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 № 3

Communication, informatization and cybersecurity systems and technologies № 3

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

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 напрямами.

The book containes 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.

Київ – 2023 – Kyiv

УДК 621
ББК Ц4 (4Укр) 39
З – 415

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. № 3. 186 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.

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

Відповідальні за випуск: Головко О. Є., Куцаєв В. В.
Зам. 113. Друк. арк. 23,25.
Ум.-друк. арк. 21,62. Обл.-вид. арк. 20,10. Формат паперу 60×84/8.
Тираж 50 прим.
Адреса друкарні ВІТІ імені Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

ISSN 2786-6610

З М І С Т

C O N T E N T S

DOI: 10.58254/viti.3.2023.01.05

УДК 004.032.6

д-р техн. наук Бараннік В. В. ORCID: 0000-0002-2848-4524 (ХНУ ім. В. Н. Каразіна)
Гаврилов Д. С. ORCID: 0000-0002-3344-7808 (ХНУРЕ)
канд. техн. наук Гуржій П. М. ORCID: 0000-0002-2552-229X (ВІТІ ім. Героїв Крут)
Колесник В. О. ORCID: 0000-0001-7919-4255 (ДНДІВСОВТ)
Цімура Ю. В. ORCID: 0000-0002-6269-3821 (ВІТІ ім. Героїв Крут)

МЕТОД АДАПТИВНОГО ЦІЛІСНОГО АРИФМЕТИЧНОГО КОДУВАННЯ З ВРАХУВАННЯМ RLE-ПЕРЕТВОРЕННЯ

У роботі запропоновано метод багаторівневої селективної обробки для підвищення доступності інформації про об'єкти критичної інфраструктури з заданим рівнем достовірності та конфіденційності. Дана технологія ґрунтується на виявленні ключової інформації на декількох етапах обробки та адаптації алгоритму RLE та цілісного арифметичного кодування до нової структури вхідних даних. Таким чином, розглянуто останній етап обробки відеоданих запропонованим підходом, який націлений на зменшення об'єму і має особливість,яка полягає в тому, що отримано подальший розвиток методу лінеаризації двовимірних трансформант на основі зигзаг-сканування. Відмінності методу полягають у проведенні векторної міжтрансформантної зигзаг-лінеаризації з врахуванням селекції спектральних компонент, що визначені як доповнюючі. Вперше розроблено метод декомпозиції лінеаризованої трансформанти на основі визначення порогу. Характерні риси методу: знаходження порогу проводиться з врахуванням наявності в групі різних типів трансформант за визначенням загальної нерівномірної кількості нерівновагових доповнюючих компонент; удосконалено цілісне арифметичне кодування на основі врахування частостей елементів словника (двословникове цілісне арифметичне кодування). Відмінні особливості методу: визначення поточних кодових складових за декомпонованим робочим інтервалом залежно від потужності словників значимих елементів та кількостей повторів. Це дозволяє додатково врахувати статистичні особливості складових RLE-структурованої лінеаризованої трансформанти та знизити довжину арифметичного коду; вперше створено технологію стиснення трансформант на основі скорочення різних видів надмірності в групах трансформант. Характерні особливості технології: RLE-структурування нерівномірної доповнюючої частини групи трансформант після їх векторної лінеаризації та декомпонування; формування двох арифметичних кодів за двословниковим принципом нерівномірного поділу робочого інтервалу залежно від типу трансформант у групі.

Ключові слова: *метод багаторівневої селективної обробки, RLE, арифметичне кодування.*

V. Barannik, D. Havrylov, P. Hurzhii , V. Kolesnyk, Y. Tsimura Adaptive integer arithmetic coding with RLE-transform.

The paper proposes a method of multilevel selective processing to increase the availability of information about critical infrastructure objects with a given level of reliability and confidentiality. This technology is based on the identification of key information at several stages of processing and adaptation of the RLE algorithm and integral arithmetic coding into a new input data structure. Thus, the last stage of processing video data by the proposed approach is considered, which is aimed at reducing the volume with the following features: further development of the method of linearization of two-dimensional transforms based on zig-zag scanning is obtained. The differences of the method lie in carrying out the vector intertransform zigzag linearization taking into account the selection of spectral components, which is defined as complementary. For the first time, a method of decomposition of a linearized transform based on the definition of a threshold has been developed. Characteristic features of the method: the threshold is found taking into account the presence in the group of different types of transformants to determine the total uneven number of non-equilibrium complementary components; the integral arithmetic coding has been improved based on taking into account the frequencies of dictionary elements (two-dictionary integral arithmetic coding). Distinctive features of the method: determination of the current code components by the decomposed working interval, depending on the capacity of the dictionaries of significant elements and the number of repetitions. This allows additionally taking into account the statistical features of the components of the RLE-structured linearized transform and reducing the length of the arithmetic code; For the first time, a transformant compression technology was created based on the reduction of various types of redundancy in groups of transformants. Characteristic features of the technology: RLE-structuring of the non-uniform complementary part of the group of transforms after their vector linearization and decomposing; the formation of two arithmetic codes according to two dictionary principles of uneven division of the working interval, depending on the type of transformants in the group.

Keywords: *multilevel selective processing method, RLE, arithmetic coding.*

Постановка проблеми.

Збільшення темпів технічного розвитку суспільства в цілому спричинило зростання взаємозв’язків між елементами на всіх рівнях та в усіх сферах життя, особливо в критично важливих галузях суспільної діяльності. Водночас розв’язання складних проблем та задач, які постійно виникають у критично важливих галузях, потребує прийняття своєчасних, обґрунтованих рішень, що вимагають аналізу та узагальнення великої кількості інформації. Припинення (порушення) функціонування систем або об’єктів критичної інфраструктури, як фізичних так і віртуальних, призводить до виникнення кризових ситуацій [1–3]. З метою мінімізації ризиків та підвищенням рівня керованості об’єктами критичної інфраструктури використовують системи відеомоніторингу з можливістю передачі даних в реальному масштабі часу. Оскільки особа, яка приймає рішення, потребує якісної та повної інформації про об’єкти відеонагляду, існує тенденція постійного зростання роздільної здатності відеоконтента, обсяг якого може значно перевищувати пропускні спроможності каналів зв’язку [4–6]. Таким чином зростання обсягів відеоконтенту вимагає використання технологій обробки даних, націлених на зменшення об’єму даних, що будуть забезпечувати виконання вимог інформаційної доступності, тобто своєчасності доставки та обробки інформації до кінцевого споживача інформації – особи, яка приймає рішення під час виникнення кризових ситуацій.

Отже, існує нагальна потреба у відшуканні шляхів підвищення доступності інформації для задоволення потреб кінцевих користувачів.

Аналіз останніх досліджень та публікацій.

Нині для селективної обробки відеоданих на базі JPEG-платформи використовуються два основні підходи. Перший підхід ґрунтується на обробці зображення в просторово-часовій області. Другий підхід ґрунтується на обробці зображення в спектральній області. У публікаціях [7; 8] викладені можливі шляхи підвищення доступності відеоданих на основі обробки в спектральній області. Основним недоліком даних підходів є важкість селекції ключової інформації при загрозі її пропуску.

В публікаціях [9–11] доведено ефективність використання цілісного арифметичного кодування з метою підвищення доступності. Ефективність базується на потоковому принципі обробки кожного окремого елементу.

В публікаціях [12; 13] запропоновано підхід багаторівневої технології обробки відеоданих, в базис якої входить процес виявлення та обробки ключових даних в просторово-часовій та спектральній областях з метою підвищення рівня достовірності та конфіденційності. Важливим є те, що після обробки подібними методами залишаються лише доповнюючі компоненти, які потребують обробки алгоритмами кодування з метою підвищення рівня доступності відеокадру.

Таким чином, аналіз та вивчення наукових робіт за тематикою дослідження показав, що підвищення рівня достовірності та конфіденційності є актуальною науково-прикладною задачею. Виходячи з зазначеного, **метою статті** є підвищення рівня доступності відеоданих завдяки удосконаленню цілісного арифметичного кодування на основі врахування частоти елементів словника після обробки алгоритмом RLE.

Постановка завдання.

З метою зменшення часу доведення відеоінформаційного ресурсу до авторизованого користувача пропонується розглянути наступний етап обробки відеоданих після обробки алгоритмами, запропонованими у публікаціях [12; 13], метою якого є зменшення об’єму завдяки подальшому розвитку алгоритму кодування без втрат на основі RLE та арифметичного кодування.

Виклад основного матеріалу.

Після обробки відеоданих алгоритмами, запропонованими у публікаціях [12; 13], наступний етап пропонується проводити таким чином.

Спочатку робити розбиття зображення на групи трансформант 2×2 (рис. 1). Координати групи трансформант на зображенні мають вигляд $(\hat{v},\hat{u})$, де $\hat{\mathrm{v}}$ – координата групи по строках, а $\hat{\mathrm{u}}$ – по стовпцях [14; 15].

