномальної поведінки користувачів та програмних застосунків, які не можна отримати іншими методами аналізу.

2. Покращити візуалізацію та звітність. OLAP-технології надають потужні можливості для візуалізації даних та генерації нерегламентованих звітів. Інтеграція даних технологій з SIEM-системами дозволить створювати візуальні панелі, графіки та звіти, адаптовані для аналізу подій у БД, щоб аналітики з безпеки мали можливість наочно надавати інформацію про події та загрози, пов'язані з БД. Це дозволить спростити моніторинг та аналіз стану БД для оперативного та обґрунтованого прийняття рішень щодо виявлення та запобігання кіберінцидентів в них.

3. Розширити можливості запитів для аналітики. OLAP-технології надають великий набір функцій для виконання складних запитів та аналітичних операцій над ними. Їхня інтеграція з SIEM-системою дозволить створювати більш гнучкі й потужні запити для аналізу

подій у БД. Це, відповідно, дозволить виявляти аномальну поведінку користувачів та виявляти аномальні запити до БД або підозрілі зміни в її структурі.

4. Покращити процес виявлення та запобігання кіберінцидентам. За допомогою OLAP-технологій SIEM-системи можуть більш ефективно аналізувати та класифікувати події БД, виявляти аномалії, незвичну поведінку користувачів, а також зв'язок між різними подіями.

5. Підвищити проактивність та прогнозованість. OLAP-технології дозволяють аналізувати великі обсяги історичних даних, що дозволить аналітикам із безпеки виявляти кібератаки, які повторюються або еволюціонують. Крім того, аналітики з безпеки можуть використовувати ці дані для створення моделей та прогнозування майбутніх потенційних кібератак або кіберінцидентів, що дозволить приймати превентивні заходи заздалегідь.

6. Централізувати управління даними. Застосування OLAP-технологій в SIEM-системах дозволить об'єднати дані про події безпеки з різнорідних різнорівневих джерел даних та систем безпеки в єдиному централізованому сховищі даних. Це значно спростить процес аналізу даних та виявлення кібератак і кіберінцидентів, так як аналітики з безпеки будуть мати доступ до повного набору даних про події, що відбуваються під час роботи з БД, який є необхідним для виявлення аномалій та проведення детального розслідування кіберінцидентів.

Отже, інтеграція OLAP-технологій із SIEM-системами для захисту БД може значно покращити процеси виявлення, аналізу та запобігання кіберінцидентів. Вона дозволить здійснювати більш глибокий та комплексний аналіз даних, підвищить оперативність реагування на кіберінциденти, а також сприятиме здійсненню проактивних заходів із захисту БД ІКС.

На рисунку 1 запропоновано удосконалену архітектуру SIEM-системи для виявлення кіберінцидентів у БД ІКС.

Рівень збору даних в архітектурі SIEM-системи дозволяє за допомогою агентів збирати з різнорідних джерел первинні дані про події в системі та здійснювати їхню первинну обробку й фільтрацію [11]. Отримані дані на цьому рівні підлягають процесу нормалізації, який перетворює різноманітні формати даних на стандартизований формат, що використовується в системі. Дані також повинні бути фільтровані для видалення зайвої або несуттєвої інформації.

Отже, для підвищення ефективності захисту БД ІКС в рамках концепції багаторівневого захисту БД виникає необхідність введення до існуючої архітектури SIEM-системи додаткових джерел даних. Перелік типових джерел, які потрібно враховувати при багаторівневому кіберзахисті БД, наведено в таблиці 1.

Таблиця 1

Розподілені джерела для підсистеми багаторівневого кіберзахисту БД

№ з/п	Тип джерела	Опис
1	Журнали подій операційних систем Windows або Linux	Якщо СКБД розгорнута на основі операційних систем (ОС) сімейства Windows, то всі дії, що відбуваються у програмних і апаратних компонентах, підключених до системи, реєструються. ОС Windows за замовчуванням використовує шість категорій журналів для реєстрації подій: журнал додатків, системний журнал, журнал безпеки, журнал служби каталогів, журнал DNS-сервера та журнал сервера реплікації файлів. Якщо СКБД функціонує в середовищі ОС Linux-подібній ОС, то є можливість знайти часову шкалу подій, пов'язаних з ядром, сервером і програмними застосунками. Дані записуються в журнали, враховуючи чотири основні категорії: журнали подій, журнали служб, журнали програм і системні журнали. Наприклад, у каталозі <i>/var/log/syslog</i> зберігаються загальні журнали активності системи, а в <i>/var/log/auth.log</i> – журнали автентифікації та авторизації
2	Журнали брандмауера	Містять деталі невдалих входів до системи, відхилені IP-адреси, вихідні маршрутизовані пакети і дії з внутрішніх серверів
3	Журнали вебсерверів	Аналіз записів журналів вебсервера надає можливість зрозуміти, які кінцеві користувачі взаємодіють із вебресурсами, що працюють з відповідними БД

№ з/п	Тип джерела	Опис
4	Журнали застосунків	Використовуються для відстеження подій, які розробники вставляють у програми
5	Журнали СВБД	Містять дані про події в БД, які отримуються під час аналізу синтаксису запитів до СКБД та поведінкового профілю користувачів БД
6	Журнали СКБД	Містять дані з журналів подій в СКБД. Наприклад, у СКБД MySQL основних журналів чотири: Error Log (стандартний журнал помилок, які виникають під час роботи сервера); Binary Log (журнал всіх команд зміни БД, необхідний для реплікації та бекапів); General Query Log (основний журнал всіх запитів); Slow Query Log (журнал повільних запитів)
7	Журнали мережі	Містять інформацію про такі події, як зловмисний трафік, зниження пропускну здатності, скидання пакетів та інші докази підозрілої активності

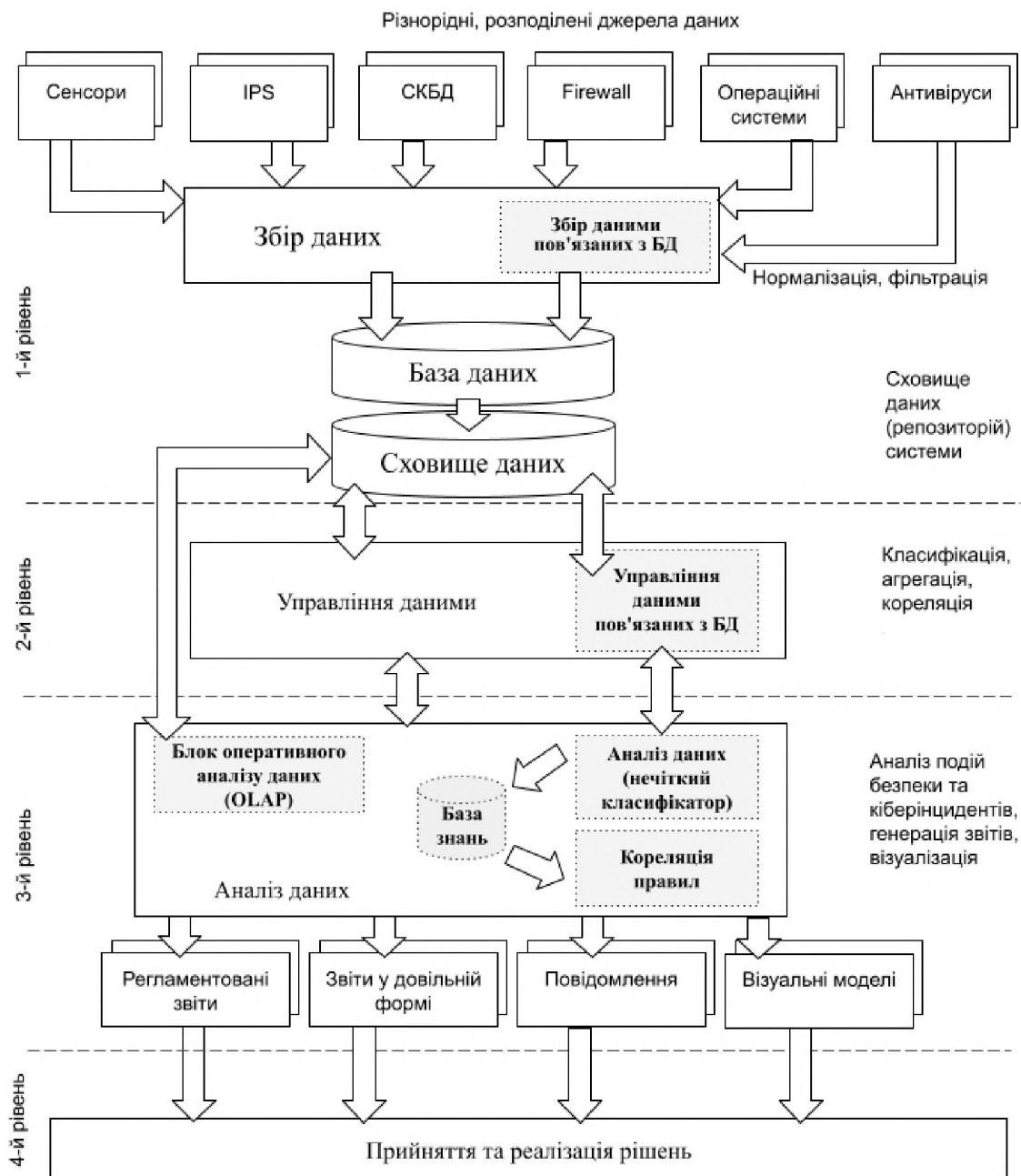


Рис. 1. Удосконалена архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів в БД ІКС



Для отримання даних із різноманітних, розподілених джерел необхідно мати набір агентів, які дозволяють зчитувати дані з них. Вони складаються з інтерфейсу доступу до певного джерела та самої інформації для передачі в SIEM-систему. Журнали роботи тих чи інших компонентів ІКС є безпосередньо джерелами даних для отримання інформації про події безпеки.

*Сховище даних* повинно забезпечувати структуроване зберігання даних про події безпеки, у тому числі пов'язані з БД, та підтримувати інтеграцію з різними джерелами даних. Для ефективного аналізу подій безпеки, які відбуваються під час роботи з БД ІКС, доцільно використовувати інформацію з розподілених джерел про події, пов'язані з нею.

Рівень управління даними стосується всіх даних про події безпеки, які зберігаються у сховищі даних SIEM-системи та які надходять як початкові дані до механізмів їхнього аналізу. Він включає виконання таких функцій, як класифікація, агрегація та пріоритезація. Класифікація, агрегація та пріоритезація дозволяють системі обробити інформацію, отриману з різних джерел, і надають контекст для ефективного аналізу та прийняття рішень щодо безпеки. Ці функції також дозволяють отримати найважливішу інформацію з різноманітних подій і повідомлень для її подальшої обробки.

У модулі *управління даними, пов'язаними з БД (CONDB)*, відбувається пріоритезація подій у рамках БД, а також їх класифікація та агрегація. Агрегація даних, пов'язаних з БД, дозволяє зменшити кількість подій, що відображаються шляхом зведення пов'язаних подій до одного представлення. Наприклад, події, пов'язані з одним користувачем, можуть бути агреговані в одну подію або групу. Класифікація даних дозволяє визначити типи подій або інцидентів на основі їхніх характеристик або атрибутів, а також допомагає представити події в структурованій формі для подальшого аналізу та обробки. Функція пріоритезації встановлює рівень важливості для кожної події, пов'язаної з БД, на основі потенційного впливу на безпеку БД.

Рівень аналізу даних відіграє ключову роль у забезпеченні безпеки та виявленні загроз у системі. Його основне завдання – обробка та аналіз великого обсягу подій безпеки, журналів, сповіщень та інших даних, що надходять до SIEM-системи. На ньому використовуються різні техніки аналізу даних для виявлення аномалій, кореляції подій і забезпечення ефективного моніторингу та реагування на безпекові інциденти. Для успішного виявлення кібератак на БД до рівня аналізу даних необхідно інтегрувати модуль аналізу даних (наприклад, нечіткий класифікатор) та модуль кореляції правил.

Особливого розгляду заслуговує застосування методів теорії нечітких множин та лінгвістичних змінних для виявлення та класифікації кіберінцидентів, пов'язаних з БД ІКС. Оскільки в теорії нечітких множин об'єкти можуть мати часткову приналежність до визначеної множини, на відміну від традиційної логіки, де об'єкт або належить до певної множини або – ні, то це дозволяє враховувати невизначеність (неповноту, обмеженість) та розмитість (нечіткість) даних, які можуть виникати під час аналізу кіберінцидентів. Відповідно, це дозволяє створювати нечіткі правила і моделі, які враховують різні рівні впевненості аналітиків із безпеки в процесі виявлення кіберінцидентів. Наприклад, можна застосовувати нечіткі правила, які ґрунтуються на лінгвістичних змінних для того, щоб визначити степінь підозрілої активності в БД або ризику виникнення кіберінциденту.

Крім того, методи теорії нечітких множин дозволяють знизити рівень хибних спрацьовувань системи та покращити точність виявлення кіберінцидентів. Вони можуть враховувати контекстні фактори, аналізувати відхилення від нормальної поведінки з врахуванням неоднозначності даних, що дозволяє покращити ефективність SIEM-системи у процесі виявлення кіберінцидентів [13].

*Модуль аналізу даних (нечіткий класифікатор) (ANLDB)* використовує методи теорії нечітких множин та лінгвістичних змінних для обробки та аналізу подій, що відбуваються

у БД. Функціональним призначенням цього модуля є виявлення аномалій під час роботи з БД для ідентифікації кіберінцидентів в ній.

Основні характеристики модуля аналізу даних про події в БД SIEM-системи, робота якого ґрунтується на методах теорії нечітких множин, включають:

- застосування нечітких правил. Модуль використовує нечіткі правила для опису аномалій та патернів поведінки в БД. Ці правила повинні містити лінгвістичні змінні та операції над ними для визначення рівня відповідності події або шаблону;

- використання нечіткої логіки для виявлення аномалій. За допомогою нечіткої логіки модуль може визначати, наскільки певна подія або група подій є аномальною в контексті роботи з БД. Використовуючи нечіткі операції, модуль може враховувати неоднозначності та невизначеності, що можуть виникати під час аналізу подій у БД;

- моделювання патернів поведінки. Модуль може використовувати нечітку логіку для моделювання типових патернів поведінки користувачів (програмних застосунків) під час роботи з БД. При цьому повинні враховуватися різні фактори, такі як типи запитів, часові затримки, обсяги даних та інші атрибути, для виявлення незвичайної або підозрілої активності;

- гнучкість та адаптивність. Робота модуля повинна бути гнучкою та адаптивною до змін у БД. Він повинен навчатися на основі нових даних та оновлювати нечіткі правила і моделі для забезпечення ефективної аналітики роботи інфраструктури кіберзахисту в змінному середовищі.

Застосування методів теорії нечітких множин та нечіткої логіки у модулі аналізу даних SIEM-системи допомагає покращити ефективність виявлення кіберінцидентів під час роботи з БД ІКС в умовах неповноти та неточності інформації, знижує кількість помилкових спрацювань та дозволяє більш гнучко моделювати складні сценарії аналізу даних для кіберзахисту.

*База знань* містить нечіткі правила для ідентифікації кіберінцидентів, у тому числі під час роботи з БД ІКС.

*Модуль кореляції ознак (COLANALDB)* використовується для виявлення зв'язків та взаємозв'язків між різними правилами, які були сформульовані та завантажені у БД SIEM-системи для аналізу подій під час роботи з БД ІКС.

Основна мета роботи модуля кореляції правил полягає в тому, щоб ідентифікувати складні кібератаки/кіберінциденти, які можуть бути непомітними під час аналізу окремих правил. У ньому аналізуються ознаки кіберінцидентів (враховуючи багаторівневість системи захисту БД) і виявляються зв'язки (кореляції) між різними подіями або шаблонами, що можуть вказувати на складні кіберінциденти/кібератаки.

Модуль кореляції ознак виконує наступні функції:

- виявлення зв'язків (кореляцій). Модуль аналізує різні правила аналізу даних про події в ІКС під час роботи з БД та відшукує спільні атрибути, взаємозв'язки або закономірності між ними. Наприклад, він може виявити, що певні події, які здавалися незначними при окремому аналізі, коли комбінуються з іншими подіями, можуть свідчити про спробу ознаки злому або несанкціонованого доступу;

- формування комплексних подій. На основі знайдених зв'язків модуль може створювати комплексні події, які включають декілька правил аналізу. Ці комплексні події можуть бути використані для виявлення більш складних кібератак або шаблонів поведінки, які не можуть бути виявлені окремими правилами;

- пріоритезація та реагування. Модуль кореляції може також допомогти у визначенні пріоритетності виявлених комплексних подій безпеки. На основі цього модуля можна визначити, які дії або заходи безпеки потрібно прийняти для запобігання кібератакам та запобігання або зменшення їхніх наслідків.

Загалом, модуль кореляції правил допомагає збільшити ефективність аналізу подій в БД ІКС шляхом виявлення складних кібератак/кіберінцидентів, які можуть бути непомітними при звичайному аналізі.