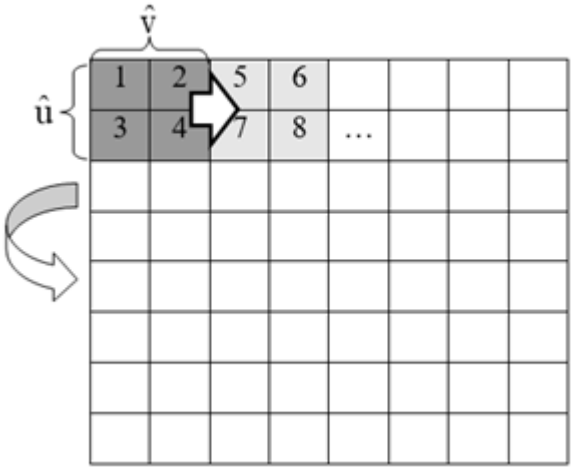


Рис. 1. Порядок розбиття відеозображення на групи трансформант 2×2

Для визначення розміру початкових даних при обробці алгоритмом RLE пропонується аналізувати службову інформацію другого етапу, а саме тип трансформанти за насиченістю. Можливі типи комбінацій для групи трансформант наведено у табл. 1.

Аналіз табл. 1 вказав на можливість визначення за номером комбінації кількості $\eta_{\text{dop}}^{(\text{trg})}$ доповнюючих компонент у групі трансформант. Це, в свою чергу, дозволяє визначити до якого моменту проводити арифметичне кодування та декодування. Також дана особливість дозволяє розділити множину доповнюючих компонент на частини відповідно до потреб (вимог).

Розділення метод декомпозиції лінеаризованої трансформанти на основі визначення порогу після RLE пропонується проводити з метою зменшення потужності словника та забезпечити умови для підвищення кількості надмірності, що скорочується в процесі арифметичного кодування. Характерні риси методу: знаходження порогу проводиться з врахуванням наявності в групі різних типів трансформант за визначенням загальної нерівномірної кількості нерівновагових доповнюючих компонент. Це матиме позитивний ефект, направлений на зменшення вихідного коду окремого кодованого символу на етапі адаптивного цілісного арифметичного кодування.

У нашому дослідженні пропонується розділяти потік доповнюючих компонент на 40 % та 60 % при кількості компонент від 180 до 217. Цей діапазон обрано з міркувань, що при комбінаціях 20–31 (табл. 1) потужність словника значень елементів буде більша ніж у випадках 1–19 та 32–35 (табл. 1), при яких потік передається повністю.

Таким чином, група трансформант, що відповідає комбінації 20–31 (табл. 1) з кількістю $\eta_{\text{dop}}^{(\text{trg})}$ доповнюючих компонент буде складатись з двох частин та матиме вигляд:

$$\eta_{\text{dop}}^{(\text{trg})} = \eta_{40\%\text{dop}}^{(\text{trg})} + \eta_{60\%\text{dop}}^{(\text{trg})}.$$

У інших випадках $\eta_{\text{dop}}^{(\text{trg})} = \eta_{100\%\text{dop}}^{(\text{trg})}$.

Таблиця 1

Можливі комбінації групи трансформант

Тип трансформанти	**Тип комбінацій**																		
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
не містить значиму інформацію	4	3	2	1	-	3	2	1	-	2	1	-	3	2	1	1	-	-	2
слабо	-	1	2	3	4	-	1	2	3	-	1	2	-	1	2	-	3	1	-
середньо	-	-	-	-	-	1	1	1	1	2	2	2	-	-	-	3	-	3	1
сильно	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1	-	1	-	1
Кількість $\eta_{dop}^{(trg)}$ доповнюючих компонент	256	255	254	253	252	246	245	244	243	236	235	234	228	227	226	226	225	225	218
Кількість сегментів для RLE-обробки	1																		
Кількість доповнюючих компонент для RLE-обробки	100% $\eta_{100\%dop}^{(trg)}$																		

Тип трансформанти	**Тип комбінацій**															
	20	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**
не містить значиму інформацію	1	-	-	1	-	2	1	-	-	1	-	-	1	-	-	-
слабо	1	2	-	-	1	-	1	2	-	-	1	-	-	1	-	-
середньо	1	1	4	2	2	-	-	-	3	1	1	2	-	-	1	-
сильно	1	1	-	1	1	2	2	2	1	2	2	2	3	3	3	4
Кількість $\eta_{dop}^{(trg)}$ доповнюючих компонент	217	216	216	208	207	200	199	198	198	190	189	180	172	171	162	144
Кількість сегментів для RLE-обробки	2												1			
Кількість доповнюючих компонент для RLE-обробки	40% $\eta_{40\%dop}^{(trg)}$, 60% $\eta_{60\%dop}^{(trg)}$												100% $\eta_{100\%dop}^{(trg)}$			

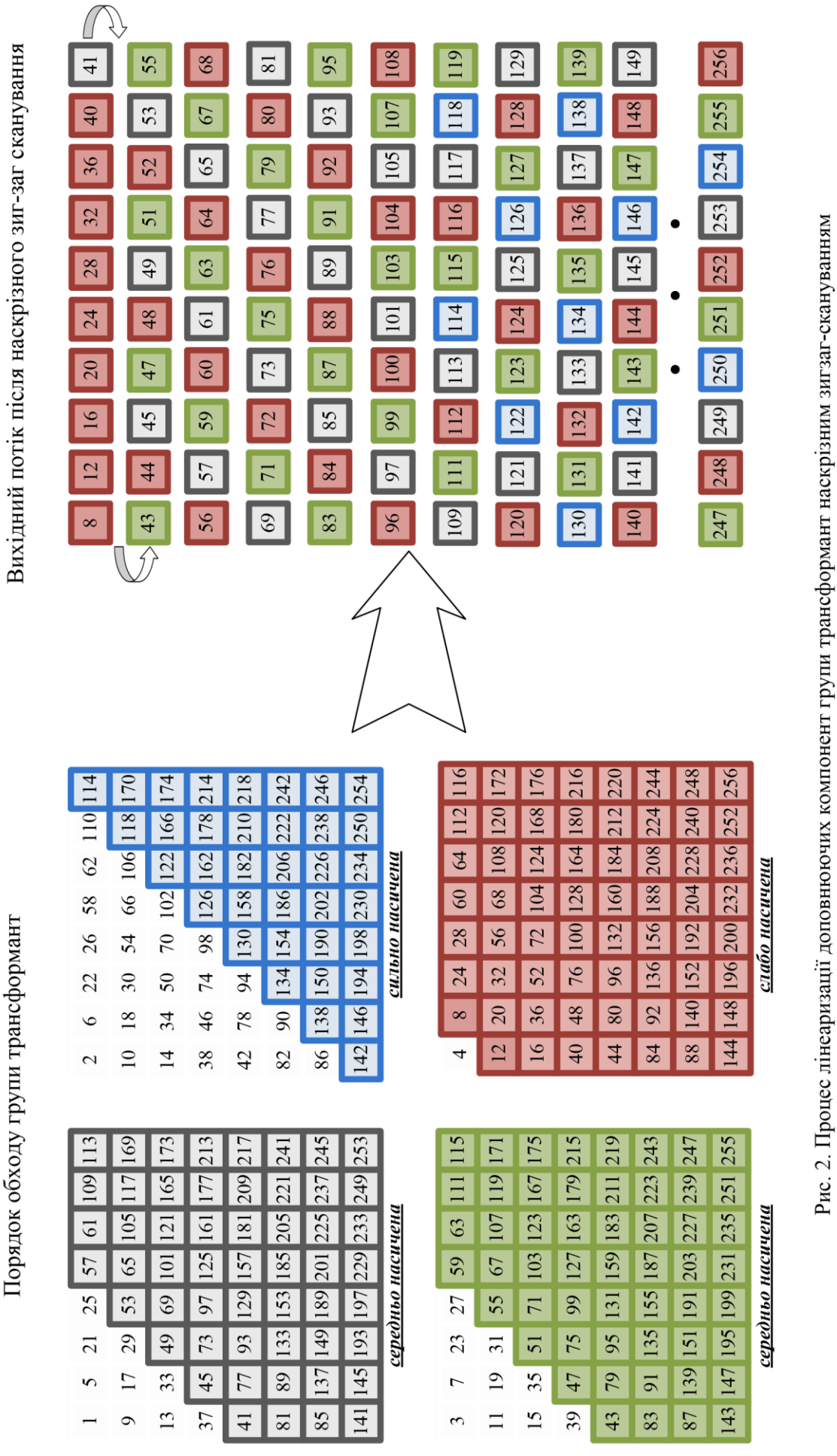


Рис. 2. Процес лінеаризації доповнюючих компонент групи трансформант наскрізним зигзаг-скануванням

Після виконання наведених вище підготовчих маніпуляцій відповідна кількість компонент подається на алгоритм обробки RLE. В результаті RLE-обробки отримуємо пару «значення елементу $a_{\iota}''^{(\hat{v},\hat{u})}$, кількість елементів $\varsigma_{\iota}''^{(\hat{v},\hat{u})}$» для квантованих компонент групи трансформант.