Отже, для ефективного кіберзахисту БД ІКС модель перспективної проактивної SIEM-системи [11] можна вдосконалити для виявлення складних кібератак/кіберінцидентів, що відбуваються під час роботи саме з БД ІКС, шляхом імплементації до неї елементів, які реалізують принцип багаторівневості кіберзахисту БД (1):

$$M_{SIEM} = \langle COL, CON, ANL, DEC \rangle, \quad (1)$$

де  $COL = \langle \{LEV\}_{l=1}^m, \{PUR\}_{i=1}^n, NOR, NORDB \rangle$  – підсистема збору та обробки даних з різномірних джерел:  $\{LEV\}_l$ ,  $l = \overline{1, m}$ , – множина рівнів кіберзахисту БД ІКС;  $\{PUR\}_{i,l}$ ,  $i = \overline{1, n}$ ;  $l = \overline{1, m}$ , – множина модулів (конекторів) завантаження даних із різномірних джерел даних із різних рівнів кіберзахисту БД ІКС;  $NOR$  – модуль нормалізації даних (приведення різних форматів даних до єдиного формату для зберігання);  $NORDB$  – модуль нормалізації та селекції даних, пов'язаних із подіями під час роботи з БД;

$CON = \langle FIL, CLS, AGR, COR, CONDB \rangle$  – підсистема керування даними:  $FIL$  – модуль фільтрації даних (видалення неважливих даних для аналізу);  $CLS$  – модуль класифікації подій на заздалегідь визначені класи;  $AGR$  – модуль агрегації подій до більш узагальненого рівня;  $COR$  – модуль кореляції подій (знаходження взаємозв'язків між різними подіями),  $CONDB$  – підсистема керування подіями, пов'язаними з БД, що включає фільтрацію, агрегацію, класифікацію та пріоритетизацію;

$ANL = \langle MDL, PRI, \{GEN\}_{m=1}^l, \{VIZ\}_{p=1}^q, BOLAP, ANLDB, CORANLDB \rangle$  – підсистема аналізу даних:  $MDL$  – модуль моделювання кібератак і кіберінцидентів та їх прогнозування;  $PRI$  – модуль пріоритетизації (визначення важливості подій безпеки);  $\{GEN\}_m$ ,  $m = \overline{1, l}$ , – множина модулів генерації регламентованих та нерегламентованих звітів;  $\{VIZ\}_p$ ,  $p = \overline{1, q}$  – множина модулів візуалізації даних;  $BOLAP$  – блок оперативного аналізу даних;  $ANLDB$  – підсистема аналізу даних, пов'язаних із БД;  $CORANLDB$  – модуль кореляції нечітких правил;

$DEC$  – підсистема прийняття на реалізації рішень.

Слід зауважити, що застосування методів теорії нечітких множин та нечіткої логіки у модулі аналізу даних про події у БД ІКС дозволяє виявляти кіберінциденти у БД, забезпечуючи при цьому більш гнучку аналітику подій безпеки. Крім того, завдяки модулю кореляції нечітких правил SIEM-система стає більш ефективнішою у виявленні складних кібератак на БД ІКС.

**Висновки.** У цій статті було розглянуто проблематику кіберзахисту БД в ІКС військового призначення.

Аналізуючи сучасні тенденції та потенційні загрози, було запропоновано підхід до багаторівневого захисту БД на рівнях СКБД і БД, операційної системи та мережі. Окрім цього, у статті була розглянута архітектура інтелектуальної SIEM-системи, яка доповнюється додатковими блоком оперативного аналізу даних (OLAP), модулями аналізу даних і кореляції ознак для ефективного виявлення та запобігання кіберінцидентам. Цей підхід дозволяє покращити рівень безпеки та надійності БД в умовах постійно зростаючих загроз кібербезпеці.

Враховуючи актуальність та постійно зростаючу складність кіберзагроз, введення запропонованого підходу та архітектури SIEM-системи в практику військових ІКС є кроком у напрямку надійного та ефективного кіберзахисту важливих даних та ресурсів.

**Перспективним напрямком подальших досліджень** є побудова моделі функціональної системи кіберзахисту БД ІКС.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Mousa, M. Karabatak, and T. Mustafa Database Security Threats and Challenges, in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. 2020: IEEE. P. 1–5. DOI: 10.1109/ISDFS49300.2020.9116436.
2. Ramyar A. Teimoor A. Review of Database Security Concepts, Risks, and Problems. *UHD Journal of Science and Technology*. 2021. Vol. 5, no. 2. P. 38–46. DOI: 10.21928/uhdjst.v5n2y2021.
3. M. I. Khan, S. N. Foley, B. O'Sullivan. Database Intrusion Detection Systems (DIDs): Insider Threat Detection via Behavioural-based Anomaly Detection Systems – A Brief Survey of Concepts and Approaches. *Emerging Information Security and Applications*. 2022. P. 178–197. DOI: 10.1007/978-3-030-93956-4.
4. R. G. Santos, J. Bernardino, M. Vieira. Approaches and Challenges in Database Intrusion Detection. *ACM SIGMOD Record*. 2014. Vol. 43, no. 3. P. 36–47. DOI: 10.1145/2694428.2694435.
5. S. Rathore, A. Sharma Database Security - Attacks, Threats and Challenges. *International Journal of Engineering Research & Technology (IJERT), ICCCS*, 2017. Vol. 5, no. 10. ISSN: 2278-0181.
6. Database Denial of Service: Attacks. *Blog*. URL: <https://securosis.com/blog/database-denial-of-service-the-attacks> (дата звернення: 03.06.2023).
7. DB-Engines Ranking // Knowledge Base of Relational and NoSQL Database Management Systems. URL: <https://db-engines.com/en/ranking> (дата звернення: 02.06.2023).
8. Oracle Database Documentation URL: <https://docs.oracle.com/en/database/> (дата звернення: 05.06.2023).
9. Microsoft SQL documentation URL: <https://learn.microsoft.com/uk-ua/sql/?view=sql-server-ver16> (дата звернення: 05.06.2023).
10. Db2 database product documentation URL: <https://www.ibm.com/support/pages/db2-database-product-documentation> (дата звернення: 05.06.2023).
11. І. Субач, В. Кубрак, А. Микитюк. Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кіберзахисту об'єктів критичної інфраструктури. *Information Technology and Security*. 2019. № 7 (2). P. 208–215. DOI: <https://doi.org/10.20535/2411-1031.2019.7.2.190570>.
12. І. Субач, О. Власенко. Інформаційні технології захисту баз даних від кібератак в інформаційних системах військового призначення”. *Information Technology and Security*. 2022. № 10 (2). P. 177–193. DOI: <https://doi.org/10.20535/2411-1031.2022.10.2.270412>.
13. І. Субач, В. Фесьоха. Модель виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу. *Зб. наук. праць ВІТІ*. 2017. № 3. С. 158–164. URL: [http://nbuv.gov.ua/UJRN/Znpviti\\_2017\\_3\\_21](http://nbuv.gov.ua/UJRN/Znpviti_2017_3_21).
14. І. Ю. Субач, В. В. Фесьоха, Н. О. Фесьоха. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій. *Information technology and security*. 2017. Vol. 5, iss. 1. Pp. 29–41. DOI: <https://doi.org/10.20535/2411-1031.2017.5.1.120554>.
15. López Velásquez J. M., Martínez Monterrubio S. M., Sánchez Crespo L. E. et al. Systematic review of SIEM technology: SIEM-SC birth. *Int. J. Inf. Secur.* 2023. DOI: <https://doi.org/10.1007/s10207-022-00657-9>.
16. M. Cinque, D. Cotroneo, A. Pecchia. Challenges and Directions in Security Information and Event Management (SIEM). *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Memphis, TN, USA, 2018. Pp. 95–99. DOI: 10.1109/ISSREW.2018.00-24.
17. K.-O. Detken, T. Rix, C. Kleiner, B. Hellmann, L. Renners. Siem approach for a higher level of it security in enterprise networks. In Proc. IDAACS, Warsaw, Poland, 2015. P. 322–327.
18. Muhammad, Adabi & Sukarno, Parman & Wardana, Aulia. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science*. 2023. Vol. 217. P. 1406–1415. DOI: 10.1016/j.procs.2022.12.339.

УДК. 681.325.6

д-р техн. наук, професор Хорошко В. О. ORCID: 0000-0001-6213-7086 (ВІТІ ім. Героїв Крут)  
канд. техн. наук Клімович С. О. ORCID: 0000-0001-7209-2176 (ВІТІ ім. Героїв Крут)  
канд. техн. наук, доцент Янковський О. Г. ORCID: 0000-0001-8041-1843 (ВІТІ ім. Героїв Крут)

## КОНТРОЛЬ ТА ДІАГНОСТУВАННЯ ПОСЛІДОВНИХ ЦИФРОВИХ СТРУКТУР

У сучасному світі цифрової електроніки послідовні цифрові структури належать до компонентів багатьох електронних систем і пристроїв. Такі системи (пристрої) широко використовують в різних галузях творчості та життєдіяльності людини, включаючи комунікаційні системи, автоматичні та автоматизовані пристрої. Завдання, пов'язані з контролем та діагностикою таких систем, супроводжуються певними труднощами. Дослідження в цьому напрямку має особливе значення для забезпечення стійкості та надійності цифрових систем у сучасних технологічних умовах. У цьому контексті вивчення особливостей діагностування, послідовних цифрових структур набуває особливого значення. Під діагностуванням розуміємо послідовне розв'язання задач визначення технічного стану, локалізацію несправності (з точністю до окремого радіоелектронного компонента) та прогнозування технічного стану на певний проміжок часу. Визначення окремого радіоелектронного компонента в складі цифрової системи означає визначення конкретної мікросхеми, функціонування якої не відповідає технічним умовам (оскільки мікросхема, незважаючи на складність та багатофункціональність, є мінімальним компонентом, що підлягає заміні). Контроль технічного стану особливо важливий у системах, яка містить велику кількість взаємодіючих між собою послідовних цифрових елементів.

Однією з ключових проблем під час розробки методів контролю послідовних цифрових структур є їхня чисельна розмірність та велика кількість логічних елементів, кожен з яких може бути джерелом помилки при виконанні простих логічних операцій. Тому інженерам доводиться розробляти нові ефективні методи та алгоритми виявлення помилок у таких системах.

**Ключові слова:** послідовні цифрові структури, великі інтегральні схеми, діагностика технічного стану, радіоелектронні компоненти.

### *V. Khoroshko, S. Klimovych, O. Yankovskiy Control and diagnostics of sequential digital structures.*

*In the modern world of digital electronics, sequential digital structures are integral components of many electronic systems and devices. Such systems and devices find extensive applications across various domains of human endeavor, including communication systems, automatic, and automated devices. The tasks associated with monitoring and diagnosing these systems come with certain challenges. Research in this field holds particular significance for ensuring the resilience and reliability of digital systems in contemporary technological environments. In this context, the study of the characteristics of diagnosing sequential digital structures assumes a special importance. Diagnosing, in this context, refers to the systematic solving of problems related to determining the technical condition, localizing malfunctions (down to individual radio-electronic components), and forecasting the technical state over a specific period. Identifying individual Radio-Electronic Components (RECs) within a digital system means pinpointing a specific microchip whose functioning does not meet the technical specifications. This is crucial, as microchips, despite their complexity and multifunctionality, constitute minimal replaceable units. Monitoring the technical condition is especially crucial in systems containing a large number of interacting sequential digital elements.*

*One of the key challenges in developing methods for monitoring sequential digital structures is their sheer numerical size and the presence of a multitude of logical elements, each of which can be a potential source of error when performing basic logical operations. Hence, engineers have to devise novel, efficient methods and algorithms for error detection in such systems.*

**Keywords:** sequential digital structures, large-scale integrated circuits, technical state diagnostics, Radio-Electronic Components.

**Постановка завдання в загальному вигляді.** На сьогодні спостерігається розширення галузей застосування засобів обчислювальної техніки. Кожні півтора – два роки відбувається зміна поколінь апаратних та програмних засобів, що пов'язано з вдосконаленням елементної бази. Понад півстоліття підтверджується закон, сформульований у 1964 році американським вченим і підприємцем, одним із засновників корпорації мікроелектроніки INTEL Гордоном Муром: кількість транзисторів, що розміщується на кристалі інтегральної схеми, подвоюється кожні 24 місяці. Враховуючи складність аналізу схем із високим ступенем інтеграції на рівні

логічних елементів і використовуючи закінченість функціональних структур в одному пристрої, необхідно розглянути алгоритми контролю функціонування (діагностування на рівні функціональних закінчених вузлів) великих інтегральних схем і цифрових пристроїв на підставі наступних припущень:

- аналіз схем, опису і перетворення їхніх структур потрібно здійснювати на рівні функціональних вузлів;
- тестові послідовності будувати на рівні завдання початкових тестових наборів для різноманітних пристроїв і визначення черговості їх генерування;
- роздільні точки шукати у процесі аналізу схеми і побудові маршрутів для проведення контрольних процедур.

При цьому слід враховувати, що системний контроль технічного стану послідовних цифрових структур і діагностика їх пов'язана зі значними матеріальними та часовими затратами. Одним зі шляхів підвищення ефективності контролю та діагностування є застосування сучасних методів та способів із використанням ЕОМ, що забезпечать швидкість в отриманні результатів про стан контрольованого об'єкта та відкине суб'єктивне тлумачення отриманих даних людиною, яка здійснює ці операції.

Технічний стан послідовних цифрових структур визначається станом її окремих елементів (тобто мікросхем), параметри яких неможливо контролювати безпосередньо.

На практиці зручно та простіше визначати лише певну кількість вихідних параметрів об'єкта контролю, які утримують у собі інформацію відносно поточного стану параметрів внутрішніх елементів об'єкта. Але таке рішення не задовольняє вимоги до функціонування технічних засобів, у складі яких використовуються послідовні цифрові структури.

Тому актуальним науковим завданням є контроль та діагностування складних цифрових схем зі зворотними зв'язками.

**Аналіз публікацій за темою дослідження.** Проведений аналіз показав, що у роботах [1–8] наведено методи, способи та принципи контролю і діагностування різних радіоелектронних систем, у тому числі з послідовними цифровими структурами.

Крім того, слід враховувати, що важливою і достатньою умовою перевірки електричних зв'язків у мікросхемі є [5]:

- доступність функціональних елементів крізь первинні входи;
- можливість транспортування несправностей до первинних виходів.

При цьому об'єкт контролю (мікросхема), як правило, лише частково відповідає згаданим у [5] умовам.

Враховуючи складність вибору контрольних точок і неможливість забезпечити доступ до них (неможливість створення додаткових контрольних виходів), доцільно розробити варіант аналізу схеми з врахуванням існуючих обмежень. Це особливо важливо у процесі контролю та діагностування схем із високим ступенем інтеграції елементів і наявності великої кількості зворотних зв'язків, що характерно для великих інтегральних схем (далі – ВІС).

Також слід враховувати, що методи та способи, які описано в літературі [9–11], не дають можливості швидко отримати результати контролю функціонального стану об'єкта та визначити елемент, який відмовив або може відмовити. При цьому, отримані результати ще слід додатково опрацьовувати. На відміну від них застосування теорії графів дозволяє вирішувати задачу оцінки функціонального стану об'єкта контролю у реальному часі та швидко визначати місце та елемент, який відмовив. Крім того, не потрібно застосовувати додаткових обчислень та обробку отриманої інформації.

**Метою статті** є застосування широко відомої теорії графів для контролю та діагностування технічного стану складної цифрової схеми зі зворотними зв'язками.

**Виклад основного матеріалу.** Враховуючи з одного боку складність аналізу схем підвищеного ступеня інтеграції на рівні логічних елементів І–НЕ, І–АБО–НЕ й т. ін. і

використовуючи закінченість функціональних структур у одному пристрої, доцільно перейти до розробки способу контролю функціонування (і діагностики на рівні функціонально закінчених вузлів) ВІС та складних цифрових пристроїв на їх основі з наступних позицій [6]:

- аналіз схем, опис і перебудову структур здійснювати на рівні функціональних вузлів типу регістрів, шифраторів, лічильників й т. ін.;
- тестові послідовності будувати на рівні завдання початкових тестових наборів щодо різних пристроїв та визначення послідовності їх генерації;
- точки розподілення шукати у процесі аналізу схеми та побудови маршрутів для проведення контрольних процедур.

Розглянемо довільну структуру з'єднання функціональних модулів, котра містить низку входів, виходів, ряд функціональних модулів послідовного типу із замкненими зворотними зв'язками (рис. 1).

Позначимо такі модулі підмножинами елементів  $A_1, A_2, A_3, \dots, A_n$ , які входять до складу множини елементів  $A$ , що визначають кількість ВІС.

Підмножина елементів модулів  $A_i \in a_1^i, a_2^i, \dots, a_k^i$  може бути описана на рівні логічних елементів типу І-НЕ, АБО-НЕ, АБО й т. ін.

Опис схеми, яка досліджується, виконано набором (1):

$$G = \{X, Y, A, \bar{U}, \delta(\lambda)\} \quad (1)$$

де  $X$  і  $Y$  – первинні входи і виходи відповідно;

$A$  – множина функціональних елементів;

$\bar{U}$  – дуги, що з'єднують елементи між собою із первинними входами (виходами),  $x_i(y_i)$ ;

$\delta(\lambda)$  – неявно задіяні функції переходів виходів.

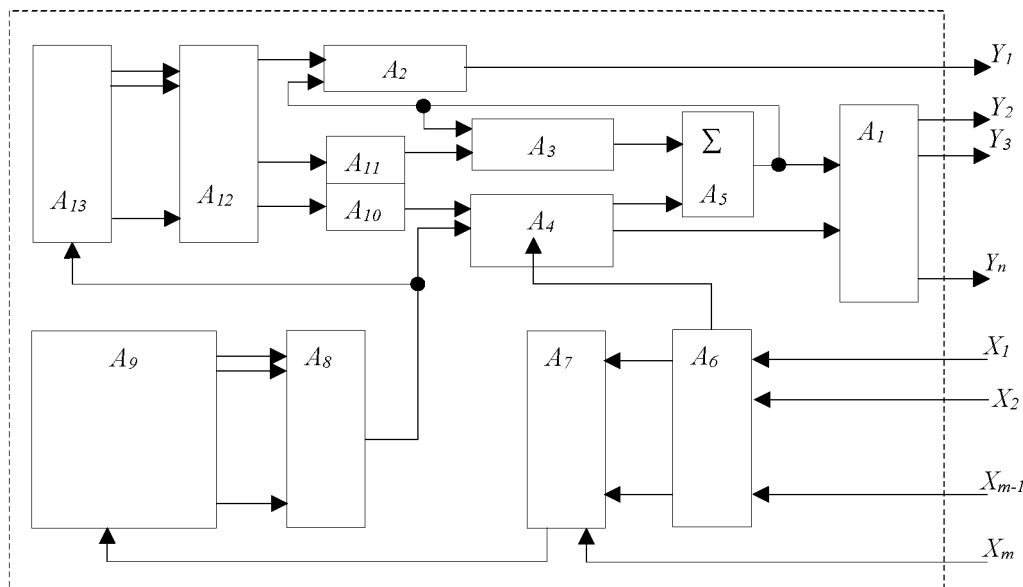


Рис. 1. Структура з'єднання функціональних модулів

Для аналізу схеми (рис. 1) з метою визначення її контролездатності використаємо ту частину її опису (2), яка відповідає значенню графу (рис. 2):

$$G = \{X, Y, A, \bar{U}\} \quad (2)$$

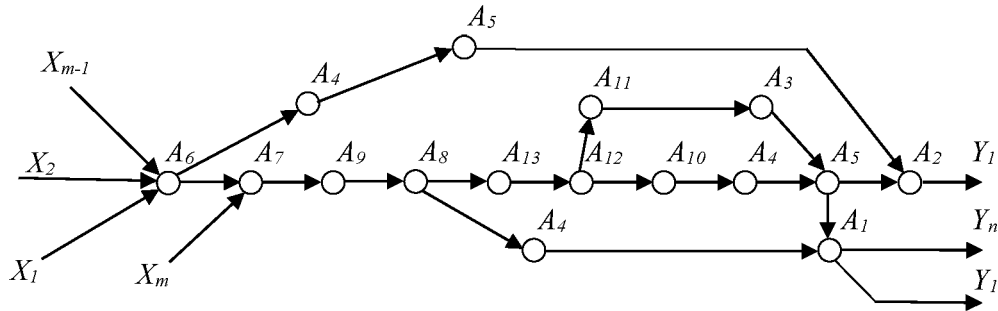


Рис. 2. Граф взаємодії функціональних модулів послідовного типу

Умовно розіб'ємо множину  $G$  на підгрупи  $G_1, G_2, \dots, G_j$  відповідно до кількості первинних виходів  $Y \in y_1, y_2, \dots, y_j$ , тоді кожний підряд  $G_j$  буде визначатися підмножиною елементів  $A_j \in a_1, a_2, a_3, \dots, a_m$ , які лежать на шляхах від  $x_j$  до  $y_j$ .