Таким чином, отримав подальший розвиток метод лінеаризації двовимірних трансформант на основі зигзаг-сканування. Відмінності методу полягають у проведенні векторної міжтрансформантної зигзаг-лінеаризації з врахуванням селекції спектральних компонент, що визначені як доповнюючі. Це забезпечує врахування структурних особливостей в середині і в потоці трансформант та створює умови для підвищення ефективності RLE-перетворення. Вперше розроблено метод декомпозиції лінеаризованої трансформанти на основі визначення порогу. Характерні риси методу: знаходження порогу проводиться з врахуванням наявності в групі різних типів трансформант за визначенням загальної нерівномірної кількості нерівновагових доповнюючих компонент. Це дозволяє: зменшити потужності словників елементів RLE-структурованої послідовності; забезпечити умови для підвищення кількості надмірності, що скорочується в процесі арифметичного кодування. Ці перетворення дозволяють зменшити потужність словника, що має позитивний ефект для наступних етапів обробки.

З метою зменшення об'єму даних пропонується проводити обробку удосконаленим адаптивним цілісним арифметичним кодуванням з урахуванням структурних особливостей. Ці особливості полягають у наявності двох типів даних, які належать до словника $\Psi\left(a''^{(\hat{v},\hat{u})}\right)$ значень елементів та словника $\Psi\left(\varsigma''^{(\hat{v},\hat{u})}\right)$ кількості повторів.

Для зменшення потужності загального словника Ψ пропонується робити модифікації, а саме:

1) якщо на передавальній стороні величина кількості повторів дорівнює одиниці ($\varsigma_{\iota}''^{(\hat{v},\hat{u})} = 1$), то дана величина нехтується (не кодується) у зв'язку з тим, що вона зустрічається найчастіше. Якість відновлення кодованої послідовності забезпечується тим, що користувачу відомо, до якого словника належить закодований елемент. У разі надходження на декодер підряд двох елементів зі словника $\Psi\left(a''^{(\hat{v},\hat{u})}\right)$ значень елементів, між ними додається одиниця, так як елементи словників чергуються;

2) так як після етапу квантування завжди буде елемент, величина якого дорівнює нулю ($a_{\iota}''^{(\hat{v},\hat{u})} = 0$), то його слід розміщувати з лівого боку у першому інтервалі ($\iota = 1$). Адже ймовірність появи даного елементу найбільша. Ця маніпуляція направлена на зменшення коду нульового елементу, що матиме позитивний ефект на рівень компресії в цілому;

3) найбільша величина $\max\left(\varsigma''^{(\hat{v},\hat{u})}\right)$ кількості повторів знаходиться в останній парі після обробки алгоритмом RLE. При цьому, значення елементу останньої пари дорівнює нулю $a_{\iota}''^{(\hat{v},\hat{u})} = 0$. Виходячи з даних міркувань, кодування останньої пари є надлишковим за умови передачі величини $\max\left(\varsigma''^{(\hat{v},\hat{u})}\right)$ кількості повторів останньої пари після обробки алгоритмом RLE у словнику $\Psi\left(\varsigma''^{(\hat{v},\hat{u})}\right)$ кількості повторів.

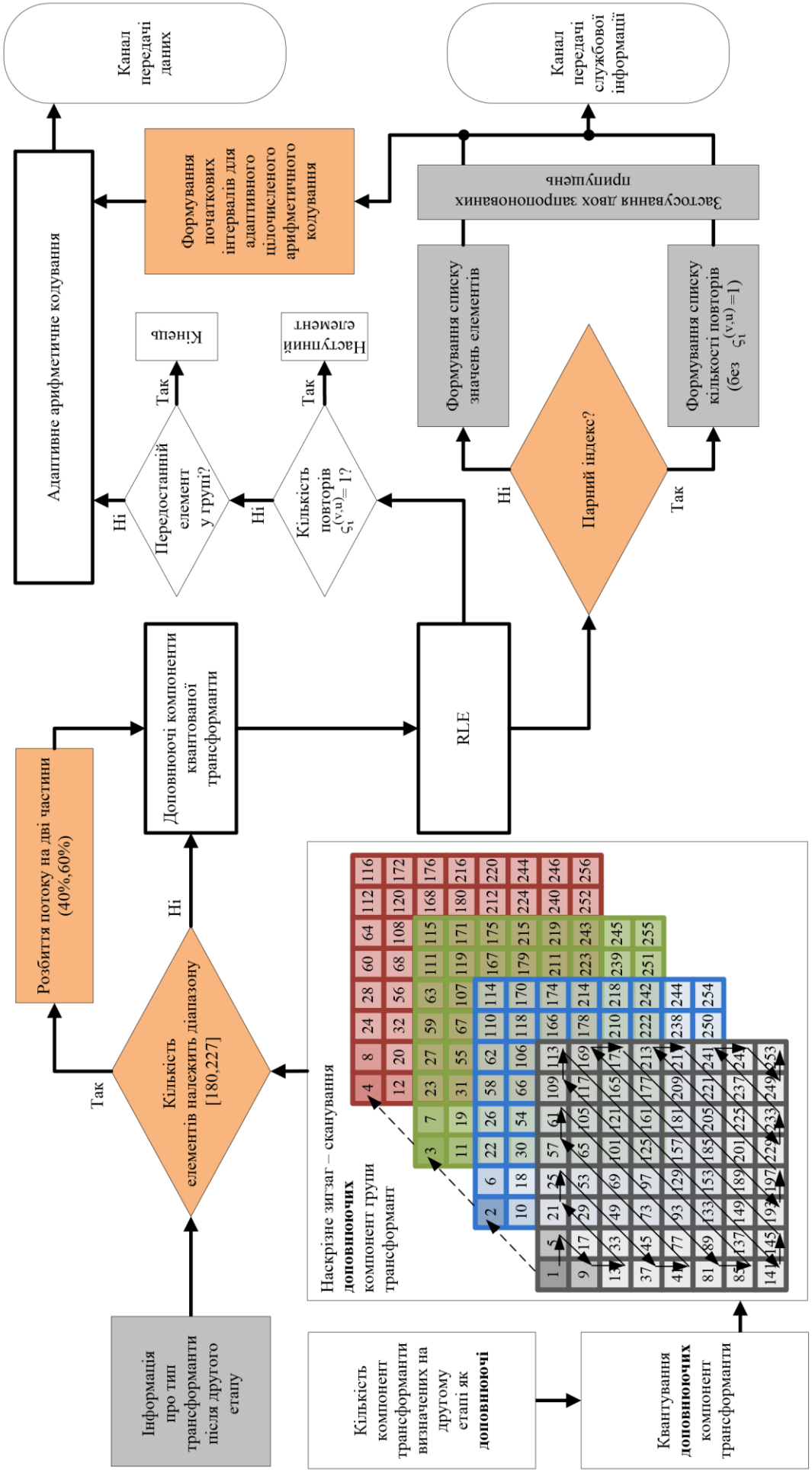


Рис. 4. Блок-схема запропонованого етапу інформаційного методу обробки відеозображення

У запропонованому методі адаптивного цілісного арифметичного кодування у робочому інтервалі компоненти зі словнику $\Psi\left(a''^{(\hat{v},\hat{u})}\right)$ значень елементу розташовуються зліва, а після них компоненти зі словнику $\Psi\left(\varsigma''^{(\hat{v},\hat{u})}\right)$ кількості повторів – справа (рис. 3).

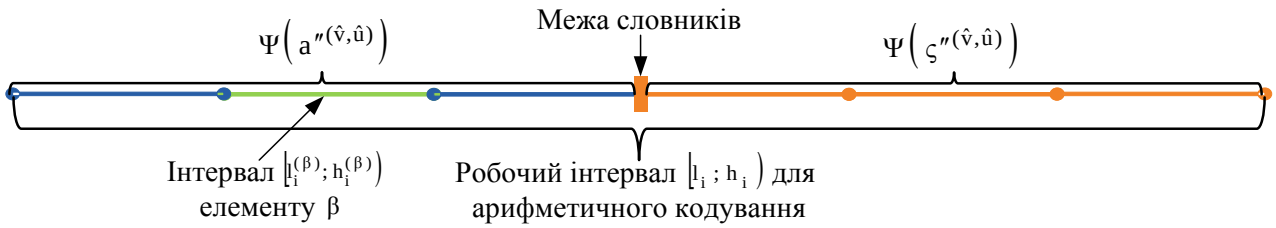


Рис. 3. Приклад побудови робочого інтервалу для арифметичного кодування

Це дозволить однозначно зрозуміти, якому словнику належить декодований елемент, так як межа словників $\Psi\left(a''^{(\hat{v},\hat{u})}\right)$ та $\Psi\left(\varsigma''^{(\hat{v},\hat{u})}\right)$ відома як на передавальній, так і на приймальній стороні. Також, це дозволяє зберегти структуру даних для RLE-декодування, що є важливим, адже як на кодер, так і з декодеру поступає потік лінеаризованих компонент $a_i^{(1,\hat{v},\hat{u})}$, зсув (втрата) елементів якого призведе до зниження рівня достовірності.

Узагальнена блок-схема запропонованого етапу методу підвищення доступності інформації про об’єкти критичної інфраструктури з заданим рівнем достовірності та конфіденційності наведена на рис. 4.

Таким чином, удосконалено цілісне арифметичне кодування на основі врахування частоти елементів словника (двословникове цілісне арифметичне кодування). Відмінні особливості методу: визначення поточних кодових складових за декомпонованим робочим інтервалом залежно від потужності словників значимих елементів та кількостей повторів. Це дозволяє додатково врахувати статистичні особливості складових RLE-структурованої лінеаризованої трансформанти та знизити довжину арифметичного коду.

Висновки.

У статті запропоновано метод багаторівневої селективної обробки для підвищення доступності інформації про об’єкти критичної інфраструктури з заданим рівнем достовірності та конфіденційності. Дана технологія ґрунтується на виявленні ключової інформації на декількох етапах обробки та адаптації алгоритму RLE та цілісного арифметичного кодування до нової структури вхідних даних. Таким чином, розглянуто останній етап обробки відеоданих запропонованим підходом, який націлений на зменшення об’єму. Задача статті, що полягала в удосконаленні цілісного арифметичного кодування на основі врахування частоти елементів словника після обробки алгоритмом RLE, є досягнутою.

Подальшим напрямком розвитку проведених досліджень може бути модифікація алгоритму RLE.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шульгін С. С. Технологія кодування трансформованих відеосегментів в нерівноваговому діагонально-позиційному просторі // Наукоємні технології. 2022. № 2 (54). С. 147–154.

2. V. Barannik. Technology of Structural-Binomial Coding to Increase the Efficiency of the Functioning of Computer Systems // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 96–100. DOI: 10.1109/ATIT58178.2022.10024205.

3. V. Barannik, A. Krasnorutsky, V. Kolesnik, V. Barannik, S. Pchelnikov, P. Zeleny. Compression method in terms of ensuring the fidelity of video images in infocommunication networks // Radioelectronic and Computer Systems, 2022, no 4 (100). pp. 10–24. DOI: 10.32620/reks.2022.5/09.

4. A. Krasnorutsky, R. Onyshchenko, D. Barannik and V. Barannik. The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 53–56. DOI: 10.1109/ATIT58178.2022.10024208.

5. V. Barannik, Y. Babenko, V. Barannik, V. Kolesnyk and D. Zhuikov. Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 66–71. DOI: 10.1109/ATIT58178.2022.10024193.

6. V. Barannik, S. Shulgin, N. Barannik and V. Barannik.Method of Coding Subbands of Non-Homogeneous Spectrum of Video Segments in Uneven Diagonal Space // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 72–75. DOI: 10.1109/ATIT58178.2022.10024236.

7. T. Belikova and S. Sidchenko. The Method Drawing up the Text with the Set Suggestive Orientation to Create a Hidden Channel // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 106–110. DOI: 10.1109/ATIT58178.2022.10024206.

8. V. Barannik, S. Shulgin, D. Barannik and Y. Sidchenko. Quadrature Compression Technology in Two-Level Polyadic Space for Infocommunication Systems // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 84–87. DOI: 10.1109/ATIT58178.2022.10024217.

9. Шульгін С. С. Метод динамічного кодування сегментів відеопотоку шляхом з’ясування структурних змін у нерівноважному діагонально-позиційному просторі // Наукоємні технології. 2022. № 3 (55). С. 238–243.

10. A. Krasnorutsky, V. Kolesnyk, A. Berchanov, V. Barannik, N. Kharchenko and O. Malko. Method of Structural-Statistical Coding of Video Segments in Spectral-Cluster Space // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 32–37. DOI: 10.1109/ATIT58178.2022.10024240.

11. O. Slobodyanyuk, A. Krasnorutsky, V. Bezruk, R. Onyshchenko, V. Kolesnyk and S. Podlesny. Approach to Coding with Improved Integrity of Video Information for Transmission in Wireless Infocommunication Networks // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 38–42. DOI: 10.1109/ATIT58178.2022.10024245.

12. D. Barannik and V. Barannik. Steganographic Coding Technology for Hiding Information in Infocommunication Systems of Critical Infrastructure // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, December 15–17, 2022, pp. 88–91. DOI: 10.1109/ATIT58178.2022.10024185.

13. Barannik, V. et al. (2023). A Method of Scrambling for the System of Cryptocompression of Codograms Service Components. 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, vol 965. Springer, Switzerland, Cham. URL: https://doi.org/10.1007/978-3-031-24963-1_26.

14. Barannik V., Barannik N., Khimenko V. Method of indirect information hiding in the process of video compression // Radioelectronic and Computer Systems. 2021. №. 4. PP. 119–131. URL: https://doi.org/10.32620/reks.2021.4.

15. Гаврилов Д. С., Бараннік В. В., Колесник В. О., Шульгін С. С., Єрмаченков А. В. та Савчук М. В. (2022) Method of Visual Data Processing in Telecommunication Network Based on JPEG Platform and Arithmetic Coding // Visnyk NTUU KPI. Seriia – Radiotekhnika Radioaparatobuduvannia, (89), pp. 21–28. DOI: 10.20535/RADAP.2022.89.21-28.

DOI: 10.58254/viti.3.2023.02.14

УДК. 621.391

канд. техн. наук Ільїнов М. Д. ORCID: 0009-0008-6945-3354 (ВІТІ ім. Героїв Крут)
канд. техн. наук Нестеренко І. К. (ВІТІ ім. Героїв Крут)
канд. техн. наук Янковський О. Г. ORCID: 0000-0001-8041-1843 (ВІТІ ім. Героїв Крут)

СПОСІБ ПОБУДОВИ КОМПЕНСАТОРА ЗАВАД НА ОСНОВІ ВИКОРИСТАННЯ БАГАТОВХОДОВИХ АНТЕННИХ СИСТЕМ

Завдання підвищення завадостійкості приймальних пристроїв радіоелектронних засобів є класичним та досить актуальним в сучасних умовах. Особливо ця проблема актуальна для систем мобільного радіозв’язку, в яких для організації зв’язку в якості приймально-передаючих антен зазвичай використовуються антени з ненаправленим випромінюванням в азимутальній площині, які особливо вразливі до дії спрямованих радіозавад. Одним із основних шляхів підвищення завадозахищеності радіоелектронних засобів рухомого об’єкта є розробка всеспрямованих антен, які мають один або більше напрямків нульового прийому та можуть електрично управлятися для мінімізації завад. Найбільш підходящою конструкцією антенної системи для вирішення вказаної задачі є варіант кільцевих антенних решіток. Кільцева антенна решітка у сукупності з діаграмо-утворюючою схемою відноситься до класу багатовходових антен, які дозволяють на практиці реалізувати схемно-просторовий метод об’єднання приймально-передаючих радіостанцій для збільшення канальної ємності системи мобільного радіозв’язку або для зменшення кількості антен на рухомих пунктах управління з метою підвищення їхньої мобільності скритності. У роботі запропонований спосіб побудови та варіант технічної реалізації компенсатора завад на основі багатовходових антенних систем на базі кільцевих антенних решіток з діаграмо-утворюючими схемами. Визначені напрямки дослідження доцільності практичного застосування пропонованого способу підвищення завадозахищеності. Реалізація запропонованої схеми побудови антенної системи у вигляді кільцевої антенної решітки малого діаметра з просторовою адаптацією відносно напрямку приходу завад дозволить суттєво підвищити завадозахищеність абонентського комплекту системи зв’язку з рухомими об’єктами та надійність системи зв’язку у цілому.

Ключові слова: *радіолінія, компенсатор завад, кільцева антенна решітка, діаграмо-утворююча схема, навмисна завада, діаграма направленості.*

M. Ilinov, I. Nesterenko, O. Iankovskii The way of construction compensator interference based on usage multi-input antenna systems.

The task of improving the immunity of receiving devices of radio-electronic means is classic and quite relevant in modern conditions. This problem is especially relevant for mobile radio communication systems, in which antennas with non-directional radiation in the azimuthal plane, which are particularly vulnerable to directional radio interference, are mainly used to organize communication as receiving and transmitting antennas. One of the main ways to increase the immunity of radio-electronic means of a moving object is the development of omnidirectional antennas, which have one or more directions of null reception and which can be electrically controlled to minimize interference. The most suitable design of the antenna system for solving the specified problem is the option of ring antenna arrays. The ring antenna array in combination with the diagram-forming circuit belongs to the class of multi-input antennas, which allow in practice to implement the circuit-space method of combining receiving and transmitting radio stations to increase the channel capacity of the mobile radio communication system, or to reduce the number of antennas at mobile points management in order to increase their stealth mobility. The work proposes a method of construction and a variant of the technical implementation of the interference compensator based on multi-input antenna systems based on ring antenna arrays with diagram-forming circuits. The areas of study of the feasibility of practical application of the proposed method of improving immunity have been determined. Implementation of the proposed antenna system construction scheme in the form of a small-diameter ring antenna array with spatial adaptation relative to the direction of interference will allow to significantly increase the immunity of the subscriber set of the communication system with moving objects and the reliability of the communication system as a whole.

Keywords: *radio line, interference compensator, ring antenna array, diagram-forming circuit, intentional interference, radiation pattern.*

Постановка завдання. Задача підвищення завадостійкості приймальних пристроїв радіоелектронних засобів (далі – РЕЗ) є класичною та не втрачає своєї актуальності протягом довгого періоду часу. Вирішення цієї задачі досягається завдяки вдосконаленню засобів і способів формування та обробки сигналів.