Побудова графів відбувається, виходячи з наступних основних положень [7]:

- граф є орієнтованим (дає можливість і підстави виконувати обхід графу, рухатися вздовж шляху від первинного виходу до входу або навпаки);
- всі маршрути, що з'єднують первинні входи і виходи, повинні бути незамкнутими,  $i = 0$  (дозволяє виділяти маршрути, для яких  $L \geq 1$ , тобто маршрути, які містять елементи зворотних зв'язків, багатовимірні маршрути).

Вибір елементів зворотних зв'язків відбувається аналізом на повторюваність елементів у маршруті, для цього достатньо провести операції логічного множення кожного елементу  $\oplus^i a_i a_{i-1} \neq 1$ .

Процес побудови підграфів по етапах можна визначити наступним порядком. Побудова первинного маршруту  $\bar{U}_1 \in \bar{U}_{x_1}, \bar{U}_{x_2}, \dots, \bar{U}_{a_i}$  у вигляді підмножини елементів  $A_{x_i} \in a_1, a_2, \dots, a_k$  видаленням їх із масиву опису графу  $G$ . Видалення відбувається зсувом вліво того рядка, на якому знаходиться елемент, який належить маршруту  $\bar{U}_{x_j}$ .

Побудова спряжених гілок, які утворилися завдяки відгалуженню, відбувається перевіркою наявності інцидентних елементів у рядках масиву, що описують елементи, із яких побудований маршрут  $A_{x_i}$ .

Якщо у  $k$ -му рядку відгалужень немає, перевіряється  $k-1$  рядок і так далі.

При наявності відгалужень у  $k$ -му рядку будується спряжена гілка.

За початкову ділянку маршруту приймається  $A_{x_i} \in a_1, a_2, a_3, \dots, a_{k-c}$  і до нього додаються інцидентні елементи  $a_{k-c}, \dots, x_{i+m}$ .

Так отримуємо маршрут (3):

$$A_{x+m} \in a_1, a_2, a_3, \dots, a_{k+1}, \dots, a_{k+m}, \dots, x_{i+m}. \quad (3)$$

Виконуючи послідовно операцію  $\oplus^i a_i a_{i-1} \neq 1$  з виразом (3) при побудові відгалуження, потрібно додатково виконати її для елементів:

$$\begin{aligned} & a_{k+1}, a_{k+2}, \dots, a_{k+m}, \\ & \oplus^c a_{k+m} a_{k-c} \neq 1, \end{aligned} \quad (4)$$

де  $c = 0, 1, 2, \dots$



У випадку знаходження однакових елементів:

при обрахунках у виразі (3) отримуємо елементи зворотного зв'язку (далі – ЗЗ);

при обрахунках у виразі (4) – елементи багатомірних маршрутів (далі – БМ).

Ділянки маршрутів, які утворюють ЗЗ і БМ, використовуються як роздільні точки для перетворення підграфу у деревовидну структуру. Для такого перетворення необхідно ввести додаткову вагу показників, котра використовується як установча або блокуюча. Визначивши за функціями переходів (виходів), через Булеві похідні, шукані значення установчих (блокуючих) входів, здійснюється перетворення тих маршрутів, що підлягають перевіркам у гілках дерева.

Побудова тестів для перетворення маршрутів здійснюється на підставі аналізу структури кожної гілки окремо.

Якщо обмежити клас схем, які розглядаються, схемами з двійковою логікою, тоді побудова тестів для кожної гілки може бути зведена до визначення допустимої кількості станів кожної гілки і умов, які забезпечують проходження сигналів по ній.

Для прикладу, візьмемо із представленої на рис. 1 структури, з кожного функціонального модуля по одному з елементів і побудуємо маршрут, який містить:

$$y_j, a_i^1, a_i^2, a_i^3, a_i^4, a_i^6 \in G_j,$$

$$a_i^1 \in A_1; a_i^2 \in A_2; \dots; a_i^6 \in A_6.$$

Допустима кількість станів маршруту визначається виразом:

$$[S_i] = [S_i^1] [S_i^2] \dots [S_i^6].$$

Роздільні точки для маршруту  $G_i$  із аналізу структури схеми знаходяться у модулях  $A_3, A_6, A_8, A_{10}, A_{11}$ . Вважаючи, що пристрій генерує стійкі рівні, визначимо потрібний стан в вузлових точках  $U_i = dA_i / dU_p$ .

Завжди доцільно генерувати установчі набори одного рівня, а в точках поділу перетворювати їх до виду, який потрібний для перевірки за допомогою функціональних елементів типу І, АБО-НЕ, тоді достатньо буде вказувати номери стимулюючих роздільних точок.

Забезпечивши перетворення послідовної структури у деревоподібну, необхідно визначити умови перевірки відповідно до структури відгалужень основної гілки.

Для перевірки функціонування на маршруті  $G_i$ , який не має установчих входів, необхідно здійснити  $n \in 2S$  експериментів при заданих станах відгалужень. Така кількість експериментів необхідна на першому етапі для визначення початкового стану маршруту  $G_j$ , при зміні початкового стану  $y_j^{0(i)} \rightarrow \overline{y_j^{1(o)}}$ , та на другому етапі для визначення правильної роботи маршруту, тобто перехід зі стану  $\overline{y_j^{1(o)}} \rightarrow y_j^{0(i)}$ .

Допустима кількість станів відгалужень може збільшувати кількість потрібних контрольних елементів, якщо зміна станів модуля (елемента)  $S_i^j$  визначається переходом відгалужень через  $S_i^j$  станів. Тоді загальна кількість потрібних елементів для перевірок  $G_i$  становить:

$$n^1 \leq 2S_1 S_1^1,$$

а для перевірки підграфу складає:

$$N = \sum_{i=1}^{i=k} n^i,$$

де  $i=1, 2, 3, \dots, k$  – кількість поділів підграфа.

Практичний інтерес представляє кількість необхідних роздільних точок і генератор для створення відповідних сигналів (умови, при яких він повинен працювати і відключатися).

Нехай ОК містить  $Y \in y_1, y_2, \dots, y_n$  первинних виходів,  $X \in x_1, x_2, \dots, x_n$  первинних входів і описується множиною  $A$  функціональних елементів. Тоді кожен вихід  $y_j$  може бути з'єднаний з  $X$  входами та  $m$  маршрутами, тоді всього може бути  $N \leq mn$  маршрутів. Однак, якщо можливих коренів дерев може бути  $G \leq n$ , то  $m$  первинних входів не завжди визначають істинне число можливих розгалужень і багатомірних маршрутів.

Якщо припустити, що число розгалужень  $U \leq z^m$ , тоді кількість можливих маршрутів відповідно збільшується до  $\overline{N}_U \leq Z^m n$ . Немає необхідності змінювати роздільні точки всіх маршрутів, так як вони не можуть бути виключені одночасно, тому слід скористатися почерговою роботою визначеної структури.

З іншого боку, припущення, що ОК складається із ряду пристроїв, які описуються підмножинами  $A_i \in a_1, a_2, a_3, \dots, a_j$ , що являють собою регулярні структури, значно спрощує аналіз пристроїв. Практично в цьому випадку необхідно передбачити роздільні точки в управляючій ланці кожного пристрою. Кількість роздільних точок:

$$N_p \approx A/n$$

Кількість можливих вузлів, які сходяться, визначається виразом:

$$N_C \leq C_n^k,$$

де  $k$  – кількість елементів, що сходяться у одній вершині.

### Висновки

Застосування теорії графів дозволяє швидко та точно визначати технічний стан об'єкта контролю (функціональних модулів послідовного типу). Також вона дає можливість знайти елемент, який відмовив, враховуючи існуючу кількість входів та виходів елемента. Цей спосіб дозволяє уникнути тих недоліків, які присутні в інших способах контролю та діагностування складних цифрових схем зі зворотними зв'язками [4].

Слід зазначити, що при побудові схеми дуже рідко виникає ситуація, коли необхідна вся сукупність вузлів, що сходяться (розходяться), тому  $N_C \ll C_n^k$ .

У цих випадках, коли така структура є, доцільно здійснювати перевірку на рівні функціональних вузлів цього типу.

Отже, результати, отримані в роботі, можуть знайти застосування під час побудови систем оцінки технічного стану складних цифрових схем та пристроїв з функціональними модулями послідовного типу.

**Подальші дослідження** слід проводити у напрямку створення ефективних тестових послідовностей, які нададуть змогу достатньо швидко та точно визначати функціональний стан ОК з функціональними модулями послідовного типу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основи технічної діагностики / За ред. П. П. Пархоменка. Луганськ: Вид. «Ноулідж», 2012. 480 с.
2. Чжан Г. Діагностика відмов цифрових обчислювальних систем / Г. Чжан, Е. Маннинг, Г. Метц. Харків: ООО «Компанія ОМІТ», 2006. 292 с.
3. Доценко Б. И. Определение эффективности проверки технического состояния систем. Техника воздушного флота. Харьков: Изд. Харьковского авиационного института, 1991. С. 23–29.
4. Кузавков В., Хорошко В., Янковський О. Технічна діагностика складних технічних об'єктів // Захист інформації. 2022. Т. 24, № 3. С. 115–120.
5. Кузавков В., Хорошко В., Янковський О., Болотюк Ю. Вимоги до засобів діагностування обчислювальних систем // Безпека інформації. 2022. Т. 28, № 3. С. 127–132.
6. Ярмолик В. Н. Контроль и диагностика цифровых узлов ЭВМ. Вильнюс: Наука и техника, 1992. 240 с.
7. Цой С. Прикладна теорія графа. Алма-Ата: Наука, 2001. 500 с.
8. Стрельников В. П. Оценка и прогнозирование надёжности электронных элементов и узлов / В. П. Стрельников, А. П. Федухин. К: Лотос, 2002. 486 с.
9. Настенко Є. А., Павлов В. А., Городецька О. К., Корнієнко Г. А. Методи моделювання складних систем і процесів / О. Г. Івахненко. К.: КПІ ім. Ігоря Сікорського, 2022. 144 с.
10. Wu Chi-Feng. Fault simulation and test algorithm generation for random access memories / Chi-Feng Wu, Chih-Tsun Huang, Kuo Liang Cheng, Cheng-Wen Wu // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2002. Vol. 21. Issue: 4. P. 480–490.
11. Li Jin-Fu. March-based RAM diagnosis algorithms for stuck-at and coupling faults / Jin-Fu Li, Kuo-Liang Cheng, Chih-Tsun Huang, Cheng-Wen Wu // IEEE Trans. on Fuzzy Systems. 2002. Vol. 10, Issue 2. P. 155–170.

УДК 004.49+004.8

д-р техн. наук, ст. наук. співроб. Чевардін В. Є. ORCID: 0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)  
канд. техн. наук Юрченко О. В. ORCID: 0000-0002-4851-0400 (ВІТІ ім. Героїв Крут)  
канд. техн. наук Залужний О. В. ORCID: 0000-0002-8722-4087 (ВІТІ ім. Героїв Крут)  
канд. техн. наук Пелешок Є. В. ORCID: 0000-0003-0033-1160 (НДІ ВР)

## АНАЛІЗ КОНКУРЕНТНИХ АТАК НА МОДЕЛІ МАШИННОГО НАВЧАННЯ СИСТЕМ КІБЕРЗАХИСТУ

Сучасні тенденції розвитку систем кіберзахисту пов'язані з широким застосуванням технологій машинного навчання для виявлення і запобігання кіберзагрозам. Водночас зловмисники шукають способи ухилення від детектування такими системами, використовуючи при цьому як традиційні методи атак, так і нові, орієнтовані виключно на протидію штучному інтелекту, – конкурентні атаки. Тому пошук шляхів протидії конкурентним атакам є актуальним науково-технічним завданням. Для їх вивчення використовують конкурентне машинне навчання (*Adversarial Machine Learning – AML*), яке полягає у моделюванні таких атак.

Метою досліджень є визначення шляхів підвищення стійкості систем кіберзахисту, що функціонують із використанням технологій машинного навчання, до впливу атак на основі *AML*-моделей.

У статті наведено приклади застосування методів машинного навчання в системах кіберзахисту. Проведено опис моделей конкурентних атак, а саме: моделі ухилення, отруєння, функціонального вилучення, інверсії та моделі атаки на належність. Розглянуто можливі сценарії їхнього здійснення. Проаналізовано приклади конкурентних атак на моделі машинного навчання для розпізнавання зображень та текстових повідомлень, виявлення алгоритмів генерації доменних імен, шкідливого програмного забезпечення в *HTTP*-трафіку, шкідливого вмісту в електронних листах, обходу антивірусних програмних засобів.

Дослідження показали, що навіть не маючи доступу до алгоритмів роботи моделей машинного навчання, можливо реалізувати обхід системи кіберзахисту. Тому для забезпечення безпеки мереж і послуг засобами кіберзахисту зі штучним інтелектом необхідно враховувати необхідність протидії конкурентним атакам. Із цією метою запропоновано: здійснювати збирання та агрегацію навчальних даних для кожної моделі машинного навчання окремо, а не отримання їх із загально-доступних джерел; проводити оптимізацію вмісту журналів подій, з урахуванням можливості використання інформації, що знаходиться в них для створення конкурентних атак; забезпечувати захист навчальних даних та алгоритмів функціонування моделей; у випадку розгортання систем кіберзахисту на об'єктах критичної інфраструктури використовувати спеціально розроблені моделі машинного навчання, яких немає в загальному доступі, що ускладнить можливість створення атаки функціонального вилучення.

**Ключові слова:** штучний інтелект, машинне навчання, глибоке навчання, конкурентне машинне навчання, конкурентні атаки, шкідливе програмне забезпечення, кібератаки, кіберзахист, кібербезпека.

### *V. Chevardin, O. Yurchenko, O. Zaluzhnyi, Ye. Peleshok Analysis of adversarial attacks on the machine learning models of cyberprotection systems.*

Modern trends in the development of cyber protection systems are associated with the widespread use of machine learning technologies to detect and prevent cyber threats. At the same time, attackers are looking for ways to evade detection by such systems, using both traditional attack methods and new ones aimed exclusively at countering artificial intelligence - adversarial attacks. Therefore, finding ways to counteract adversarial attacks is an urgent scientific and technical task. *Adversarial Machine Learning (AML)* is used to study them, which consists in simulating such attacks.

The purpose of research is to determine ways to increase the resilience of cyber defense systems operating with the use of machine learning technologies to the impact of attacks based on *AML* models.

The article provides examples of the application of machine learning methods in cyber protection systems. The models of adversarial attacks are described, namely: models of evasion, poisoning, functional extraction, inversion, and models of membership inference attack. Possible scenarios of their implementation are considered. Examples of adversarial attacks on machine learning models for recognizing images and text messages, detecting domain name generation algorithms, *HTTP* traffic malware, malicious content in e-mails, bypassing antivirus software are analyzed.

Studies have shown that even without access to the algorithms of machine learning models, it is possible to bypass the cyber protection system. Therefore, to ensure the security of networks and services by means of cyber protection with artificial intelligence, it is necessary to take into account the need to counter adversarial attacks. For this purpose, it is proposed to: collect and aggregate training data for each machine learning model individually, instead of obtaining them from publicly available sources; optimize the content of event logs, taking into account the possibility of using the information contained in them to create adversarial attacks; to ensure the protection of training data and algorithms of

*the functioning of models; in the case of deploying cyber protection systems on critical infrastructure objects, use specially developed machine learning models that are not publicly available, which will complicate the possibility of creating a functional extraction attack.*

**Keywords:** artificial intelligence, machine learning, deep learning, adversarial machine learning, adversarial attacks, malware, cyberattacks, cyber defense, cyber security.

**Постановка завдання в загальному вигляді.** В наш час штучний інтелект (*Artificial Intelligence – AI*) активно застосовується в системах кіберзахисту. Машинне навчання (*Machine Learning – ML*) є компонентом *AI*. Одним із напрямків досліджень у сфері *ML* є глибоке навчання (*Deep Learning – DL*). Системи кіберзахисту на основі *ML* здійснюють детектування кібератак, шкідливого програмного забезпечення (далі – ШПЗ), виявлення аномалії в мережі та ін. [1; 2], однак *ML*-моделі також є об'єктом кібератак. Атаки, що призводять до прийняття хибних рішень *ML*-моделлю, називають конкурентними (*adversarial attacks*) [3]. Вивченням можливостей зловмисників і їхніх цілей, а також розробкою методів атак, що експлуатують вразливості *ML*-моделей на етапах розробки, навчання і використання, займається конкурентне машинне навчання (*Adversarial Machine Learning – AML*) [4; 5].

Враховуючи, що майбутній розвиток систем кіберзахисту пов'язаний із широким застосуванням моделей *ML*, гострим та актуальним науково-технічним завданням є дослідження існуючих *AML*-моделей та пошук шляхів протидії конкурентним атакам.

#### **Аналіз останніх публікацій**

Значна кількість досліджень із кібербезпеки, присвячених застосуванню методів машинного навчання, свідчить про їхню вагомую роль у сфері кіберзахисту інформаційно-комунікаційних систем [1; 2; 6–10]. Зокрема, дерево рішень використовується для виявлення вторгнень [1; 6]. Для виявлення аномальної поведінки IoT (Internet of Things) пристроїв застосовується метод опорно-векторних машин та *k*-найближчих сусідів [8]. Останній також знаходить місце при виявленні фішингових атак [7]. Наївний баєсів класифікатор застосовується для виявлення аномального вмісту мережевих пакетів [9]. Логістична регресія дозволяє виявляти шкідливий ботнет-трафік [10]. Однак ці інструменти, за своєю суттю, не є надійними та безпечними. Зловмисники, які хочуть уникнути виявлення незахищеними моделями машинного навчання, можуть зробити це з відносною легкістю. В існуючих наукових публікаціях наведено перелік відомих атак на моделі машинного навчання та їхню класифікацію [11], розглянуто основні аспекти безпеки технологій машинного навчання та напрямки здійснення атак [12], але не проведено аналіз прикладів успішних атак на системи кіберзахисту, що функціонують на основі штучного інтелекту.

**Метою статті** є визначення шляхів підвищення стійкості систем кіберзахисту, що функціонують із використанням технологій машинного навчання, до впливу атак на основі *AML*-моделей.

#### **Виклад основного матеріалу**

Відомими методами детектування подій у кіберпросторі є сигнатурний та поведінковий аналізи. Алгоритми на основі сигнатурного аналізу не забезпечують захист від використання поліморфних кодів та диверсифікації ШПЗ. Для розв'язання цих задач, як правило, застосовують поведінковий аналіз на основі *ML*-моделей. Для таких систем зловмисники розробляють свої методи, прийоми та способи обходу. Відомі приклади атак описані в матриці *MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems)* [13] – базі знань про прийоми і методи дій проти моделей машинного навчання. *ATLAS* було розроблено з метою підвищення обізнаності фахівців щодо наявних загроз. До неї увійшли дані, отримані з досвіду *IBM, NVIDIA, Bosch, Microsoft* та інших відомих компаній, які відіграють важливу роль у сфері інформаційних технологій. Наведена матриця надає аналітикам безпеки систематизовану картину загроз для *ML*-моделей.

У процесі створення будь-якої моделі машинного навчання здійснюється збирання, аналіз та оброблення даних, навчання, перевірка роботи моделі та її впровадження. Після

впровадження користувачі мають змогу надсилати запити та отримувати відгуки (результати роботи) *ML*-моделі. Відповідно, існують два напрямки здійснення шкідливого впливу на *ML*-моделі: вплив на етапі навчання моделі (перед впровадженням) і вплив на етапі її використання (на етапі отримання відгуку моделі). На цих етапах можуть бути реалізовані різні моделі атак, а саме: модель ухилення (*evasion model*), модель отруєння (*poisoning model*), модель функціонального вилучення (*functional extraction model*), модель інверсії (*inversion model*) та модель атаки на приналежність (*model of membership inference attack*) [4]. У таблиці 1 наведено опис цих моделей та вказано етапи, на яких вони застосовуються.

Таблиця 1

**AML-моделі атак**

Модель атаки	Опис атаки	Етап атаки
Модель ухилення ( <i>Evasion model</i> )	Зловмисник змінює запит до моделі, щоб отримати бажаний результат (обійти захист). Для цього йому потрібно вивчити функціонування моделі, навіть не знаючи її алгоритмів. Такі атаки виконуються шляхом надсилання різних за змістом запитів до моделі та спостереження за результатом (відгуком моделі)	Використання
Модель отруєння ( <i>Poisoning model</i> )	Зловмисник отримує доступ та змінює навчальні дані <i>ML</i> -моделі або саму модель, щоб отримати бажаний результат її роботи. Модель може бути «перепрограмована» для виконання нового непередбаченого розробниками завдання. Доступ до навчальних даних також може призвести до компрометації особистих даних користувачів	Навчання
Функціональне вилучення ( <i>Functional Extraction model</i> )	Зловмисник створює (відтворює) функціонально еквівалентну модель (офлайн-копію моделі) шляхом ітераційних запитів до моделі <i>ML</i> та оцінки відгуків. Це дозволяє зловмиснику перевірити створену офлайн-копію моделі перед подальшою атакою на онлайн-модель (робоча модель)	Використання
Модель інверсії ( <i>Inversion model</i> )	На основі аналізу відгуків моделі зловмисник здійснює прогнозування вхідних даних цієї моделі. Аналізуючи ці дані зловмисник може дізнатись інформацію про суб'єкт даних	Використання
Модель атаки на приналежність ( <i>Model of membership inference attack</i> )	Зловмисник визначає, чи є вказаний запис даних частиною набору даних для навчання моделі. Виявлення таких даних може призвести до проблем із конфіденційністю у випадках, якщо модель навчали, використовуючи конфіденційну інформацію	Використання

Розглянуті моделі атак можуть бути реалізовані за наступними сценаріями.

*Сценарій 1. Атака на основі відгуку ML-моделі (Inference Attack)* (рис. 1). Це найпоширеніший сценарій, при якому зловмисник може лише надсилати запити до моделі і спостерігати за її відповіддю (модель розгортається як кінцева точка *API – Application Programming Interface*). Зловмисник контролює вхідні дані в модель, але він не знає, як ці дані обробляються [14].

Атаки за цим сценарієм мають за мету створення такого набору даних, при обробці якого модель видаватиме хибні результати. Один із результатів його виконання описано в [15]. На працездатність була перевірена *ML* модель розпізнавання образів, що використовує нейронні мережі. В наведеному прикладі було застосовано метод швидкого градієнта (*Fast Gradient Sign Method – FGSM*) для генерації конкурентних (*adversarial*) вхідних даних (зображень) та здійснено їх тестування на згортковій нейронній мережі “*GoogLeNet*”.

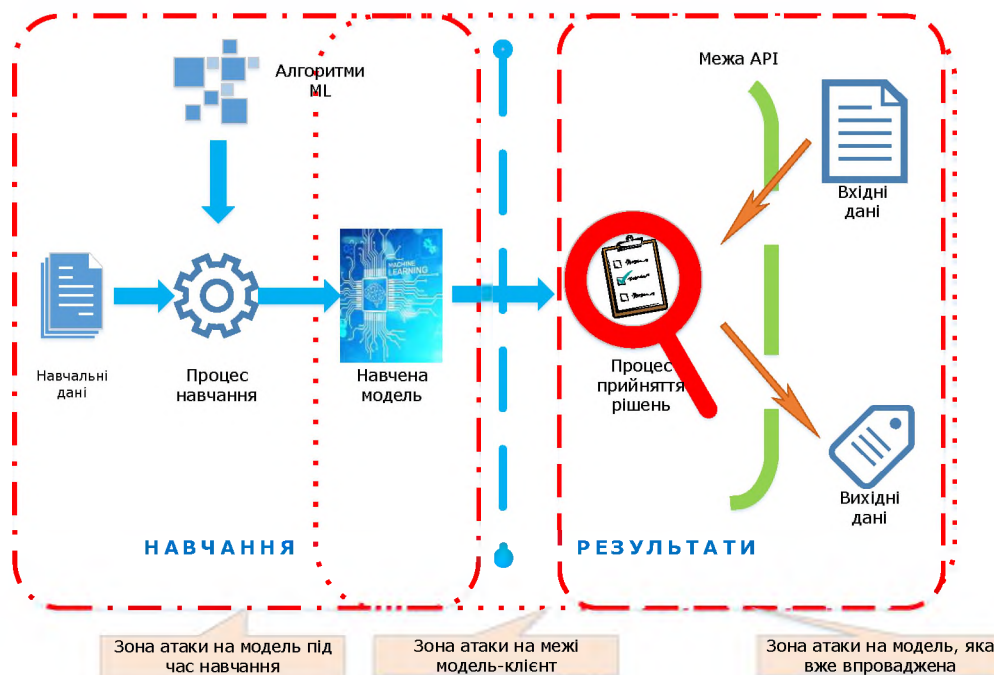


Рис. 1. Зони атак на моделі машинного навчання

Суть методу полягає в тому, що зломисник модифікує вихідне зображення в напрямку градієнта функції втрат відносно вхідного зображення. Значення змін має бути настільки малим, щоб не бути детектованим. Якщо розмір конкурентної пертурбації  $\|\eta\|_\infty < \varepsilon$  (де  $\|\eta\|_\infty$  – максимальна або нескінченна норма), то конкурентний зразок можна обчислити за формулою (1) [15]:

$$\hat{x} = x + \varepsilon \cdot \text{sign}(\nabla_x J(\theta, x, y)), \quad (1)$$

де  $x$  – вхідне зображення;

$J(\theta, x, y)$  – функція втрат;

$\theta$  – параметри моделі;

$Y$  – зображення, яке має розпізнати згорткова мережа;

$\nabla_x$  – градієнт функції втрат.

У наведеному прикладі значення максимально-допустимих змін, що вносяться в зображення,  $\varepsilon = 0,007$ .

На рисунку 2 продемонстровано застосування методу *FGSM*.

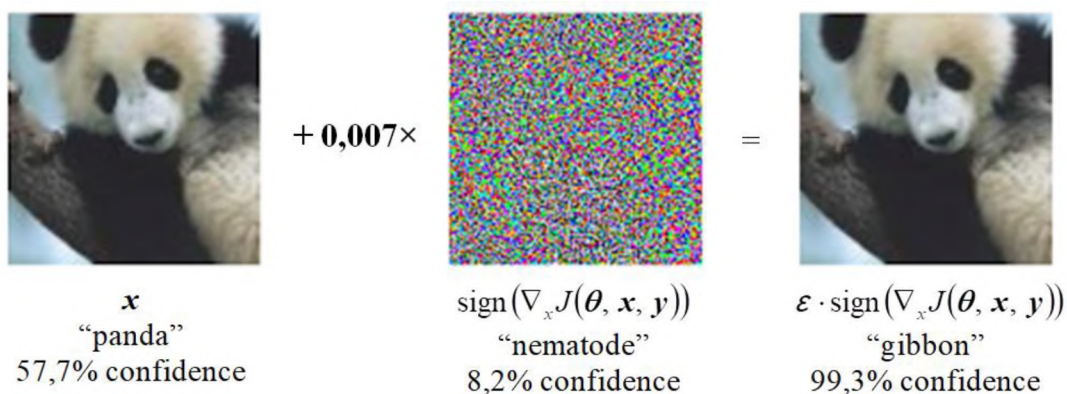


Рис. 2. Приклад виконання атаки на впроваджену модель розпізнавання зображень

Спочатку модель розпізнала панду на фотографії з ймовірністю 57,7 %. Потім до зображення додали незначний шум, створений за алгоритмом *FGSM*. Після накладання зображень модель з ймовірністю 99,3 % розпізнала панду як гібона, хоча людина безпомилково визначила б зображений об'єкт як панду.

*Сценарій 2. Атака на ML-модель під час її навчання (Training Time Attack)* (див. рис. 1). У цьому випадку зловмисник контролює навчальні дані, отримавши попередньо доступ до них [14]. Один із результатів виконання такого сценарію описано в [16]. Корпорація *Microsoft* створила *Tau*, чат-бот у *Twitter*, для молоді США. Він був розроблений, щоб охопити широкі кола молоді з її специфічним сленгом. *Tau* використовував взаємодію з користувачами *Twitter* як навчальні дані для покращення своєї лексики та розширення словарного запасу. Розробники сподівались, що властивість боту накопичувати необхідну лексичну інформацію призведе до покращення рівня спілкування з користувачами. Група користувачів *Twitter* об'єдналася з наміром зіпсувати бот *Tau*, використовуючи такий зворотний зв'язок. У своїх скоординованих зусиллях вони використали функцію «повторюй за мною», яка була вбудована в *Tau*. Вже через 16 годин чат-бот створив 95 000 повідомлень і вони були переважно лайливими та образливими. Внаслідок цієї скоординованої атаки навчальні дані *Tau* були отруєні і *Microsoft* зупинила дію свого чат-бота. Те, що починалося цікавим експериментом, менш ніж за добу зазнало краху.

*Сценарій 3. Атака на межі ML-модель – клієнт (Attack on Edge/Client)* (див. рис. 1). У цьому випадку модель встановлена у клієнта (наприклад, у телефоні) або використовується на межі модель – клієнт (наприклад, інтернет-речей). Зловмисник може оцінити алгоритми функціонування моделі шляхом застосування методів реверс-інжинірингу до служби, встановленої у клієнта [14]. Приклад атаки за цим сценарієм буде наведено нижче.

Розглянуті сценарії ілюструють атаки за допомогою «чорної скриньки». Також ці сценарії атак використовуються при налаштуванні «білої скриньки», коли зловмисник отримує доступ до архітектури *ML*-моделі, вихідного коду або навчальних даних. Подібні підходи застосовуються і під час здійснення атак на *ML*-моделі систем кіберзахисту.

Розглянемо декілька прикладів успішних атак на системи кіберзахисту, які використовують штучний інтелект.

#### **Ухилення від детектування ШПЗ в HTTP-трафіку Deep Learning моделлю.**

Дослідницька група *Palo Alto Networks Security AI* випробувала *DL*-модель для виявлення трафіку контролю та управління (*C2*-трафік) шкідливим програмним забезпеченням у *HTTP*-трафіку (робоча модель). Вказана модель була запропонована в роботі: «*URLNet: Learning a URL representation with deep learning for malicious URL detection*» [17]. Проаналізувавши статтю, дослідники створили функціонально еквівалентну модель (ФЕМ) та навчили її на датасеті *C2*-трафіку *HTTP*-протоколу, що містив близько 33 мільйонів нешкідливих і 27 мільйонів шкідливих заголовків *HTTP*-пакетів. Оцінка моделі показала близько 99 % «*true positive*» результатів, при цьому «*false positive*» результатів було менше 1 %.

Тестування ФЕМ здійснювалось на заголовках *HTTP*-пакетів відомих зразків *C2*-трафіку ШПЗ. Достовірність виявлення ШПЗ перевищила 99 %. Наступним кроком було створення зразків ухилення від детектування шляхом видалення полів із заголовка пакета, які зазвичай не використовуються для передачі *C2*-трафіку (наприклад, керування кешем, встановлення з'єднання тощо). Отримані зразки тестувались на розробленій моделі та коригувались доти, доки не було забезпечено ухилення від виявлення.

За допомогою створених зразків було виконано онлайн-ухилення від робочої моделі виявлення ШПЗ. Створені пакети були визначені як доброякісні з достовірністю >80 % [18]. Загальна схема ухилення зображена на рисунку 3.



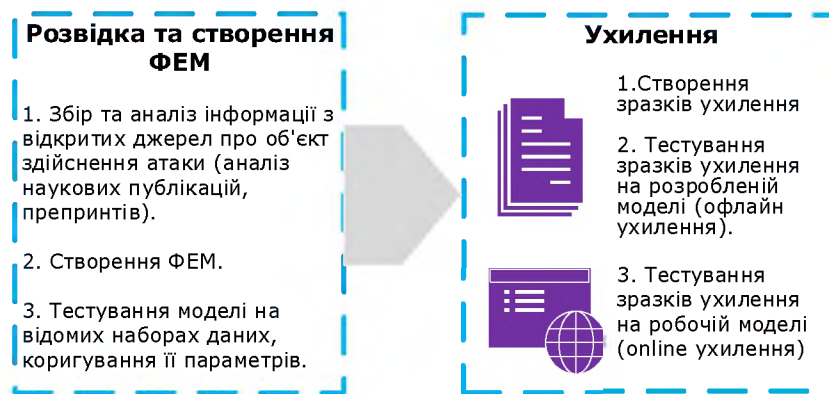


Рис. 3. Схема ухилення від детектування ШПЗ в HTTP-трафіку

### Ухилення від виявлення доменних імен, що створені з використанням Domain Generation Algorithm (DGA).

Дослідницька група *Palo Alto Networks Security AI* змогла обійти детектор, який здійснює виявлення доменних імен, що створені з використанням *Domain Generation Algorithm (DGA)* [19]. Спочатку дослідники провели пошук наукових праць та технічних рішень на основі штучного інтелекту, що пов'язані з виявленням *DGA*. Далі вони протестували загальнодоступну модель виявлення *DGA*, що базується на згортковій нейронній мережі (*Convolutional Neural Network – CNN*), на наборі даних доменних імен (створених *DGA*), який містить 50 мільйонів доменних імен із 64 сімейств ботнетів. Точність виявлення ботнетів склала більш ніж 70 % на 16 сімействах ботнетів (25 %). На наступному кроці, скориставшись результатами наукових публікацій [20], дослідники розробили техніку «мутації» доменних імен. Внаслідок експерименту було виявлено, що після того, як у доменне ім'я, згенероване *DGA*, одноразово вставили лише один рядок, рівень виявлення всіх 16 сімейств ботнетів *DGA* впав до менш ніж 25 %.

Запропонована дослідниками техніка «мутації» дозволяє уникати виявлення *DGA ML*-моделями, не обмежуючись обходом засобів захисту на основі *CNN* [19]. Загальна схема ухилення зображена на рисунку 4.

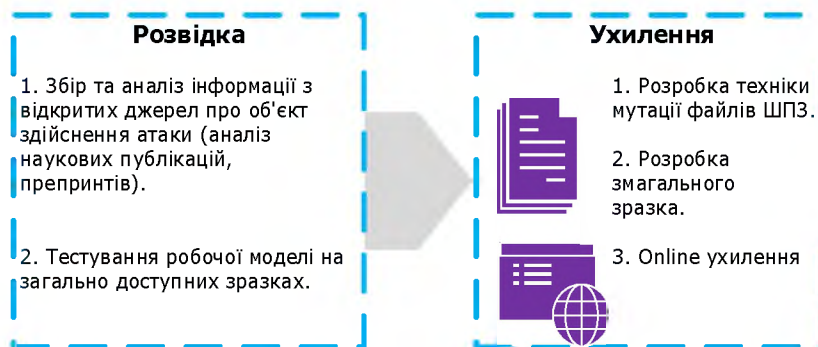


Рис. 4. Схема ухилення від виявлення DGA ботмереж у доменних іменах

### Масоване отруєння (Poisoning).

Дослідниками компанії *McAfee* було помічено незвичне збільшення кількості звітів про відоме сімейство програм-вимагачів [21]. Під час розслідування справи було виявлено, що багато зразків цього сімейства були подані через популярну платформу обміну вірусами протягом короткого проміжку часу (*VirusTotal*). Подальше дослідження показало, що на основі подібності рядків усі зразки були еквівалентними, а на основі подібності коду вони

були схожими на 74–98 %. Цікаво, що час компіляції був однаковий для всіх зразків. Після додаткових досліджень було встановлено, що зловмисники використовували «metame» – інструмент маніпулювання метаморфічним кодом, щоб маніпулювати вихідними (не шкідливими) файлами для створення «мутантних» варіантів [22]. Створені варіанти не завжди були виконуваними файлами, але *ML*-модель класифікувала їх як одне й те саме сімейство програм-вимагачів.