Особливо ця проблема актуальна для систем мобільного радіозв’язку, в яких для організації зв’язку в якості приймально-передаючих антен зазвичай використовуються антени з ненаправленим випромінюванням в азимутальній площині.

Такі антенні системи особливо вразливі до дії спрямованих радіозавад. Тому завдання підвищення завадозахищеності РЕЗ рухомих об’єктів, у складі яких використовуються всеспрямовані антени, є актуальним.

Аналіз останніх досліджень. Одним із основних шляхів підвищення завадозахищеності РЕЗ рухомого об’єкта є розробка всеспрямованих антен, які мають один або більше напрямків нульового прийому (або мінімумів) та можуть електрично управлятися для мінімізації завад [1].

Найбільш підходящою конструкцією антенної системи для вирішення вказаної задачі є варіант кільцевих антенних решіток (КАР). В загальному вигляді така антенна система являє собою антенну решітку з випромінюючими елементами, які розташовані по колу (наприклад, навколо відбиваючої поверхні (труби), яка виконує одночасно роль траверси для закріплення випромінювачів), та діаграмо-утворюючою схемою (ДУС). КАР у сукупності з ДУС відносяться до класу багатовходових антен, які дозволяють на практиці реалізувати схемно-просторовий метод об’єднання приймально-передаючих радіостанцій для збільшення канальної ємності системи мобільного радіозв’язку або для зменшення кількості антен на рухомих пунктах управління з метою підвищення їхньої мобільності скритності [2].

Окрім можливості використовувати КАР з метою підвищення завадозахищеності РЕЗ, збільшення канальної ємності системи та зменшення кількості антен, подібні антенні системи дозволяють вирішувати й інші практичні задачі, а саме [3]:

– формувати задані діаграми направленості в азимутальній площині;

– підключати декілька передавачів (приймачів) безпосередньо без використання комбайнерів та приймальних розподіляючих панелей;

– формувати поле випромінювання у пріоритетному напрямку;

– бути складовою частиною радіопеленгаторів.

Недоліком вищерозглянутих робіт є те, що в них не вирішено завдання реалізації схеми побудови антенної системи у вигляді кільцевої антенної решітки малого діаметра з просторовою адаптацією відносно напрямку приходу завад для підвищення завадозахищеності абонентського комплекту системи зв’язку з рухомими об’єктами та надійності системи зв’язку у цілому.

Метою статті є вирішення наукового завдання щодо обґрунтування шляхів підвищення завадостійкості приймальних пристроїв радіоелектронних засобів зв’язку з рухомими об’єктами.

Виклад основного матеріалу.

При використанні КАР на рухомому об’єкті, де найважливішою вимогою до антенного пристрою є його масогабаритні показники, необхідно мінімізувати розміри антени, кількість випромінюючих елементів та забезпечити жорсткість конструкції у цілому. Тому на рухомих об’єктах доцільно використовувати КАР з мінімальною кількістю випромінювачів – три, чотири елементи з малим радіусом у поперечному перерізі. Така компоновка дозволяє розмістити випромінюючі елементи КАР у радіопрозорому обтічнику.

Для реалізації необхідного амплітудно-фазового розподілу струмів у випромінювачах КАР застосовуються ДУС, які виконуються у різних варіантах.

Для синфазного (мода нульового порядку) та квадратурного (мода першого порядку) збудження випромінюючих елементів ДУС може бути реалізована на квадратурних тридецибельних відгалужувачах (квадратурні мости).

На рисунку 1 представлено варіант КАР з діаграмо-утворюючої схемою, яка побудована з використанням квадратурних мостів М1, М2, М3, М4:

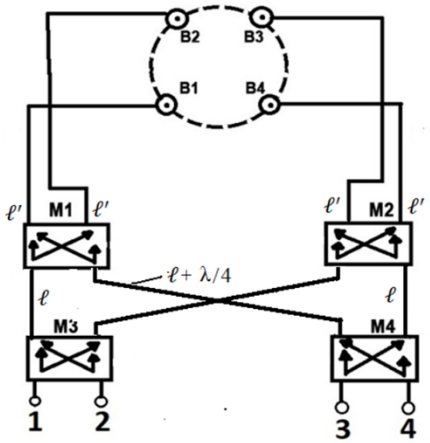


Рис. 1. ДУС на квадратурних мостах

Випромінюючі елементи антенної решітки В1, В2, В3 і В4 мають вигляд рівномірно розташованих в просторі по колу вертикальних симетричних вібраторів, які підключені до мостів М1, М2, М3 і М4. Відмінною особливістю даної ДУС є те, що виходи мостів з’єднуються між собою відрізками коаксіальних фідерів або іншими фідерними лініями (лініями передач) з довжиною l та $l + \lambda/4$, а з випромінювачами – відрізками l'. При такому компонуванні ДУС реалізується фазове збудження випромінювачів згідно з таблицею 1.

Таблиця 1

Варіанти компонування ДУС

№ входу	**Фази струмів, град.**			
	В1	**В2**	**В3**	**В4**
1	0	90	180	270
2	90	180	90	180
3	180	90	180	90
4	270	180	90	0

Такий амплітудно-фазовий розподіл струмів у випромінюючих елементах КАР дозволяє формувати у азимутальній площині чотири незалежні діаграми направленості (ДН) з ненаправленим випромінюванням поля у просторі. Вигляд ДН для випадку радіусу КАР $R = 0.25\lambda$, де λ – довжина хвилі робочого діапазону, показаний на рисунку 2.

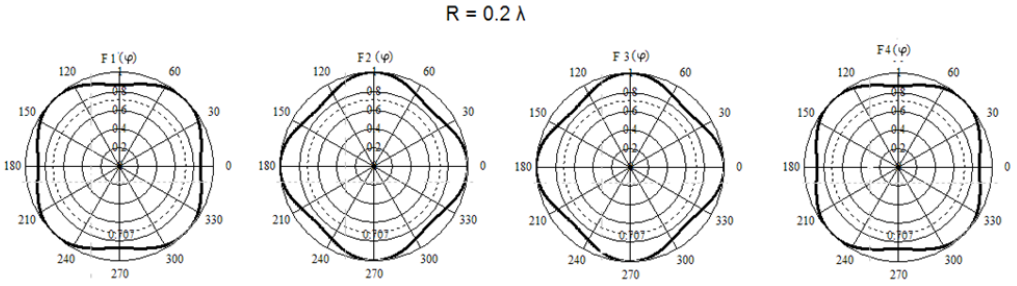


Рис. 2. ДН чотиривходової антенної решітки

Формування поля випромінювання в азимутальній площині визначається не тільки амплітудно-фазовим розподілом струмів у випромінюючих елементах КАР, але й її геометричними розмірами в поперечній площині, що наочно показано на рисунку 3.

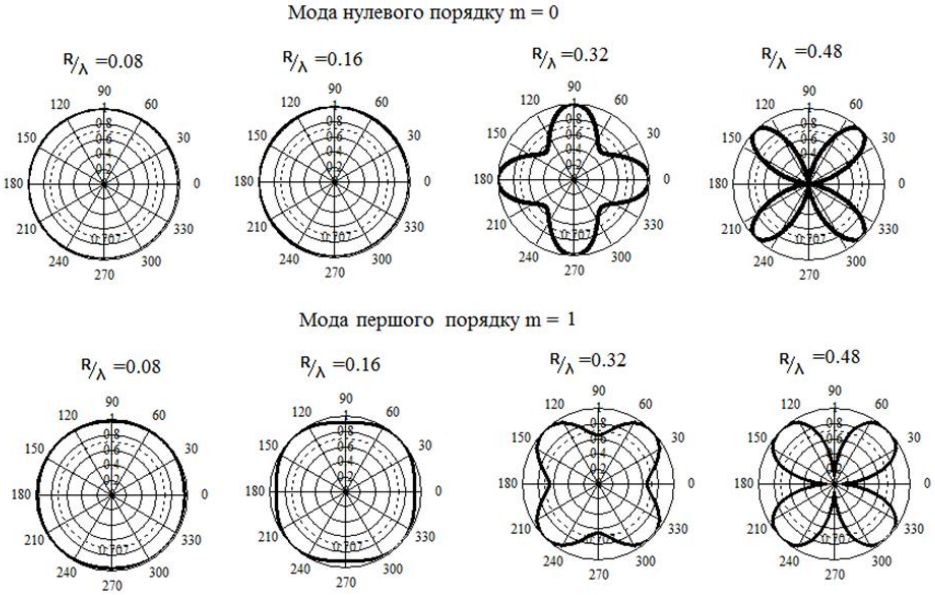


Рис. 3. ДН чотирьохелементних КАР у азимутальній площині

Аналіз теоретичних досліджень дозволяє сформулювати наступні висновки:

– при синфазному збудженні елементів решітки (мода «0»), а також при збудженні у послідовності фаз 90-180-90-180 при радіусі решітки 0.25λ, присутня незначна нерівномірність ДН у азимутальній площині (приблизно 0,6 дБ). При зменшенні радіуса решітки ДН стає практично рівномірною. Цей випадок справедливий як за відсутності центральної відбиваючої поверхні (труби), так й за її наявності;

– при квадратурному збудженні елементів решітки (мода «1») нерівномірність ДН зростає і дорівнює приблизно 2 дБ при радіусі решітки 0.25λ. Максимум випромінювання орієнтований під кутом 45°, а мінімум – 0°. При зменшенні радіуса до 0.12λ нерівномірність становиться менше ніж 1 дБ, й у подальшому при зменшенні радіуса решітки зменшується. Цей ефект також не залежить від наявності труби у центрі решітки. У роботі [4] ці розрахунки підтверджено експериментально.