Послідовність дій зловмисника була такою: крок 1 – використання зразка зловмисного програмного забезпечення з поширеного сімейства програм-вимагачів як основи для створення «мутантних» варіантів; крок 2 – завантаження на платформу VirusTotal зразків «мутантів». Як наслідок, системи захисту почали класифікувати файли як сімейство програм-вимагачів, хоча більшість із цих файлів навіть не запускались. Зразки «мутантів» отруїли набір даних, які *ML*-модель використовує для ідентифікації та класифікації цього сімейства програм-вимагачів. Схема масованого отруєння зображена на рисунку 5.



Рис. 5. Схема масованого отруєння моделі детектування програм-вимагачів

#### Обхід виявлення ШПЗ системою «Cylance AI».

Дослідники компанії *SkylightCyber* [13] змогли знайти універсальний спосіб обходу антивірусного програмного засобу (АВПЗ) «Cylance», який функціонує на основі штучного інтелекту. Компанією було проведено дослідження моделі штучного інтелекту, що використовується в АВПЗ «Cylance». Спочатку було здійснено емпіричне тестування різних нешкідливих і шкідливих файлів та визначено, що оцінка може коливатися від –1000 для найбільш шкідливих файлів до +1000 для найбільш безпечних файлів. Надалі, з метою визначення механізму підрахунку балів, для подальшого обходу було здійснено реверс інжиніринг коду програми. Проаналізовано процес вилучення ознак з виконуваних файлів PE (Portable Executable) формату та особливості формування вектору ознак. На основі проведених досліджень вдалось сформулювати список рядків, які необхідно додати до шкідливого файлу для того, щоб значно зменшити ймовірність його детектування. З використанням розробленого способу 88,4 % модифікованих шкідливих файлів було детектовано як нешкідливі. Схему дій зловмисників зображено на рисунку 6.

#### Обхід виявлення шкідливого вмісту в електронному листуванні.

Випадок CVE-2019-20634 описує [19], як дослідники із *Silent Break Security* змогли ухилитися від системи захисту електронної пошти *ProofPoint*, яка використовує заголовки електронних листів для детектування шкідливого вмісту. Спочатку надсилається велика кількість електронних листів та збираються оцінки моделі *ML Proofpoint*. Визначається, яка змінна в оцінці відповідає за безпеку електронної пошти. Використовуючи ці оцінки, дослідники відтворили режим машинного навчання, побудувавши ФЕМ. Висновки, отримані внаслідок використання офлайн-моделі, дозволили дослідникам створювати шкідливі

електронні листи, які змогли обійти системи захисту електронної пошти *ProofPoint*. Порядок дій дослідників зображено на рисунку 7.

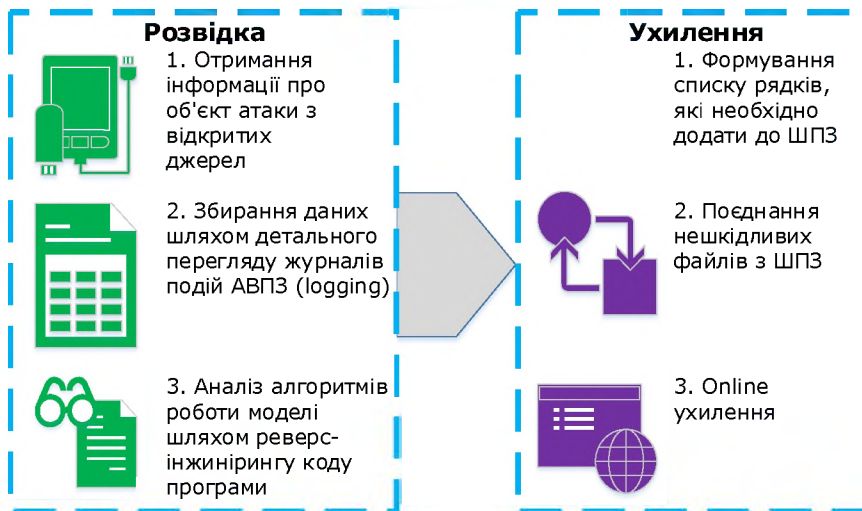


Рис. 6. Схема обходу моделі виявлення ШПЗ

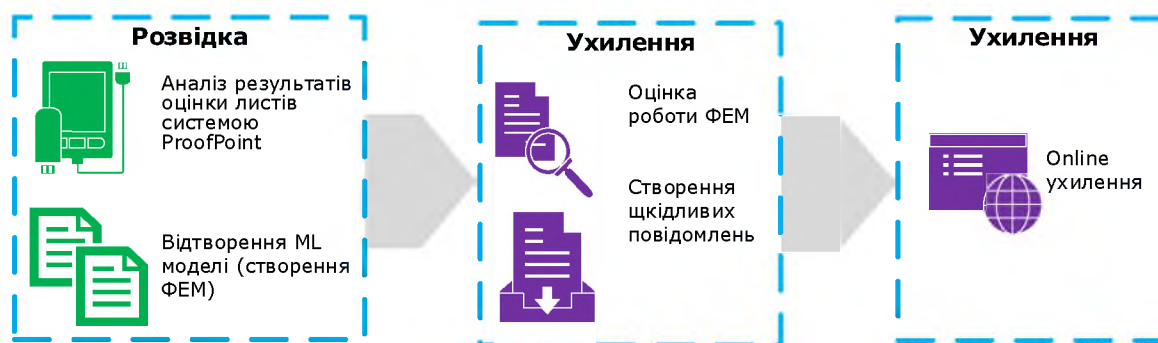


Рис. 7. Схема ухилення від детектування шкідливого вмісту в електронних листах

### Висновки

У роботі досліджено *ML*-моделі виявлення вторгнень, аномалій, фішингових атак, шкідливого програмного забезпечення та ботнетів, які реалізовані на основі дерева рішень, методу опорно-векторних машин, *k*-найближчих сусідів, наївного баєсового класифікатора, логістичної регресії, а також штучних нейронних мереж. Розглянуто існуючі *AML*-моделі та проведено аналіз прикладів їхнього застосування для здійснення конкурентних атак ухилення, отруєння, функціонального вилучення на системи кіберзахисту на основі *ML*-моделей.

Дослідження показали, що навіть не маючи доступу до алгоритмів роботи моделей машинного навчання, можливо реалізувати обхід системи кіберзахисту. Наприклад, дослідницька група «*Palo Alto Networks Security AI*» досягла зниження ефективності виявлених ботнетів моделлю глибокого навчання на 25 % та обійшла згорткову нейронну мережу виявлення ШПЗ в *HTTP*-трафіку у 80 % випадків. Шляхом ефективної реалізації моделі ухилення від виявлення ШПЗ антивірусним програмним засобом «*Cylance*» дослідникам компанії «*SkylightCyber*» вдалося обійти захист в 88,4 % випадків. Здійснивши атаку на відому платформу обміну вірусами «*VirusTotal*», зловмисникам вдалось отруїти навчальний набір даних *ML*-моделі, що призвело до хибного детектування програм-вимагачів.

Отже, для забезпечення безпеки мереж і послуг засобами кіберзахисту зі штучним інтелектом необхідно враховувати необхідність протидії конкурентним атакам, а саме:

- забезпечувати збір та агрегацію навчальних даних кожною системою окремо, а не отримувати їх із загально-доступних джерел;
- здійснювати оптимізацію вмісту журналів подій, з урахуванням можливості використання інформації, що знаходиться в них, для створення конкурентних атак;
- у випадку розгортання систем кіберзахисту на об'єктах критичної інфраструктури використовувати спеціально розроблені *ML*-моделі, яких немає в загальному доступі, що ускладнить можливість створення їх ФЕМ;
- забезпечити захист навчальних даних та алгоритмів функціонування *ML*-моделей.

**Напрямок подальших досліджень** є аналіз існуючих методів підвищення стійкості систем кіберзахисту зі штучним інтелектом до впливу конкурентних атак.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Al-Omari M., Rawashdeh M., Qutaishat F., Alshira'H M., Ababneh N. An intelligent tree-based intrusion detection model for cyber security // Journal of Network and Systems Management. 2021. Vol. 29 (2). P. 1–18. DOI: 10.1007/s10922-021-09591-y.
2. Xin, Yang & Kong, Lingshuang & Liu, Zhi & Chen, Yuling & Li, Yanmiao & Zhu, Hongliang & Mingcheng, Gao & Hou, Haixia & Wang, Chunhua. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access. 2018. P. 1-1. URL: [https://www.researchgate.net/publication/325159145\\_Machine\\_Learning\\_and\\_Deep\\_Learning\\_Methods\\_for\\_Cybersecurity](https://www.researchgate.net/publication/325159145_Machine_Learning_and_Deep_Learning_Methods_for_Cybersecurity).
3. Heinrich, Kai & Graf, Johannes & Chen, Ji & Laurisch, Jakob & Zschech, Patrick. Fool me Once, Shame on you, Fool me Twice, Shame on me: A Taxonomy of Attack and Defense Patterns for AI Security. 2020. URL: [https://www.researchgate.net/publication/341180631\\_Fool\\_me\\_Once\\_Shame\\_on\\_you\\_Fool\\_me\\_Twice\\_Shame\\_on\\_me\\_A\\_Taxonomy\\_of\\_Attack\\_and\\_Defense\\_Patterns\\_for\\_AI\\_Security](https://www.researchgate.net/publication/341180631_Fool_me_Once_Shame_on_you_Fool_me_Twice_Shame_on_me_A_Taxonomy_of_Attack_and_Defense_Patterns_for_AI_Security).
4. NIST AI 100-2e2023 ipd. Adversarial Machine Learning. A Taxonomy and Terminology of Attacks and Mitigations. URL: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf>.
5. Kianpour, Mazaher & Wen, Shao-Fang. Timing Attacks on Machine Learning: State of the Art. 2020. URL: [https://www.researchgate.net/publication/335382520\\_Timing\\_Attacks\\_on\\_Machine\\_Learning\\_State\\_of\\_the\\_Art](https://www.researchgate.net/publication/335382520_Timing_Attacks_on_Machine_Learning_State_of_the_Art).
6. P. I. Radoglou-Grammatikis and P. G. Sarigiannidis. An Anomaly-Based Intrusion Detection System for the Smart Grid Based on CART Decision Tree // 2018 Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, 2018. P. 1–5. DOI: 10.1109/GIIS.2018.8635743.
7. Moorthy R. S., Pabitha P. Optimal detection of phishing attack using SCA based K-NN // Procedia Computer Science. 2020. Vol. 171. P. 1716–1725.
8. S.-Y. Lee, S.-r. Wi, E. Seo, J.-K. Jung and T.-M. Chung. ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach // 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 2017. P. 1–6. DOI: 10.1109/ATNAC.2017.8215434.
9. Swarnkar M., Hubballi N. OCPAD: One class Naive Bayes classifier for payload based anomaly detection // Expert Syst. Appl. Oct. 2016. Vol. 64. P. 330–339.
10. R. Bapat et al. Identifying malicious botnet traffic using logistic regression // Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2018. P. 266–271. DOI: 10.1109/SIEDS.2018.8374749.
11. Katja Auernhammer, Ramin Tavakoli Kolagari, and Markus Zoppelt. Attacks on Machine Learning: Lurking Danger for Accountability. AAAI 2019. URL: [https://www.researchgate.net/publication/330737530\\_Attacks\\_on\\_Machine\\_Learning\\_Lurking\\_Danger\\_for\\_Accountability](https://www.researchgate.net/publication/330737530_Attacks_on_Machine_Learning_Lurking_Danger_for_Accountability).
12. S. Herpig. Securing artificial intelligence – Part 1: The attack surface of machine learning and its implications. Think Tank at the Intersection of Technology and Society, Stiftung Neue Verantwortung, Berlin, Oct. 2019. [Online]. URL: [https://www.stiftung-nv.de/sites/default/files/securing\\_artificial\\_intelligence.pdf](https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf).
13. ATLAS Matrix. URL: <https://atlas.mitre.org/matrices/ATLAS/>.
14. Adversarial Machine Learning. URL: <https://atlas.mitre.org/resources/adversarial-ml-101/>.

15. Goodfellow, Ian & Shlens, Jonathon & Szegedy, Christian. (2014). Explaining and Harnessing Adversarial Examples. arXiv 1412.6572. URL: [https://www.researchgate.net/publication/269935591\\_Explaining\\_and\\_Harnessing\\_Adversarial\\_Examples](https://www.researchgate.net/publication/269935591_Explaining_and_Harnessing_Adversarial_Examples).
16. Peter Lee. Learning from Tay's introduction // Microsoft. 2016. URL: <https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/>.
17. Le, Hung & Pham, Quang & Sahoo, Doyen & Hoi, Steven. URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection (2018). URL: [https://www.researchgate.net/publication/323118482\\_URLNet\\_Learning\\_a\\_URL\\_Representation\\_with\\_Deep\\_Learning\\_for\\_Malicious\\_URL\\_Detection](https://www.researchgate.net/publication/323118482_URLNet_Learning_a_URL_Representation_with_Deep_Learning_for_Malicious_URL_Detection).
18. Evasion of Deep Learning Detector for Malware C&C Traffic. Actor: Palo Alto Networks AI Research Team. Incident Date: 2020.
19. Botnet Domain Generation Algorithm (DGA) Detection Evasion. Actor: Palo Alto Networks AI Research Team. Incident Date: 2020. URL: <https://atlas.mitre.org/studies/AML.CS0001>.
20. B. Yu, J. Pan, J. Hu, A. Nascimento and M. De Cock. Character Level based Detection of DGA Domain Names, 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 2018, pp. 1–8. URL: <https://ieeexplore.ieee.org/document/8489147>.
21. VirusTotal Poisoning. Incident Date: 2020. URL: <https://atlas.mitre.org/studies/AML.CS0002>.
22. Metame: metamorphic code engine for arbitrary executables. URL: <https://github.com/a0rtega/metame>.
23. Bypassing Cylance's AI Malware Detection. Actor: Skylight Cyber. 2019. URL: <https://skylightcyber.com/2019/07/18/cylance-i-kill-you/>.
24. CVE-2019-20634 Detail. National Vulnerability Database. 2022. URL: <https://nvd.nist.gov/vuln/detail/CVE-2019-20634>.

УДК 621.007.5

канд. техн. наук Штаненко С. С. ORCID: 0000-0001-9776-4653 (ВІТІ ім. Героїв Крут)  
д-р техн. наук Самохвалов Ю. Я. ORCID: 0000-0001-5123-1288 (КНУ ім. Тараса Шевченка)  
д-р техн. наук Толюпа С. В. ORCID: 0000-0002-1919-9174 (КНУ ім. Тараса Шевченка)

## ПІДХІД ДО ВИЗНАЧЕННЯ ТЕХНІЧНОГО СТАНУ МІКРОПРОЦЕСОРНИХ СИСТЕМ, РЕАЛІЗОВАНИХ НА ПРОГРАМНО-РЕКОНФІГУРОВАНІЙ ЛОГІЦІ

У статті запропоновано підхід до визначення технічного стану мікропроцесорних систем, реалізованих на програмованих логічних інтегральних схемах. Проведено аналіз існуючих методів та способів визначення технічного стану мікропроцесорних систем, реалізованих на одній або декількох великих/надвеликих інтегральних схемах (далі – ВІС/НВІС) з жорсткою внутрішньою архітектурою, наведено недоліки та переваги. З метою підвищення ефективності визначення технічного стану мікропроцесорних систем, реалізованих на програмно-реконфігурованій логіці, у статті запропоновано інтелектуалізувати процедуру контролю, виявлення та локалізації несправностей шляхом застосування нейронної мережі, реалізуючи при цьому концепцію створення нейромережевої системи розпізнавання технічного стану. Значимо, що задача визначення технічного стану складних технічних систем, якими є мікропроцесорні системи, за багатьма критеріями збігається із задачею розпізнавання образів, тому, використовуючи нейронну мережу, можна досягти більш високих результатів у процесі діагностування несправностей мікропроцесорних систем порівняно з класичними системами діагностування. Передбачається, що запропонована діагностична система з елементами штучного інтелекту буде безпосередньо вбудована в мікропроцесорну систему, реалізуючи при цьому концепцію вбудованих систем контролю та діагностування. Реалізація запропонованого підходу завдяки застосуванню інтелектуальних систем дозволить значно підвищити достовірність визначення технічного стану мікропроцесорних систем і, як наслідок, може стати основою під час проєктування високонадійних, живучих, резильєнтних, кіберстійких складних технічних систем.

**Ключові слова:** мікропроцесорна система, програмно-реконфігурована логіка, технічний стан, інтелектуальна система, нейронна мережа.

**S. Shtanenko, Y. Samokhvalov, S. Toliupa. Approach to determining the technical state of microprocessor systems implemented on software-reconfiguration logic.**

The article proposes an approach to determining the technical state of microprocessor systems implemented on programmable logic device (PLD). An analysis of the existing methods and ways of determining the technical condition of microprocessor systems implemented on one or more large/very large integrated circuits (LSI/VLSI) with a rigid internal architecture is carried out, the disadvantages and advantages are given. In order to improve the efficiency of determining the technical state of microprocessor systems implemented on software-reconfigurable logic, the article proposes to intellectualize the procedure of control, detection and localization of faults by using a neural network, while implementing the concept of creating a neural network system for recognizing the technical state. Note that the task of determining the technical condition of complex technical systems, which are microprocessor systems, coincides with the passing of pattern recognition according to many criteria, therefore, using a neural network, it is possible to achieve higher results in diagnosing malfunctions of microprocessor systems compared to classical diagnostic systems. It is assumed that the proposed diagnostic system with elements of artificial intelligence will be directly embedded in the microprocessor system, while implementing the concept of embedded control and diagnostic systems. The implementation of the proposed approach thanks to the application of intelligent systems will allow to significantly increase the reliability of determining the technical state of microprocessor systems and, as a result, can become the basis for the design of highly reliable, durable, resilient, cyber-resistant complex technical systems.

**Keywords:** microprocessor system, software-reconfigurable logic, technical condition, intelligent system, neural network.



**Постановка завдання.** Сучасні мікропроцесорні системи ґрунтовно увійшли в наше повсякденне життя, пройшовши шлях від обчислювальних пристроїв на інтегральних схемах з малим та середнім ступенем інтеграції, а також універсальних та управляючих електронно-обчислювальних машин, побудованих на функціональних елементах (логічні, запам'ятовуючі, індикаційні тощо), до багатопроцесорних систем із *CISC*, *RISC*, *MISC* архітектурами, реалізуючи при цьому концепцію «Система на кристалі» [1].

На сьогодні мікропроцесорні системи широко використовуються в різних галузях діяльності, таких як: машинобудування та верстатобудування, авіація, автомобілебудування, атомна енергетика, банківська сфера, військово-промисловий комплекс. Крім цього, широке застосування мікропроцесорні системи знайшли в якості основи побудови автоматичних, автоматизованих систем різного призначення, а також в якості системи управління технологічними процесами.

Слід зазначити, що сучасні мікропроцесорні системи характеризуються великою різноманітністю функціональних можливостей, ступенем складності та специфікою технологій, що застосовуються для їхньої розробки та виготовлення. Крім цього, кожна зі складових мікропроцесорної системи (апаратна або програмна частина) має свої особливості та характерні властивості, які обумовлюють існування досить специфічних різновидів несправностей її стану загалом. Так, наведені специфічні особливості мікропроцесорних систем, а також поява сучасної елементної бази у вигляді програмно-реконфігурованих інтегральних схем викликали значні зміни, як у процесі створення мікропроцесорних систем, так і в процесі розробки методів та засобів контролю й діагностування з метою виявлення та локалізації несправностей, пов'язаних як з хіміко-фізичними процесами елементної бази, так і з навмисними та ненавмисними несприятливими впливами. **Отже, актуальним науковим завданням** є створення сучасної системи технічного діагностування мікропроцесорних систем, здатної оцінювати та прогнозувати технічний стан, а також виявляти та локалізувати несправності, виходячи з того, що мікропроцесорні системи реалізовані відповідно до концепції «Система на кристалі», а в якості елементної бази використовується програмно-реконфігурована логіка.

**Аналіз останніх публікацій.** На сьогодні питанням технічного діагностування складних технічних систем, якими є мікропроцесорні системи, присвячено велику кількість наукових праць. Так, у роботі [2] проведено досить повний аналіз існуючих видів контролю, як універсальних, так і спеціалізованих обчислювальних систем, застосування яких дозволить виявляти несправності мікропроцесорних систем. У роботі [3] представлено методи тестового та функціонального діагностування цифрових пристроїв, які є основою мікропроцесорної системи, при цьому застосування цих методів дозволить оперативно локалізувати несправності. У роботі [4] запропоновано перспективний безконтактний, індукційний метод діагностування радіоелементів технічно-складних радіоелектронних блоків, що дозволяє розпізнавати як технічний стан контрольованого об'єкта, так і виявляти радіоелектронний компонент, який спровокував його несправність. Робота [5] розглядає підходи щодо прогнозування технічного стану, які ґрунтуються на теорії дефектоутворення та стохастичних процесах зміни струму в напівпровідникових структурах залежно від часу напрацювання радіоелектронного обладнання. В роботах [6; 7] розглянуто можливість застосування штучних нейронних мереж щодо вирішення задач технічної діагностики складних технічних систем, а саме: визначення та прогнозування технічного стану електромеханічних систем, а також виявлення і локалізації несправностей в стабілізаторах напруги змінного струму. Робота [8] присвячена застосуванню нейронної мережі в сукупності з експертною системою в медичній сфері для діагностування хвороб, моніторингу стану пацієнтів, прогнозування результатів лікування, а також підтримки прийняття рішення щодо діагностування та лікування хворих.

Проте, проведений аналіз свідчить, що традиційні методи визначення технічного стану мікропроцесорних систем орієнтовані, як правило, на конкретну архітектуру мікропроцесорної системи, що не завжди є прийнятним для використання щодо інших типів архітектур. Також має місце оцінка технічного стану не самої мікропроцесорної системи, а її складових (процесора, модулів пам'яті, модулів введення/виведення даних, периферійного обладнання), які являють собою окремі інтегральні мікросхеми, на відміну від програмованих логічних інтегральних схем (далі – ПЛІС), на яких можлива реалізація концепції «Система на кристалі». До відома, «Система на кристалі» являє собою обчислювальну систему, архітектура якої розробляється цільовим чином для вирішення прикладної задачі (або класу задач) і реалізується у вигляді комплексу функціонально спеціалізованих апаратних і програмних компонент на базі мікроелектронної реконфігурованої платформи [9]. Крім цього, якщо розглядати нейронні мережі як сучасні системи технічного діагностування, то, як правило, вони орієнтовані на сферу медичної діагностики. Якщо розглядати з точки зору технічного діагностування складних технічних систем, то останні мають сталий стан, на відміну від мікропроцесорних систем, реалізованих в базисі ПЛІС, які мають властивість реконфігурації внутрішньої алгоритмічної структури внаслідок несприятливих впливів. Так, згідно з [10] властивість реконфігурації алгоритмічної структури безумовно підвищує надійність, живучість, резильєнтність та кіберстійкість складної технічної системи в процесі функціонування, але при цьому висуває питання щодо розробки та застосування методів технічного діагностування систем, які перебувають у динамічному стані та реалізовані на програмно-реконфігурованій логіці.

Враховуючи вказане, **метою статті** є підхід до визначення технічного стану мікропроцесорних систем, реалізованих в базисі ПЛІС, в основі якого лежить нейромережева технологія, яка реалізує концепцію вбудованих систем контролю та діагностування і здатна адаптуватися до зміни алгоритмічної структури мікропроцесорної системи внаслідок несприятливих впливів.

**Задача визначення технічного стану та шляхи її вирішення.** Визначення технічного стану мікропроцесорних систем нині проводиться системами контролю та діагностування (далі – СКД). При цьому під контролем розуміється процес отримання інформації, що дозволяє визначити технічний стан мікропроцесорної системи шляхом застосування апаратних, програмних і комбінованих методів й засобів контролю, а також відповідність отриманої інформації вимогам, що висуваються до системи [11].

Діагностування, зі свого боку, є сукупністю задач перевірки правильного функціонування мікропроцесорної системи, а також задач пошуку та локалізації несправностей, що порушують правильне функціонування [12]. У більшості випадків всі ці задачі вирішуються вбудованими системами контролю та діагностування (далі – ВСКД) мікропроцесорних систем, а також системами діагностування сервісних центрів.

Слід зауважити, що існуючі СКД розробляються на стохастичних та детермінованих принципах. Стохастичні СКД будуються на основі ймовірнісних моделей об'єктів контролю та випадкових стимулюючих впливів. Детерміновані СКД засновані на детермінованих моделях об'єктів контролю та регулярних методах побудови стимулюючих впливів у інтегрованому середовищі систем автоматизованого проектування (далі – САПР). Враховуючи, що детерміновані СКД вимагають значних обчислювальних ресурсів, найбільш перспективними є СКД, побудовані на стохастичних принципах.

Зазначимо, що визначення технічного стану мікропроцесорних систем стохастичними методами виконується як у процесі їхнього функціонування, так і в перервах між роботою [13]. Так, на першому етапі в якості систем контролю і пошуку несправності, як правило, використовуються ВСКД. На наступних етапах з метою локалізації несправності можуть використовуватися як ВСКД, так і спеціалізовані діагностичні засоби вбудованого та



зовнішнього виконання. При цьому вирішується задача пошуку та локалізації несправностей. Зазначимо, що для діагностичних засобів необхідно також забезпечити збирання та обробку діагностичної інформації, пошук несправності при цьому здійснюється перевіркою ознаки наявності несправності. Так, для мікропроцесорних систем ознаками наявності несправності є відхилення діагностичних параметрів від номіналу, вихід характеристик за допустимі межі, відсутність логічних сигналів перемикавання тощо. Загалом наявність несправності визначається перевіркою виконання умов:

$$x_i = \begin{cases} 1 & \text{при } y_i > y_{i0} \\ 0 & \text{при } y_i < y_{i0}; \end{cases} \quad \bar{x}_i = \begin{cases} 1 & \text{при } y_i < y_{i0}; \\ 0 & \text{при } y_i > y_{i0}; \end{cases}$$

де  $x_i$ ,  $\bar{x}_i$  – ознаки  $i$ -несправності;  $y_i$ ,  $y_{i0}$  – поточне та еталонне значення діагностичного параметру.

Діагностична інформація про технічний стан мікропроцесорної системи визначається у контрольних точках у вигляді значень діагностичних параметрів, тобто у вигляді векторів діагностичних ознак у просторі технічного стану мікропроцесорної системи. Наприклад, для мікропроцесорних систем діагностичними параметрами є: параметри на постійному струмі, динамічні параметри, а також функціональна поведінка [14]. При цьому задача визначення технічного стану полягає у розпізнаванні двох станів: правильного ( $A_1$ ) та неправильного функціонування об'єкту контролю ( $A_2$ ). Ситуація  $A_2$  є об'єднанням великої кількості ймовірнісних подій (несправностей):

$$A_2 = \bigcup_{\mu=1}^N A_{\mu},$$

де  $|N|$  – потужність простору технічного стану мікропроцесорної системи.

Враховуючи вищесказане, визначення технічного стану можна представити як задачу розпізнавання образів – прийняття рішення про належність поточної ситуації із заданим вектором діагностичних ознак до того чи іншого класу діагнозів  $A_{\mu}$ ,  $\mu = 1, N$ . При цьому пошук рішень у просторі станів ґрунтується на перевірці статистичних гіпотез та математично формулюється наступним чином.

За вектором діагностичних ознак  $X = \{x_1, \dots, x_n\}$ , де  $x_i$  – значення  $i$ -ї ознаки, необхідно знайти максимальне значення функції, що вирішується  $A_k : H_k$ , яка відноситься до класу  $A_{\mu}$ , якщо вектор діагностичних ознак  $X$  належить до класу  $A_{\mu}$ ,

$$\exists_{\max}(A_{\mu} : H_k) \supseteq (X \in A_{\mu}).$$

За такого підходу основна мета діагностування полягатиме у визначенні класу діагнозу, до якого належить ситуація  $A$ . Так, під час розпізнавання мають справу з ситуаціями  $A_{\mu}$ , поділеними на множини (несправності) та відповідні множини технічних станів (множини несправностей або їх відсутності). При цьому вирішення задачі розпізнавання, тобто визначення технічного стану, зводиться до знаходження значень вирішальної функції, на основі якої вибирається гіпотеза про віднесення ситуації до того чи іншого класу технічних станів.

Отже, під діагностуванням розуміється вирішення задачі перевірки (контролю) правильного функціонування мікропроцесорної системи, а також задачі пошуку (виявлення) та локалізації несправностей, що порушують правильне функціонування. За такої постановки задача діагностування передбачає, по-перше, задання простору можливих технічних станів (найбільш ймовірна несправність) і, по-друге, наявність формалізованих методів побудови

засобів діагностування, реалізація яких забезпечить виявлення (розпізнавання) несправностей із заданого простору з необхідною достовірністю правильного діагностування.

**Розпізнавання технічного стану мікропроцесорних систем на основі нейронної мережі.** Так, останнім часом, згідно з [15; 16] набирає популярності принципово новий підхід до побудови систем розпізнавання, які визначають технічний стан складних технічних систем, що функціонують в умовах неповної, нечіткої та суперечливої інформації, і полягає цей підхід у застосуванні інтелектуальних систем. На відміну від експертних систем та систем підтримки прийняття рішень, в яких використовується досвід (інтелект) фахівців (експертів), інтелектуальні системи мають здатність до навчання та самонавчання (використовуючи власні знання та досвід). Зазначимо, що до категорії інтелектуальних систем належать нейронні мережі, основна ідея яких полягає у наслідуванні дії біологічних нейронів, з метою створення комп'ютерної системи, здатної обробляти інформацію так, як обробляє мозок людини. Нейронна мережа являє собою сукупність вузлів (нейронів), які організовані у велику кількість взаємодіючих шарів з метою обробки вхідних даних, виділення патернів та генерації вихідних результатів. Кожен нейрон отримує вхідні сигнали, обчислює їхню вагу та застосовує певну активаційну функцію для генерації вихідного сигналу. Цей процес розгортання взаємодії між нейронами повторюється через всі шари мережі, що дозволяє нейронній мережі вирішувати задачі розпізнавання, класифікації, передбачення та інші задачі у сфері штучного інтелекту.

Так, на рисунку 1 зображено модель розпізнавання технічного стану об'єкта діагностування, яку можна представити у вигляді сукупності підсистем.

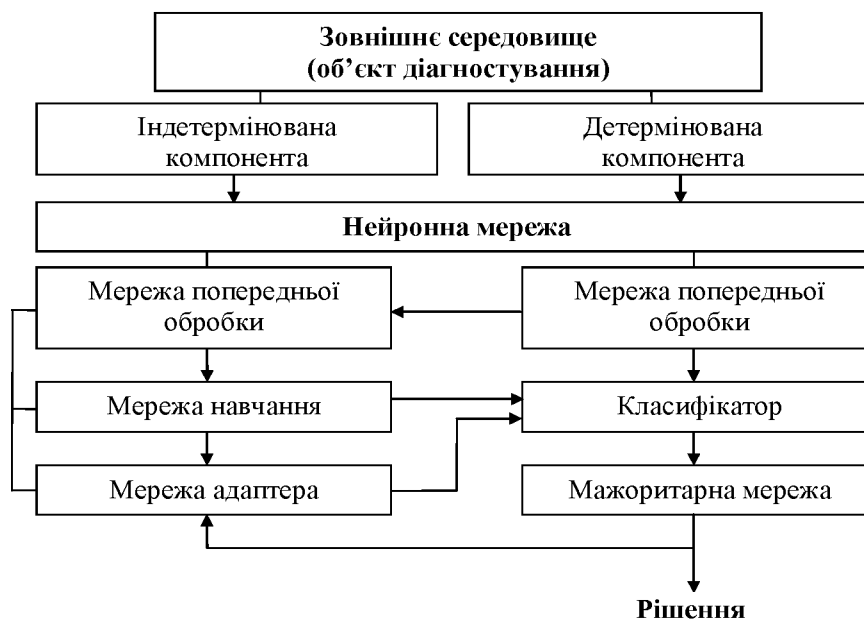


Рис. 1. Узагальнена модель розпізнавання технічного стану

Розв'язання задачі розпізнавання у загальному вигляді дозволяє визначити шляхи та методи вирішення задачі підвищення ефективності діагностичної системи визначення технічного стану [17]. Розглянемо задачу більш детально. Нехай  $\epsilon$  множина об'єктів діагностування  $W = \{\omega_i\}$ ,  $i = 1, \dots, \rho$ , яка розбивається на кінцеве число підмножин, які

являють собою технічні діагнози (класи)  $L = \{A_\mu\}$ ,  $\mu = 1, \dots, M$ . Сукупність  $L = \bigcup_{\mu=1}^M A_\mu$

називається простором технічних станів, як правило, визначена не в повному обсязі, задана

лише деяка апріорна інформація  $J(M)$  про неї, тобто кількість діагнозів  $M$  – невідома. Об'єкти діагностування  $W_i \in$  сукупністю значень деяких вимірювань, що становлять діагностичний портрет об'єкта розпізнавання. Сукупність  $N$  значень ознак, що визначають словник діагностичних ознак  $X = \{x_j\}$ ,  $j=1, \dots, N$ , за якими власне проводиться розпізнавання, може бути знайдена за допомогою перетворення (попередньої обробки)  $J(\omega_i)$ , тобто  $x_j = J(\omega_i) \omega_i$ . Вимірювання (спостереження) об'єктів діагностування  $W_i$  пов'язані зі значними дестабілізуючими факторами (несприятливими впливами), а отже, ознаки об'єктів діагностування, що розпізнаються, та їхні портрети будуть ймовірнісними, що може бути враховано функцією щільності ймовірності (ФЩІ)  $f(x)$  – сумішшю розподілів ознак за всіма класами:

$$f(x) = \sum_{\mu=1}^M f(A_\mu) f(x/A_\mu),$$

де  $f(A_\mu)$  – ФЩІ появи  $\mu$ -го класу;  $f(x/A_\mu)$  – ФЩІ умовних ймовірностей ознак  $x_i$  при появі  $\mu$ -го класу.

Зазначимо, що просторово-часові зміни параметрів об'єкта діагностування  $\omega_i$  вимагають враховувати динаміку зміни  $f(x)$  як часового процесу, що відображає динамічність діагностичного об'єкту. Крім цього, у процесі навчання сукупність випадкових відображень об'єктів  $\Pi(x)$  об'єкта діагностування трансформуються на так званий ймовірнісний діагностичний портрет об'єкта  $\Pi(x)$ :

$$\Pi(x) = Y_{\text{навч.}}(x)x,$$

де  $Y_{\text{навч.}}$  – оператор підсистеми навчання в системі розпізнавання, що визначає її цільове та функціональне призначення. При цьому ймовірнісний діагностичний портрет виконує роль узагальненого ймовірнісного еталону, що формується в процесі навчання та використовується у процесі розв'язання задачі визначення технічного стану [18].

Отже, задача діагностичного розпізнавання полягає в тому, щоб для даного об'єкта діагностування  $W_i$ , алфавіту технічних діагнозів  $L = \{A_\mu\}$ ,  $\mu=1, \dots, M$  (або апріорної інформації  $J(M)$ ) та словника діагностичних ознак  $X = \{x_j\}$ ,  $j=1, \dots, N$  на підставі отриманого опису  $X_j$  та його ймовірнісного портрета  $\Pi(x)$  прийняти рішення про відповідність об'єкта діагностування  $\omega_i$  до одного з діагнозів  $A_\mu$ , тобто

$$H(W_i/A_\mu) \rightarrow W_i \in A_\mu, \mu=1, \dots, M.$$

Можливість динамічної зміни структури об'єкта діагностування, тобто  $\omega_i(t) \in W(t) \rightarrow \text{var}$ , призводить до невідповідності значень  $\omega_i$  та  $A_\mu$ , у чому проявляється суперечливість інформації під час розпізнавання. При цьому приймається твердження, що система розпізнавання і об'єкт діагностування розглядаються як єдина антропогенна система. Цим обумовлюється адекватність властивостей системи розпізнавання, які відображають взаємні зв'язки елементів її структури.