При синфазному збудженні випромінювачів решітки малого радіуса (мода нульового порядку) пропонується розглядати КАР як вібраторний випромінювач зі збільшеним поперековим перерізом [4].

При квадратурному збудженні випромінювачів КАР (мода 1) залежність параметрів антени від її радіусу істотна. Зовнішні характеристики КАР (з повним циклом зміни фази) не змінюються при зменшенні радіусу, а опір випромінювання, відповідно й вхідний опір кожного випромінювача, суттєво змінюється. У КАР малого діаметру, коли $R \leq 0.12\lambda$, збільшується взаємний вплив між випромінювачами. Однак розв’язка між входами ДУС зберігається, що підтверджується результатами експериментальних досліджень [5].

Таким чином, ДН в азимутальній площині КАР на різних входах ДУС (різних фазових модах) будуть мати майже однакову амплітуду напруженості електричного поля випромінювання, але різну фазу залежно від азимутальної координати.

Комбінація цих двох мод із рівними амплітудами дає діаграму кардіоїдної форми, в якій напрямок нуля може змінюватись шляхом зміни фазового зсуву діаграми будь-якої моди. Зміна фаз при комбінації двох мод дозволить змінювати кут формування нуля ДН антени.

Використовуючи розглянутий математичний апарат, у роботі пропонується технічне рішення, яке дозволяє суттєво підвищити завадозахищеність абонентського комплекту системи зв’язку з рухомими об’єктами та надійність системи зв’язку у цілому.

На рисунку 4 показана функціональна схема простої чотирьохелементної КАР, яка дозволяє формувати нуль у ДН з можливістю управління його положенням у азимутальній площині.

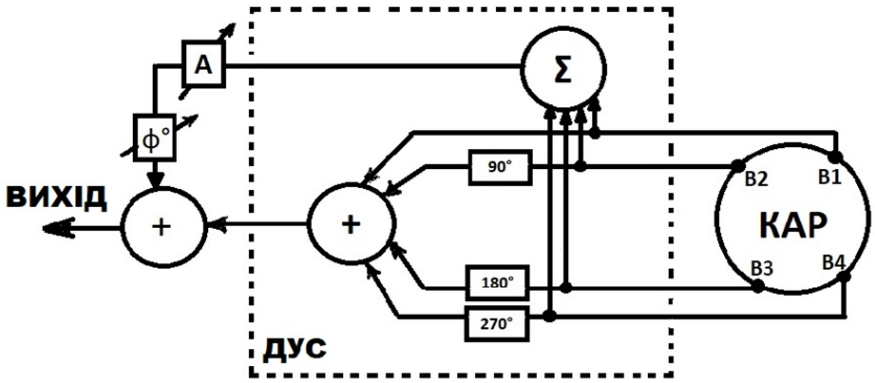


Рис. 4. Функціональна схема компенсатора завад

Атенюатор А на рисунку 4 вирівнює амплітуди полів у дальній зоні від двох фазових мод. Зміна фази фазообертача на φ призводить до азимутального кутового обертання нуля ДН на кут φ. Зміна кутового положення нуля ДСА забезпечується не зміною амплітуд та фаз сигналів для всіх 4-х елементів решітки, а зміною тільки одного фазового зсуву.

Для формування нуля ДН необхідно забезпечити згасання сигналу від сильної компоненти (моди) до рівня сигналу слабкої компоненти і вже потім сигнали від двох компонентів об’єднати. З цього випливає, що результуюче посилення антени (у всеспрямованій частині діаграми) буде приблизно на 3 дБ вище, ніж у слабкої моди. При великому радіусі решітки забезпечується сталість посилення антени на двох модах (не більше 0,15 дБ) у смузі частот більше октави [5].

Наведені результати показують, що ефективність решітки із застосуванням узгоджених навантажень 50 Ом у ДУС забезпечуються у смузі частот ± 10 % [5]. Розширення робочої смуги частот (більш ніж ± 20 %) може бути досягнуто застосуванням багатопозиційного атенюатора, який встановлює на кожній робочій частоті необхідне згасання.

У [6] наведені результати експериментального дослідження чотирьохелементних кільцевих решіток радіусом 0.04λ на частоті 153 МГц з нулем у ДН (рис. 5), положенням якого можна керувати. Вид ДН для малогабаритних КАР слабо залежить від радіуса решітки, однак при зменшенні радіуса решітки зменшується її коефіцієнт підсилення антени.

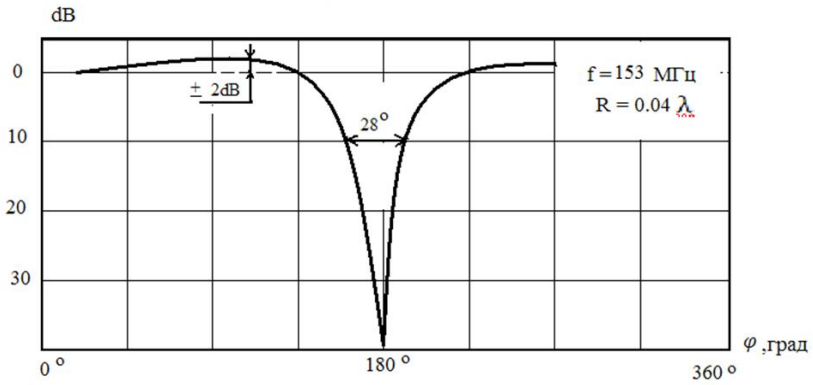


Рис. 5. Експериментальна ДН чотирьохелементної антени радіусом 0.04λ з керованим нулем

Зазначимо, що глибина нуля прагне до нескінченності (тобто більш ніж на 50 дБ) в кутах, які відповідають розташуванню елементів решітки. Якщо нуль спрямований у куті між елементами решітки, коли існує незначне відхилення від всеспрямованості складових мод, глибина нуля зменшується приблизно до рівня -27 дБ.

Для зменшення ширини провалу (нуля) ДН в [7] пропонується змінити компоновку ДУС. Ширина провалу (виміряна за рівнем -10 дБ) може бути зменшена з 60° до 28°. Це досягається включенням до схеми другого атенюатора А2, який компенсує нерівномірність всеспрямованої ДН. Схему, що забезпечує зменшення ширини нуля ДН

(додатковий вирівнюючий атенюатор) та розширення ширини робочої смуги частот (підключення узгоджених навантажень 50 Ом), наведено на рисунку 6 [7].

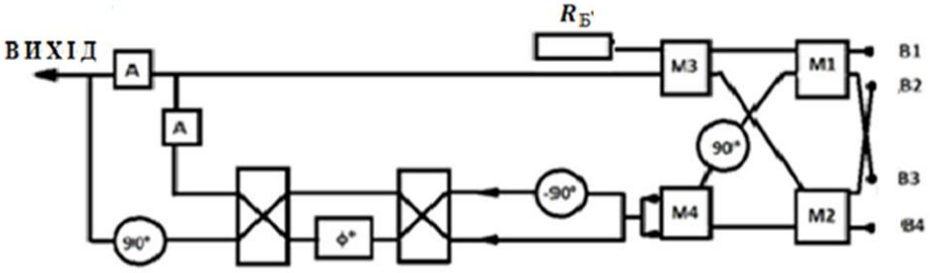


Рис. 6. Широкосмугова функціональна схема компенсатора завад

При максимальному згасанні у атенюаторі А2 схема перетворюється на вид, зображений на рисунку 4, і має такі ж характеристики. Зменшення ширини нуля ДН є причиною зменшення посилення антени для складової ДН з нулем.

Висновки. Незважаючи на те, що КАР призначена для заглушення завади, її виходи можливо також використовувати з автоматичними ланцюгами, які управляють напрямком нуля ДН.

Автори зазначають, що описаний тип решітки можна використовувати як приймальну антену з чутливістю до напрямку приходу хвилі (аналог радіопеленгатора). Для цього до виходів двох мод необхідно підключити входи фазового детектора. Вихід фазового детектора можна калібрувати напрямом кута приходу прийнятої хвилі. Сигнал з виходу фазового детектора може бути використаний для автоматичного або адаптивного управління кутовим положенням нуля ДН. Бажано, щоб на систему керування нулем ДН не впливали вид використовуваної модуляції та умови прийому.

Таким чином, реалізація запропонованої схеми побудови антенної системи у вигляді КАР малого діаметра з просторовою адаптацією відносно напрямку приходу завади дозволить суттєво збільшити завадозахищеність радіостанції у мережах зв’язку з рухомими об’єктами.

Подальші напрямки досліджень передбачають вивчення можливості практичного застосування пропонованого способу підвищення завадозахищеності. Планується провести експериментальні випробування макета КАР з керованим нулем ДН.

Також планується розглянути можливості використання як дискретних 8 (6)-бітних фазообертачів, так й фазообертачів, які можуть бути побудовані за квадратурною схемою з двома електрично керованими атенюаторами в синфазному та квадратурному каналах. Для виключення залежності роботи системи автоматичного формування нуля ДН від використовуваної модуляції та умов прийому корисного сигналу планується використати незамкнуту систему автоматичного управління (без зворотного зв’язку). При цьому до пам’яті контролера (процесора), який управляє атенюаторами і фазообертачем, завчасно вносяться дані щодо співвідношення рівня сигналу на виході фазового детектора від кута приходу сигналу завади. У пам’яті також зберігаються докладні характеристики пристрою для забезпечення лінійності і компенсації частотної залежності ослаблення. Пристрій, що планується розробити, також повинен врахувати помилки вибірки даних у присутності корисного та завадового сигналів при різних співвідношеннях їхніх потужностей та різних співвідношеннях кутів приходу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Борисов І. В., Гурський Т. Г., Ільїнов М. Д., Гриценок К. М. Підвищення ефективності функціонування систем радіозв’язку за рахунок використання адаптивних антенних решіток // Збірник наукових праць ВІТІ. 2015. № 1. С. 16–24.

2. Гриценюк К. М., Гурський Т. Г. Методика формування діаграми спрямованості кільцевої антенної решітки радіостанції мобільної радіомережі в умовах навмисних завад // Збірник наукових праць ВІТІ. 2018. № 3. С. 6–16.

3. Боголій С. М., Гурський Т. Г., Макарчук В. І., Хижий О. І. Підвищення завадозахищеності мобільних радіомереж з використанням технології адаптивного діаграмоутворення // Збірник наукових праць ВІТІ. 2022. № 2 (2). С. 5–14.

4. Davies D.E.N., Rizk M.S.A.S. A broadband experimental null-steering antenna system for mobile communications. Proc/ IERE? 1978, Vol. 48, № 10.

5. Davies D.E.N., Rizk M.S.A.S. A small radius circular array antenna with 3600 null-steering capability/ - Int/ Conf/ Antennas and Propag., London, 1978, p. 60–64.

6. Rahim T., Guy J.R.F., Davies D.E.N. A wideband UHF circular array. – Proceeding of IEE Antennas and Propagation Conference, York, 1981, 13–16 April.

7. Ломан В. И., Нестеренко И. К. Поляризационный компенсатор помех // Известия. вузов. Радиоэлектроника. Том 28. № 3. 1985. С. 59–61.

DOI: 10.58254/viti.3.2023.03.21

УДК 004.9

канд. техн. наук Іляш Ю. Ю. ORCID: 0009-0006-5786-7205
(Прикарпатський національний університет ім. Василя Стефаника)

ІМПЛЕМЕНТАЦІЯ СИСТЕМИ ДІАГНОСТИКИ СКЛАДНОСТІ ПАРОЛЯ

Системи діагностики паролів стають все більш актуальними в сучасному світі в зв'язку з ростом кількості інтернет-сервісів та потреби у захисті особистих даних. Діагностика складності пароля дозволяє оцінити стійкість пароля до різних видів атак, що включають брутфорс, словникові атаки та інші методи.

У роботі розроблено систему перевірки складності пароля, яка дозволяє врахувати нові підходи до формування унікальності вибраної послідовності символів на противагу стандартним методам, які використовуються в найпоширеніших системах генерування паролів, таких як довжина, наявність спецсимволів і цифр, використання великих і малих літер. У роботі пропонується здійснювати перевірку на наявність повторень та збігів з найтиповішими паролями, для чого до розробленої системи підключено базу даних на 10 000 паролів.

Для пришвидшення перевірки на збіги використано алгоритм відстані Левенштейна. Алгоритм Левенштейна працює за допомогою динамічного програмування. Він розглядає два рядки, які мають бути порівняні, і створює матрицю, яка показує мінімальну кількість редагувальних операцій, необхідних для перетворення одного рядка в інший. Дана реалізація дозволила отримати більшу швидкодію генерування порівняно з існуючими системами. У роботі детально прописані алгоритми роботи всіх основних етапів перевірки пароля на складність та запропонована кодова реалізація мовою Javascript. Алгоритм Левенштейна може бути корисним для визначення подібності текстів або для пошуку можливих правильних варіантів неправильно написаних слів. Також, його можна використовувати для реалізації автозаповнення в програмах, які використовують введення користувача.

Реалізована система може бути інтегрована в багато різних програм та вебсервісів для автоматичного визначення складності пароля, що дозволяє використовувати її в різних областях, таких як банківська сфера, медичні сервіси та інші. В результаті роботи над проектом було підтверджено, що використання системи діагностики складності пароля може значно зменшити ризик несанкціонованого доступу до систем, що містять важливу конфіденційну інформацію.

Ключові слова: *алгоритм Левенштейна, генерування пароля, складність пароля, брутфорс.*

Y. Iliash Implementation of the password complexity diagnostic system.

Password diagnostic systems are becoming increasingly relevant in the modern world due to the growth of internet services and the need to protect personal data. Evaluating password complexity allows for assessing the strength of passwords against different types of attacks, including brute force, dictionary attacks, and other methods.

In this work, a system for checking password complexity was developed, which takes into account new approaches to forming the uniqueness of the selected sequence of characters. As opposed to standard methods used in the most common password generating systems, such as length, the presence of special characters and numbers, and the use of upper and lower case letters, this work proposes to check for repetitions and matches with the most common passwords. For this purpose, a database of 10,000 passwords was connected to the developed system.

To speed up the checking for matches, the Levenshtein distance algorithm was used. The Levenshtein algorithm works using dynamic programming. It considers two strings that need to be compared and creates a matrix that shows the minimum number of editing operations required to transform one string into the other. This implementation allowed for faster password generation compared to existing systems. The work details the algorithms for all the main stages of password complexity checking and proposes code implementation in Javascript.

The Levenshtein algorithm can be useful for determining text similarity or searching for possible correct variants of misspelled words. It can also be used for implementing autocomplete in programs that use user input.

The implemented system can be integrated into many different programs and web services for automatic password complexity determination, allowing for its use in various areas such as banking, medical services, and others. As a result of work on this project, it has been confirmed that using a password complexity diagnostic system can significantly reduce the risk of unauthorized access to systems containing important confidential information.

Keywords: *levenstein algorithm, password generation, password complexity, brute force*.

Постановка проблеми. Створення пароля високої складності – це досить складна задача. Через високу обчислювальну потужність сучасних комп'ютерів підбір паролів стає значно простішим. З метою безпеки краще використовувати паролі, які будуть складнішими для підбору системами брутфорсу.

У сучасному медійному та мобільному світі розробка нових алгоритмів передбачає візуалізацію досліджень, створення інтерфейсу користувача. Тому не менш важливим

завданням є створення вебсайту, на якому можна буде перевірити свій пароль на складність та отримати поради щодо його покращення.

Завдяки розробленим алгоритмам можна отримати дані про складність паролів та збільшити рівень безпеки користування вебсервісами. Створений алгоритм може порівнювати введені паролі на схожість із паролями, які внесені в його базу паролів, стандартні системи не роблять такої валідації.

Реалізована система допомагатиме створювати складніші паролі, що знизить ризик злому акаунтів та втрати даних.

Аналіз публікацій за темою дослідження.

Велику увагу безпеці даних приділяють в медичній сфері, забезпечуючи віддалений доступ і перевірку стану здоров'я пацієнтів у будь-який час і в будь-якому місці. У таких випадках важливі системи генерування надійного пароля, щоб дані не були викрадені зловмисниками [1; 2]. На сучасному етапі розвитку систем захисту та безпеки значну увагу приділяють так званим ботнетам, які стали основною загрозою для інфраструктури на основі Інтернету речей, націлених на такі вразливості програмного забезпечення, як слабкі паролі або паролі за замовчуванням, щоб зібрати армію скомпрометованих пристроїв, які можуть служити смертоносною кіберзброєю проти цільових систем, мереж і служб. У статтях описують шляхи та зусилля щодо пом'якшення цієї проблеми шляхом розробки системи виявлення вторгнень, яка знаходиться всередині пристроїв Інтернету речей, щоб забезпечити покращену видимість, таким чином досягаючи посилення безпеки таких пристроїв [3; 4].

Проте описані дослідження стосуються вже внутрішніх аспектів систем зберігання даних, неналежна увага приділяється до первинного етапу реєстрації користувачів, та вибір способів захисту даних, зокрема рівень складності пароля до кабінету, акаунту, емейла. Високий рівень складності пароля, вже може на первинному етапі відсікти левову частку зловмисників, або, принаймні, суттєво збільшити час на підбір ключів.

Метою статті є розробка шляхів імплементації системи діагностики складності пароля для зменшення ризику несанкціонованого доступу до систем, що містять важливу конфіденційну інформацію.

Виклад основного матеріалу.