З точки зору системного аналізу, ефективність системи розпізнавання залежить від параметрів (діагностичних ознак) об'єкта діагностування  $X = \{x_j\}$ ,  $j=1, \dots, N$  і параметрів структури самої системи  $S = \{S_k\}$ ,  $k=1, \dots, d$ , причому параметри структури системи розпізнавання характеризуються як елементами структури, так і зв'язками між ними.

Відповідно, ефективність системи розпізнавання у загальному вигляді оцінюється функціоналом

$$E = E[\{x_j\}_{j=1, \dots, N}; \{S_k\}, k=1, \dots, d],$$

і вирішення задачі підвищення ефективності зводиться до пошуку його екстремуму при обмеженнях на витрати, які пов'язані з отриманням алфавіту діагнозів  $L$ , вимірюванням та обробкою словника діагностичних ознак  $X$  математичного забезпечення функціонування та апаратною реалізацією системи розпізнавання ( $r_0$ ), тобто:

$$E_{\max} = \max_{\substack{x, s \\ j, k}} E[\{x_j\}_{j=1, \dots, N}; \{S_k\}, k=1, \dots, d]$$

при забезпеченні  $C_{r_0} \leq C_{r_{\text{опн}}}$ .

При цьому кожен елемент діагностичної системи розпізнавання можна представити послідовністю дій з відомими зв'язками між входом і виходом. На рисунку 2 представлено узагальнену модель системи розпізнавання у вигляді сукупності функціональних підсистем, кожній з яких відповідає деякий детермінований або стохастичний оператор.

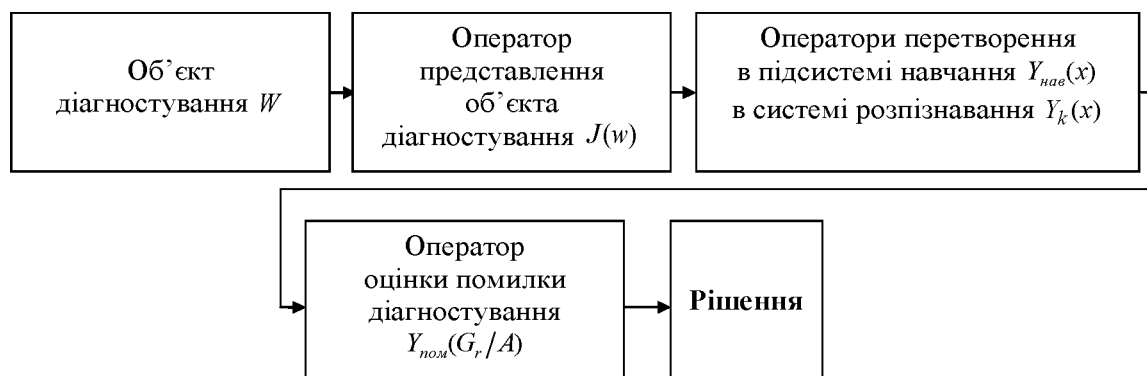


Рис. 2. Узагальнена модель розпізнавання стану у вигляді сукупності підсистем

Так, для побудови систем розпізнавання в [19] запропоновано дискретно-подійний підхід, в основі якого лежить нейронна мережа, яка є частиною об'єкта діагностування і базується на законі адекватності структури нейронної мережі об'єкту діагностування. При цьому синергізм об'єкта діагностування та нейронної мережі може бути представлений у вигляді сукупності технічних станів, що підлягають розпізнаванню, а також впливів, що заважають правильному функціонуванню. Крім цього, фазова траєкторія динамічної системи, яка реалізує дискретно-подійний підхід (далі дискретно-подійна система), є кусково-постійною і формується подіями у вигляді послідовності відрізків, які відображають послідовність станів системи, а тривалість кожного відрізка – час перебування у відповідному стані.

Дискретно-подійні системи (далі – ДПС) можуть бути представлені тільки стохастичними у вигляді логічних, алгебраїчних чи орієнтованих на функціонування моделей. Математичний апарат для опису стохастичних моделей, орієнтованих на функціонування ДПС, обраний на основі ланцюга Маркова. Таке математичне представлення дозволяє описати функціонування ДПС в якості елемента об'єкта діагностування і оптимально відобразити його на структуру детермінованої частини нейронної мережі. При цьому число станів ДПС визначає точність кусково-постійної апроксимації неперервної фазової траєкторії динамічного об'єкта. Зазначимо, що підвищення точності кусково-постійної апроксимації фазової траєкторії безперервної системи вимагає введення простору технічних станів  $A$  великої розмірності, що ускладнює аналітичний опис. Виходом із ситуації є можливість збільшення

(склеювання) станів, тобто перехід від простору конфігурацій  $\Omega = A^T$  до простору станів  $\Omega_B = B^T$ . При цьому нові макростани можуть бути отримані шляхом об'єднання попередніх станів таким чином:

$$B_k = \sum_{j \in \{K\}} A_j; k=1, \dots, p; j=1, \dots, r; p < r,$$

де  $\{K\}$  – множина індексів станів системи  $\{A_j\}$ , об'єднаних у  $B_k$ .

Об'єкт діагностування для системи розпізнавання технічного стану на основі нейронної мережі може бути представлено у вигляді сукупності ДПС, що підлягають розпізнаванню, зі зв'язаними дискретними технічними станами.

Узагальнена модель системи розпізнавання технічного стану на основі нейронної мережі має структуру (рис. 3), яка містить: сенсорну матрицю, що сприймає ланцюг Маркова у вигляді сукупності спостережень; сукупність нейронних ансамблів (класифікаторів), визначається числом кластерів  $M$ ; нейронне поле, що враховує апріорну інформацію у вигляді ймовірностей гіпотез  $P$ ; нейронне поле, що враховує значення елементів платіжної матриці  $C$ ; мажоритарну мережу, що приймає рішення  $G$  про розпізнавання технічного стану; мережу навчання.

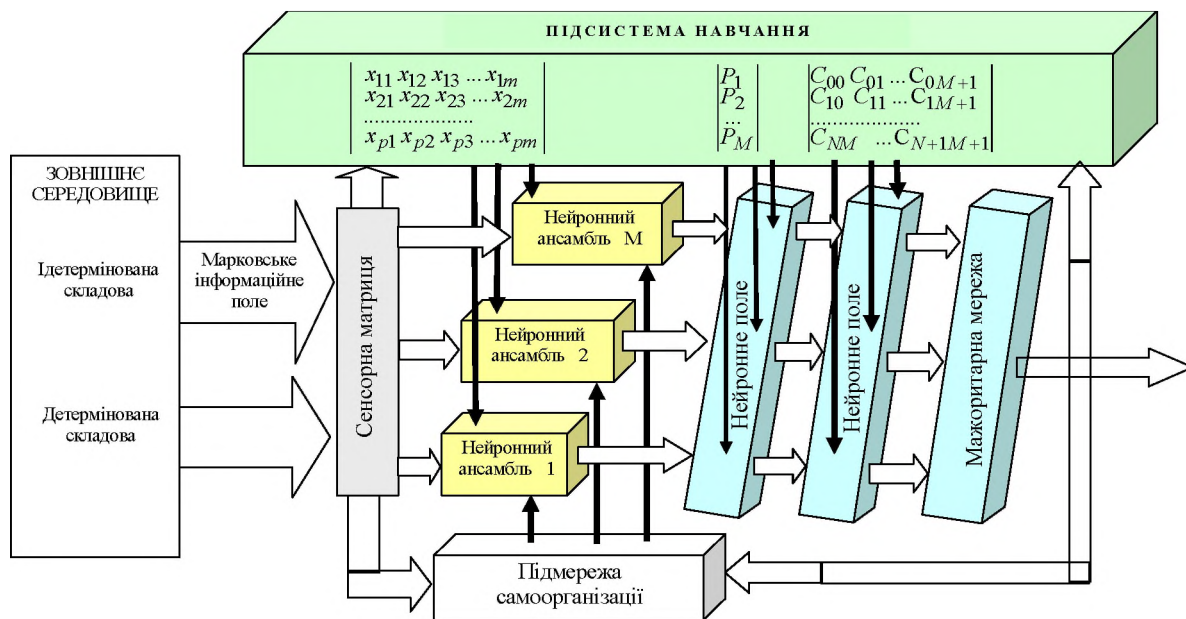


Рис. 3. Узагальнена модель системи розпізнавання технічного стану на основі нейронної мережі

Так, маючи множину вимірювань діагностичних ознак об'єкта діагностування, необхідно розробити таку процедуру обробки вимірювань, що дозволяє автоматично отримувати інформацію про технічний стан всіх його елементів.

Діагностичні ознаки сприймаються сенсорною матрицею у вигляді сукупності спостережень:  $X = (X_1, X_2, \dots, X_m)$ ,  $i=1, 2, \dots, n$ , де  $X_i = (X_{li}, X_{2i}, \dots, X_{ij}, \dots, X_{pi})$ . В окремому сенсорному каналі відбувається редукція вибіркового простору  $X$ , у результаті якої маємо послідовність дискретних змінних  $U_k, k=1, 2, \dots, n-1$ , які приймають значення  $Z_1, Z_2, \dots, Z_r$ . Далі необхідно синтезувати структуру нейроподібного класифікатора, що реалізує вирішальну функцію  $\gamma(U)$  на редукованому вибіркового просторі  $U$ .

При цьому послідовність дискретних змінних  $U_k, k=1, 2, \dots, n-1$ , які приймають значення  $z_a, a=1, 2, \dots, r$ , можна апроксимувати векторами  $\Xi, \Phi(0)_\mu$  та  $\Xi, \Phi(k)_\mu$ , де  $\Xi$  – деяка гранична функція.

Використовуючи векторні позначення, можна записати:

$$\ln l_\mu = (\Xi, \Phi(0)_\mu) + (\Xi, \Phi(k)_\mu) = |\Xi| |\Phi(0)_\mu| \cos(\Xi \wedge \Phi(0)_\mu) + |\Xi| |\Phi(k)_\mu| \cos(\Xi \wedge \Phi(k)_\mu)$$

де  $|\Xi|, |\Phi(0)_\mu|, |\Phi(k)_\mu|$  – модулі векторів  $\Xi, \Phi(0)_\mu, \Phi(k)_\mu$ ;  $\Xi \wedge \Phi(0)_\mu, \Xi \wedge \Phi(k)_\mu$  – кути між цими векторами.

Зазначений вище вираз цілком визначає оптимальну структуру класифікатора при фіксованих  $j$  та  $i$ . Він дозволяє виконати інтерпретацію функціонування синтезованої структури наступним чином.

На вхід кожного шару, який складається з  $n$ -нейронів, надходить один і той самий вектор збудження. При цьому шари розрізняються ефективністю своїх зв'язків.

Якщо довжини векторів для всіх шарів однакові, то величина збудження шару при незмінному  $\Xi$  буде залежати тільки від кутів між  $\Xi \wedge \Phi(0)_\mu$  та  $\Xi \wedge \Phi(k)_\mu$ . Це свідчить, що максимально збуджується той шар, вектори  $\Phi(0)_\mu$  та  $\Phi(k)_\mu$  якого колінеарні вектору  $\Xi$ . При цьому рішення приймається за номером максимально збудженого шару.

Структура найпростішої системи розпізнавання технічного стану на основі нейронної мережі являє собою набір  $M+1$  шарів, які формують  $M+1$  вихідних сигналів. При цьому шар складається з  $n$ -нейронів, рівень збудження яких визначається як

$$Y_\mu(k) = \sum_{\alpha=1}^n \Xi_\alpha(k) \Phi_\alpha(k)_\mu.$$

Зазначимо, що кожен нейрон здійснює кодування методом мічених ліній, при якому певним значенням процесу надаються відповідні визначені (мічені) лінії  $Z_1, Z_2, \dots, Z_a, \dots, Z_k$  і, відповідно, певному значенню параметра процесу відповідає один максимально збуджений синоптичний зв'язок  $\Xi_\alpha(k) = 1$ . На відміну від типового нейрона, синоптичні зв'язки якого рівнозначні, у нейрона, що здійснює кодування методом мічених ліній, синоптичні зв'язки мають пріоритет. Синоптичному входу з більшим  $\alpha$  номером відповідає більше значення інформативного параметра процесу. Крім цього, ще одна відмінність полягає у тому, що в  $k$ -й момент часу збуджується тільки один синоптичний зв'язок і, тим самим, значно спрощується задача введення і управління граничними значеннями  $\Xi$  за допомогою вагової функції  $W$ . Дійсно

$$Y_\mu(k) = \sum_{\alpha=1}^r \Xi_\alpha(k) \Phi_\alpha(k)_\mu - \Xi_\alpha(k)_\mu = \sum_{\alpha=1}^r \Xi_\alpha(k) \Phi_\alpha(k)_\mu. \quad (1)$$

При  $\Xi_\alpha(k)_\mu = 0$  структура системи розпізнавання є квазілінійною, а при  $\Xi_\alpha(k)_\mu > 0$  вона має нелінійні граничні властивості.

Зазначимо, що другий шар нейронів реалізує операцію

$$\ln l_\mu(k) = \sum_{k=0}^n Y_k(k). \quad (2)$$

При цьому він з'єднаний з першим шаром проєкційними зв'язками, які встановлюють однозначну відповідність між нейронами різних полів, тобто передають збудження з одного шару в інший. У свою чергу, вхідною інформацією для третього шару нейронів є вектор  $\ln L(U) = (\ln l_0(U), \ln l_1(U), \dots, \ln l_m(U))$ , який виконує роль мажоритарного логічного

пристрою. При цьому вирази (1) і (2) цілком визначають структуру системи розпізнавання технічного стану.

Далі введемо матрицю зв'язків  $k$ -ї групи сенсорів із  $k$ -м нейроном, склавши її з індикаторів збудження:

$$\Xi = \begin{Bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_k \end{Bmatrix}.$$

Крім цього введемо також поняття коефіцієнта міжнейронного зв'язку  $S$  у шарі:

$$S_{kl} = \begin{cases} 1, & \text{якщо є зв'язок між } k\text{-ю групою нейронів і } l\text{-м нейроном;} \\ 0, & \text{в іншому випадку.} \end{cases}$$

Утворимо матрицю міжнейронних зв'язків, яка складається з коефіцієнтів міжнейронних зв'язків:

$$S = \begin{Bmatrix} S_{00} & S_{01} & \cdots & S_{0n-1} \\ S_{10} & S_{11} & \cdots & S_{1n-1} \\ \cdots & \cdots & \cdots & \cdots \\ S_{n-1} & S_{nn} & \cdots & S_{n-1n-1} \end{Bmatrix}.$$

Матриці  $\Xi(k)$  та  $S$  цілком визначають структуру зв'язків в шарі. Для випадку  $Y=0$  матриця  $S$  вироджується в діагональну з розмірністю  $n \times n$ . При цьому синтезовані структури передбачають фіксований об'єм вибірки, тобто система розпізнавання технічного стану спостерігає відразу всю фазову траєкторію. В свою чергу, інформаційне поле сприймається сенсорною матрицею у вигляді сукупності спостережень:

$$X = \begin{Bmatrix} x_{11} & x_{12} & \cdots & x_{1i} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2i} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots & \vdots & \cdots \\ x_{p1} & x_{p2} & \cdots & x_{pi} & \cdots & x_{pn} \end{Bmatrix}.$$

Кожен стовпчик  $x_i = (x_{i1}, x_{i2}, \dots, x_{pi})$ ,  $i = 1, 2, \dots, n$  і рядок  $x_j = (x_{j1}, x_{j2}, \dots, x_{ji})$ ,  $j = 1, 2, \dots, p$  матриці  $X$  являє собою відповідно  $n$ - і  $p$ -мірні вектори процесів, які спостерігаються, з  $np$ -мірними густинами ймовірностей. Можлива  $M+1$  гіпотеза  $H_0, H_1, \dots, H_\mu, H_M$  про належність інформаційного поля, що спостерігається, до  $\mu$ -го класу. Крім цього відомі також апіорні ймовірності гіпотез  $P = P\{H_\mu\}$ ,  $\mu = 0, 1, \dots, M$  та платіжна матриця:

$$C = \begin{Bmatrix} C_{00} & C_{01} & C_{02} & \cdots & C_{0M+1} \\ C_{10} & C_{11} & C_{12} & \cdots & C_{1M+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ C_{M+10} & C_{M+11} & C_{M+12} & \cdots & C_{M+1M+1} \end{Bmatrix},$$

елемент  $C_{jm}$  якої є платою за рішення  $\gamma_\mu$ , коли істинною була гіпотеза  $H_j$ ,  $j = \mu = 0, 1, \dots, M$ . Простір рішень  $G = (\gamma_0, \gamma_2, \dots, \gamma_M)$  складається з  $M+1$  елементів, де  $\gamma_\mu$  – рішення прийняти гіпотезу  $H_\mu$ . Отже, задача системи розпізнавання технічного стану полягає в тому, щоб за результатами спостереження прийняти одну з гіпотез і відхилити інші.



Середній ризик під час прийняття рішення системою розпізнавання технічного стану визначається так:

$$R = \sum_{j=0}^m \sum_{\mu=1}^m C_{j\mu} P_j \int_{G_\mu} w(x_1, x_2, \dots, x_m) H_0 / X.$$

Мінімальне значення середнього ризику досягається у тому випадку, якщо до області  $G_\mu$  прийняття рішення  $\gamma_\mu$  система розпізнавання віднесе точки  $X$  вибіркового простору, що задовольняють системі нерівностей:

$$\sum_{j=1}^m (C_{ij} - C_{j\mu}) \frac{P_i w(x_1, x_2, \dots, x_i, \dots, x_m) / H_i}{P_i w(x_1, x_2, \dots, x_i, \dots, x_m) / H_0} \geq C_{0\mu} - C_{0j}. \quad (3)$$

Якщо ввести вектор відносин правдоподібності  $l(x) = [l_0(x), l_1(x), l_\mu(x), \dots, l_m(x)]$ , де  $l_\mu(x) = \frac{w(x_1, x_2, \dots, x_i, \dots, x_m) / H_\mu}{w(x_1, x_2, \dots, x_i, \dots, x_m) / H_0}$ , тоді систему нерівностей (3) можна представити у вигляді:

$$\sum_{i=1}^m (C_{ij} - C_{j\mu}) \frac{P_i}{P_j} l_i(x) \geq C_{0\mu} - C_{0j}, \quad j \neq \mu.$$

При цьому вектор  $l(x)$  несе всю інформацію про гіпотези, що перевіряються, і для прийняття рішення за результатом спостереження достатньо обчислювати компоненти  $M$ -мірного вектора відносин правдоподібності. Отже, задачу обчислення  $l(x)$  і прийняття рішення в структурі системи розпізнавання технічного стану на основі нейронної мережі вирішує класифікатор (рис. 4).

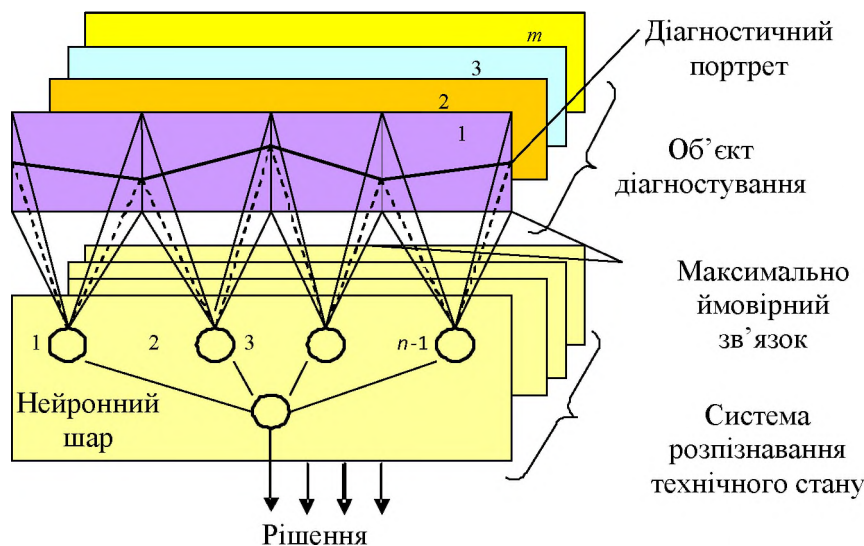


Рис. 4. Структура системи розпізнавання технічного стану

Наведена структура розпізнавання технічного стану містить  $m$ -нейронних шарів, які визначаються кількістю класів технічних станів, що розпізнаються. При цьому клас технічних станів відповідає нейронному шару, а кількість класів визначається глибиною пошуку несправності. Оскільки мікропроцесорна система містить множину можливих несправностей, що призводять до неправильного функціонування, простір технічних станів породжує нейронний шар статистичним описом класу через ймовірний діагностичний портрет

(ймовірнісну діагностичну матрицю). Отже, число шарів у структурі системи розпізнавання технічного стану визначатиметься числом класів, тобто числом структурних елементів, які мають ознаки неправильного функціонування.

Крім цього зазначимо, що число нейронів у шарі визначається обсягом статистичної вибірки ( $n$ ). При цьому великі статистичні вибірки збільшують розмірність простору технічних станів, представлених діагностичним портретом (набором симптомів), а малі неможливо однозначно пов'язати як симптоми з діагнозом. Оптимальним буде такий діагностичний портрет, який дозволяє отримати необхідний обсяг діагностичної інформації у контрольних точках. При цьому число нейронів у шарі визначається діагностичним портретом (набором симптомів) та числом контрольних точок в об'єкті контролю та діагностування.

Враховуючи викладене, процес розпізнавання технічного стану можна інтерпретувати таким чином. На вхід системи розпізнавання технічного стану надходить діагностична інформація у вигляді набору симптомів (діагностичного портрета), при цьому частина нейронів збуджується. Рівень збудження залежить від ймовірності зв'язку передачі збудження і визначається вагою  $G_\alpha(k)$ . На виходах нейронів створюється відображення діагностичної інформації у вигляді розподілу збуджень. Залежно від рівня збудження (ваги) збуджується певний синаптичний зв'язок, який передає збудження з вагою  $G_\alpha(k)$ , що є ефективністю синапсу. Реакція нейрона в алгоритмі розпізнавання технічного стану визначається добутком попарних оцінок ймовірностей з виходів рецепторів та відповідних ваг синаптичних зв'язків, що записується у вигляді:

$$g_i(k) = \prod_{\alpha=1}^r G_\alpha(k) d_\alpha(k),$$

де  $d_\alpha(k) = \begin{cases} 1, & \text{при } X_\alpha = U_\alpha \\ 0, & \text{при } X_\alpha \neq U_\alpha \end{cases}$  – індикатор рівня збудження нейрона.

При цьому  $G_\alpha(k)$  – величина ефективності синаптичного зв'язку  $\alpha$ -входу нейрона;  $U_\alpha$  – еталонне значення  $\alpha$ . В результаті на виході шару формується сигнал

$$A_i(X) = \prod_{k=1}^n \prod_{\alpha=1}^r g_i(k).$$

Підбиваючи підсумок, можемо констатувати, що сукупність шарів є нейронною мережею. Такі діагностичні нейронні мережі є спрощеною просторово-часовою моделлю, оскільки не враховують її нелінійність. При цьому вони мають асоціативні властивості, що нагадують властивість біологічних систем. Окрім цього, в цих системах інформація про технічний стан об'єкта контролю представляється мережею пов'язаних станів-вузлів та впорядкованим поширенням активності по мережі. Це мережа одночасно активних елементів, які обробляються (станів та переходів-асоціацій), локальні взаємодії яких у часі визначають поведінку діагностичної системи, складовою якої є об'єкт контролю.

**Висновки.** Запропоновано підхід до визначення технічного стану мікропроцесорних систем за допомогою нейронної мережі, який в подальшому може виступати в якості конкурента вбудованим системам контролю та діагностування. Зазначено, що застосування існуючих методів і засобів технічного діагностування мікропроцесорних систем, які реалізовані на програмно-реконфігурованій елементній базі і функціонують в умовах несприятливого впливу, є малоефективним. Це пов'язано, перш за все, з неповною, нечіткою і суперечливою інформацією про технічний стан мікропроцесорних систем, із складністю отримання якісного діагностичного портрета, а також зі здатністю мікропроцесорної системи, реалізованої на програмно-реконфігурованій елементній базі, змінювати свою внутрішню

алгоритмічну структуру в процесі функціонування. Виходячи з цього, застосування нейронної мережі та програмно-реконфігурованої елементної бази відкриває нові можливості щодо проектування не лише адаптивних мікропроцесорних систем до несприятливих впливів, а й адаптивних вбудованих систем контролю та діагностування з елементами штучного інтелекту. Такий синергізм нейронної мережі та мікропроцесорної системи дає в подальшому поштовх інтелектуалізувати не лише процедуру визначення технічного стану, а і процедуру відновлення правильного функціонування мікропроцесорної системи шляхом реконфігурації її внутрішньої алгоритмічної структури.

#### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Furber S. Microprocessors: the engines of the digital age. *Proc Math Phys Eng Sci.* 2017 Mar; 473(2199):20160893. DOI: 10.1098/rspa.2016.0893. Epub 2017 Mar 15. Erratum in: *Proc Math Phys Eng Sci.* 2017 May; 473(2201):20170304. PMID: 28413353; PMCID: PMC5378251.
2. Локазюк В. М., Заєць О. М. Тестове комбіноване діагностування персональних комп'ютерів // Вимірювальна та обчислювальна техніка в технологічних процесах: зб. наук. пр. Хмельницький: ТУП, 2000. С. 160–163.
3. Shtanenko S., Samokhvalov Y., Iohov O., Maliuk V. Microprocessor systems based on programmable logic devices as an object of diagnostics // *Advanced Information Systems.* 2022. № 6 (1). P. 81–87. URL: <https://doi.org/10.20998/2522-9052.2022.1.14>.
4. Вишнівський В. В., Жердев М. К., Креденцер Б. П., Кузавков В. В., Редзюк Є. В. Безконтактний індукційний метод діагностування радіоелектронних блоків // *Збірник наукових праць ВІКНУ ім. Тараса Шевченка.* Київ. 2013. ип. 43. С. 17–23.
5. Кузавков В. В., Хусаїнов П. В. Прогнозування технічного стану однотипних програмно-апаратних засобів // *Інформатика та математичні методи в моделюванні.* 2018. Т. 8. № 1. С. 57–68.
6. Бабокин Г. И., Шпрехер Д. М. Применение нейронных сетей для диагностики электромеханических систем // *Горный информационно-аналитический бюллетень.* 2011. S 4. С. 132–139.
7. Горева Т. И., Портнягин Н. Н., Пюкке Г. А. Нейросетевые модели диагностики технических систем // *Вестник КРАУНЦ. Физ.-мат. Науки.* 2012. Вып. 1 (4). С. 31–43. DOI: <http://dx.doi.org/10.18454/2079-6641-2012-4-1-31-43>.
8. Мартинюк Т. Б., Круківський Б. І. Класифікаційний аналіз методів сортування // *Вісник ВПІ.* 2023. Вип. 3. С. 77–83.
9. Палагин А. В., Яковлев Ю. С. Особенности проектирования компьютерных систем на кристалле ПЛИС // *Математичні машини і системи.* 2017. № 2. С. 3–14. ISSN 1028-9763.
10. Shtanenko S., Samokhvalov Y., Toliupa S., Silko O. The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) *Emerging Networking in the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering.* 2023. Vol 965. Springer, Cham.
11. Пинкевич В. Ю., Платунов А. Е. Тестирование и отладка встраиваемых вычислительных систем на основе уровневых моделей // *Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* 2018. № 5 (117). Т. 18. С. 801–808.
12. Иыуду К. А. Надежность, контроль и диагностика вычислительных машин и систем. М.: Высшая школа, 1989. 216 с.
13. Jäger, Reinhold. Computer diagnostics – a survey: Practical applications of computerized assessment: Theoretical principles and perspectives. *European Review of Applied Psychology / Revue Européenne de Psychologie Appliquée.* 1991. № 41. P. 247–268.
14. Гуляев В. А. Техническая диагностика управляющих систем. Киев: Наукова думка, 1983. 208 с.
15. Поморова О. В. Теоретичні основи, методи та засоби інтелектуального діагностування комп'ютерних систем: монографія. Хмельницький: ТОВ «Триада-М», 2007. 253 с.

16. Герасимов Б. М. Інтелектуальні системи підтримки прийняття рішень / Б. М. Герасимов, В. М. Локазюк, О. Г. Оксіюк, О. В. Поморова. К: Видавництво Європейського університету, 2007. 335 с.
17. Philippe G. Schyns. Diagnostic recognition: task constraints, object information, and their interactions, *Cognition*. Vol. 67, Issues 1–2. 1998. P. 147–179. ISSN 0010-0277.
18. Креденцер Б. П., Толюпа С. В., Шкваб В. К., Штаненко С. С. Аналіз засобів тестування і діагностики телекомунікаційної мережі // Збірник наукових праць ВІКНУ ім. Тараса Шевченка. 2007. № 7. С. 117–121.
19. Лукова-Чуйко Н. В. Методи інтелектуального розподілу даних в системах виявлення мережових вторгнень та функціональна стійкість інформаційних систем до кібератак: монографія / Н. В. Лукова-Чуйко, С. В. Толюпа, В. С. Наконечний, М. М. Браїловський. К.: Формат, 2021. 370 с.

### АВТОРИ НОМЕРА

1. **Беляков Роберт Олегович** – кандидат технічних наук, доцент, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
2. **Бернацький Андрій Петрович** – старший викладач кафедри спеціальних систем та робототехнічних комплексів факультету бойового застосування систем управління та зв'язку Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
3. **Власенко Олександр Володимирович** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
4. **Гримуд Андрій Геннадійович** – доктор філософії, старший викладач кафедри телекомунікаційних систем та мереж факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
5. **Данилюк Ігор Андрійович** – головний науковий співробітник науково-дослідного управління (перспектив розвитку інформаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
6. **Залужний Олексій Вікторович** – кандидат технічних наук, старший викладач кафедри кібербезпеки факультету бойового застосування систем управління та зв'язку Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
7. **Карпенко Андрій Олександрович** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
8. **Клімович Сергій Олегович** – кандидат технічних наук, начальник кафедри захисту інформації в телекомунікаційних системах та мережах факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
9. **Легкобит Володимир Сергійович** – старший викладач кафедри комп'ютерних інформаційних технологій факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
10. **Мельник Борис Олександрович** – кандидат технічних наук, начальник науково-дослідного відділу розвитку озброєння та військової техніки Сил спеціальних операцій науково-дослідного управління розвитку озброєння та військової техніки Сухопутних військ Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, м. Київ, Україна.
11. **Новікова Ірина Вікторівна** – старший науковий співробітник науково-дослідного відділу Інституту логістики та підтримки військ (сил) Національного університету оборони України, м. Київ, Україна.
12. **Овчаренко Ігор Володимирович** – кандидат військових наук, професор кафедри технічного забезпечення, доцент Інституту логістики та підтримки військ (сил) Національного університету оборони України, м. Київ, Україна.
13. **Остапчук Віктор Миколайович** – начальник Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
14. **Пелешок Євген Володимирович** – кандидат технічних наук, науковий співробітник Науково-дослідного інституту воєнної розвідки.
15. **Радзівілов Григорій Данилович** – кандидат технічних наук, професор, заступник начальника Військового інституту телекомунікацій та інформатизації ім. Героїв Крут з наукової роботи, м. Київ, Україна.
16. **Радченко Микола Миколайович** – науковий співробітник науково-дослідної лабораторії (розвитку мереж зв'язку на базі безпілотних авіаційних комплексів) науково-

дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

17. **Романюк Валерій Антонович** – доктор технічних наук, професор, професор кафедри автоматизованих систем управління факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

18. **Самохвалов Юрій Якович** – доктор технічних наук, професор, професор кафедри інтелектуальних технологій Київського Національного університету ім. Тараса Шевченка, м. Київ, Україна.

19. **Сидоркін Павло Григорович** – старший науковий співробітник науково-дослідної спеціальної лабораторії № 2 Науково-дослідного центру Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ, Україна.

20. **Стоцький Іван Володимирович** – викладач кафедри комп'ютерних інформаційних технологій факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

21. **Субач Ігор Юрійович** – доктор технічних наук, професор, завідувач спеціальної кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ, Україна.

22. **Толюпа Сергій Васильович** – доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського Національного університету ім. Тараса Шевченка, м. Київ, Україна.

23. **Фесенко Олексій Дмитрович** – викладач кафедри кафедри технічного та метрологічного забезпечення факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

24. **Хорошко Володимир Олексійович** – доктор технічних наук, професор, науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

25. **Чевардін Владислав Євгенійович** – доктор технічних наук, начальник кафедри кібербезпеки факультету бойового застосування систем управління та зв'язку Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

26. **Шаповал Віталій Михайлович** – начальник науково-дослідного відділу математичного та програмного забезпечення Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

27. **Штаненко Сергій Станіславович** – кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

28. **Юрченко Олег Васильович** – старший викладач кафедри кібербезпеки факультету бойового застосування систем управління та зв'язку факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

29. **Янковський Олег Георгійович** – кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

## ПАМ'ЯТКА АВТОРУ

Наукові статті у фахових виданнях повинні мати такі необхідні елементи:

**постановка проблеми** у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

**аналіз останніх досліджень і публікацій**, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття;

**формулювання мети статті** (постановка завдання);

**виклад основного матеріалу** дослідження з повним обґрунтуванням отриманих наукових результатів (моделей та результатів моделювання);

**висновки** з дослідження з визначенням наукової новизни;

**перспективи** подальших досліджень автора у даному напрямку.

**Список використаних джерел** повинен містити не менше 10–15 посилань бажано терміном видання не більше 10 років.

Рукопис подається у текстовому редакторі – **Microsoft Word 10 (не нижче)**.

Формат аркуша – **A4 (210 мм × 297 мм)**.

Розмір полів: зліва – **20 мм**, справа – **20 мм**, зверху – **20 мм**, знизу – **20 мм**.

Стиль – **normal** (звичайний), інтервал між рядками – **1,0**, абзацний відступ – **1 см**. Шрифт – **Times New Roman**, розмір шрифту – **12 пт**, із виключенням переносів.

Анотацію друкують курсивом, шрифт **Times New Roman**, розмір шрифту – **10 пт**. Анотацію та ключові слова подають українською та англійською мовами. Обсяг кожної анотації з ключовими словами – **1800 знаків** із пробілами. Анотація повинна бути структурована таким чином: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після анотації 5–7 ключових слів українською, англійською мовами. Список використаних джерел оформляється 11 шрифтом, згідно з ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання.

Не приймаються праці, у яких відсутній повний опис наукових результатів, що засвідчує їх, достовірність, або в яких повторюються результати, опубліковані раніше в інших наукових працях, що входять до списку основних (Постанова ВАК України від 10.02.99 № 1 – 02/3).

Статті, які містять загальновідому науково-технічну інформацію, плагіат, не розглядаються й не друкуються.

**Рукопис статті** потрібно подавати разом із зазначеними документами українською мовою: *акт експертизи; довідка про автора (авторів)*.

В один випуск «Системи і технології зв'язку, інформатизації та кібербезпеки» приймається не більше однієї статті за темою дисертації.

Редакційна колегія залишає за собою право вносити в рукопис зміни редакційного характеру.

Телефон для довідок: 256-22-37, 256-22-73, внутрішній 442-37, 442-73.

Електронна адреса для надання статей: **[naukaviti@gmail.com](mailto:naukaviti@gmail.com)**, **[naukaviti@viti.edu.ua](mailto:naukaviti@viti.edu.ua)**.

Етапи представлення статті для науковців інституту:

1. Стаття подається на розгляд головному редактору та після погодження – відповідальному редактору.

2. Після позитивного розгляду редколегією стаття подається коректору (кімната № 5 редакційно-видавничого відділу) для вчитки та корегування.

Виправлення електронного варіанта статті.

Друкування виправленого варіанта статті, отримання розпису коректора про виправлення помилок, що були виявлені, на останньому аркуші статті.

3. Виправлена стаття передається разом із супровідними документами відповідальному редактору для формування комп'ютерного макета збірника.