Аналіз задачі та реалізація алгоритмів. Після аналізу систем перевірки паролів на різних вебсайтах було встановлено, що приблизно 95 % сайтів використовують прості правила для перевірки складності пароля: якщо є символи від [a-z], [A-Z], [0-9] та [@-$], то пароль вважається складним. Якщо, наприклад, ввести пароль "Password1@", то він без проблем пройде перевірку сайтом, хоча сучасними комп'ютерами такі паролі зламуються дуже легко, але пароль "whait-ready-black-adddsdf" не пройде і вважатиметься слабким, хоча його підібрати набагато складніше. Тому було вирішено створити набір правил та реалізацію вебсайту, що дозволить робити перевірки надійніше і точніше.

Основними критеріями складності пароля визначено:

– довжину. Якщо додати 2 символи до пароля, складність підбору збільшиться в 500 разів (якщо використовуються символи ASCII). Мінімально рекомендована довжина – 8 символів, оптимальна – більше 11;

– наявність спецсимволів і цифр. Не всі системи підбору паролів використовують спецсимволи під час процесу підбору;

– використання як малих, так і великих букв. Це збільшує діапазон символів і на процес підбору потрібно більше часу;

– відсутність повторень символів на кшталт "ааа" та послідовностей цифр за зростанням чи спаданням на кшталт "1234" та "9876";

– відсутність поширених комбінацій на клавіатурі «qwerty» та «asdfgh»;

– відсутність повторів та стандартних слів "Pass","Password" та інших. Повтори полегшують процес підбору, а стандартні слова внесені в бази паролів систем для брутфорсу.

Використовуючи дані критерії, було створено алгоритм перевірки складності пароля. Його створення було розділено на декілька етапів. Алгоритм було реалізовано методами мови програмування JavaScript. Першим етапом було створення перевірки на довжину.

```
<script type="text/javascript" >
  var strength;
  var pass;
  addEventListener('keydown', function checkpass(){
     strength = 100;
     pass = document.getElementById('password').value;
     if (pass.length < 8) {
        strength -= 90;
     }
     else
     if (pass.length >= 8 && pass.length < 12)
        strength += pass.length;
     else
        strength += pass.length * 5;
  });
</script>
```

У цьому скрипті створено змінну strength, яка буде змінювати своє значення залежно від довжини пароля. Якщо пароль менше 8 символів, її значення буде дорівнювати 10. Якщо від 8 до 11, значення буде дорівнювати 100 + довжина пароля, а якщо більше 12, її значення буде дорівнювати 100 + довжина пароля, помножена на 2.

Ці значення були обрані через те, що паролі до 8 символів підбираються методом брутфорсу до 3 днів, а з кожним наступним символом складність підбору зростає в 256 разів, якщо використовується кодування символів ASCII. При довжині пароля більше 11 символів комп’ютерам стає складніше підбирати паролі, тому що кількість можливих комбінацій зростає у 256 разів з кожним додатковим значенням і обчислювальна потужність сучасних комп’ютерів може бути недостатньою. Наприклад, сильний пароль на 14 символів звичайний комп’ютер може підбирати декілька трильйонів років. Функція checkpass() викликається при натисканні користувачем будь-якої клавіші. Вибір саме такого способу її виклику зумовлений тим, що набагато зручніше просто вводити пароль в текстове поле вебсторінки і він буде перевірятися в реальному часі, ніж вводити пароль на натискати кнопку “перевірити”.

Наступним кроком була реалізована перевірка на наявність великих і малих букв, цифр і спецсимволів у паролі.

```
<script type="text/javascript" >
   var strength;
   var pass;
   var s_letters = "qwertyuiopasdfghjklzxcvbnm";
   var c_letters = "QWERTYUIOPLKJHGFDSAZXCVBNM";
   var numbers = "0123456789";
   var special = "!@#$%^&*()_-+=\|/.,:;[]{}";
   var check_s = false;
   var check_c = false;
   var check_n = false;
   var check_sp = false;
   addEventListener('keydown', function checkpass(){
      strength = 100;
      pass = document.getElementById('password').value;
      if (pass.length < 8) {
         strength -= 90;
```

```
        }
        else
        if (pass.length >= 8 && pass.length < 12)
          strength += pass.length;
        else
          strength += pass.length * 5;
        pass = pass.split('');
        for (let i = 0; i < pass.length; i++) {
          if (!check_s && s_letters.indexOf(pass[i]) !== -1) {
            check_s = true;
            strength += 50;
          }
          else if (!check_c && c_letters.indexOf(pass[i]) !== -1){
            check_c = true;
            strength += 50;
          }
          else if (!check_n && numbers.indexOf(pass[i]) !== -1){
            check_n = true;
            strength += 50;
          }
          else if (!check_sp && special.indexOf(pass[i]) !== -1){
            check_sp = true;
            strength += 50;
          }
        }
      });
    </script>
```

Після доповнення даний скрипт отримав змінні s_letters, c_letters, numbers, special, в яких зберігаються малі і великі букви, числа і спецсимволи, які можна використовувати в паролях на будь-яких вебресурсах, та змінні check_s, check_c, check_n та check_sp, які зберігають значення результатів перевірки на наявність малих і великих літер, чисел і спецсимволів. Перевірка відбувається за допомогою циклу. Перед циклом змінна pass, що містить пароль, розбивається на окремі символи, після чого в тілі циклу кожен символ порівнюється із набором символів зі змінних, які були ініціалізовані раніше. Після перевірки значення змінних check_s, check_c, check_n та check_sp встановлюється true, якщо перевірку було пройдено, або false, якщо перевірку не було пройдено. Також за кожну пройдену перевірку до змінної strength додається 50.

Наступним кроком було реалізовано перевірку на повтори трьох і більше символів.

```
<script type="text/javascript" >
    var strength;
    var pass;
    var s_letters = "qwertyuiopasdfghjklzxcvbnm";
    var c_letters = "QWERTYUIOPLKJHGFDSAZXCVBNM";
    var numbers = "0123456789";
    var special = "!@#$%^&*()_-+=\|/.,:;[]{}";
    var check_s = false;
    var check_c = false;
    var check_n = false;
    var check_sp = false;
    var repeated = 0;
    addEventListener('keydown', function checkpass(){
      strength = 100;
```

```
        pass = document.getElementById('password').value;
        if (pass.length < 8) {
          strength -= 90;
        }
        else
        if (pass.length >= 8 && pass.length < 12)
          strength += pass.length;
        else
          strength += pass.length * 5;
        pass = pass.split('');
        for (let i = 0; i < pass.length; i++) {
          if (!check_s && s_letters.indexOf(pass[i]) !== -1) {
            check_s = true;
            strength += 50;
          }
          else if (!check_c && c_letters.indexOf(pass[i]) !== -1){
            check_c = true;
            strength += 50;
          }
          else if (!check_n && numbers.indexOf(pass[i]) !== -1){
            check_n = true;
            strength += 50;
          }
          else if (!check_sp && special.indexOf(pass[i]) !== -1){
            check_sp = true;
            strength += 50;
          }
          if (pass[i]===pass[i-1]){
            repeated++;
          }
          else
            repeated=0;
          if (repeated >= 3){
            strength-=50;
          }
        }
      });
    </script>
```

Для реалізації цієї перевірки було створено змінну repeated. Перевірка відбувається в циклі. Якщо даний символ рівний попередньому, то значення змінної росте. Якщо значення змінної repeated більше або дорівнює 3, то від значення змінної strength віднімається 30.

Наступним кроком була реалізована перевірка на послідовності по зростанню та спаданню, стандартні слова та комбінації на клавіатурі. Для того щоб спростити цей процес, було вирішено створити базу паролів, в якій збережено стандартні послідовності та слова. Вона буде зберігатися в файлі формату .json та імопортуватися в головний скрипт. Для спрощення створення даної бази було використано дані Марка Бернета зі статті "10,000 Top Passwords" [3].

```
<script type ="text/Javascript>
import {passes} from "./passes.json"
passes = passes.split('\n');

function levenshtein(s1, s2, costs) {
```

```
    var i, j, l1, l2, flip, ch, chl, ii, ii2, cost, cutHalf;
    l1 = s1.length;
    l2 = s2.length;
    costs = costs || {};
    var cr = costs.replace || 1;
    var cri = costs.replaceCase || costs.replace || 1;
    var ci = costs.insert || 1;
    var cd = costs.remove || 1;
    cutHalf = flip = Math.max(l1, l2);
    var minCost = Math.min(cd, ci, cr);
    var minD = Math.max(minCost, (l1 - l2) * cd);
    var minI = Math.max(minCost, (l2 - l1) * ci);
    var buf = new Array((cutHalf * 2) - 1);
    for (i = 0; i <= l2; ++i) {
        buf[i] = i * minD;
    }
    for (i = 0; i < l1; ++i, flip = cutHalf - flip) {
        ch = s1[i];
        chl = ch.toLowerCase();
        buf[flip] = (i + 1) * minI;
        ii = flip;
        ii2 = cutHalf - flip;
        for (j = 0; j < l2; ++j, ++ii, ++ii2) {
            cost = (ch === s2[j] ? 0 : (chl === s2[j].toLowerCase()) ? cri : cr);
            buf[ii + 1] = Math.min(buf[ii2 + 1] + cd, buf[ii] + ci, buf[ii2] + cost);
        }
    }
    return buf[l2 + cutHalf - flip];
}
var strength, length_of, pass, s_letters = "qwertyuiopasdfghjklzxcvbnm",
    c_letters = "QWERTYUIOPLKJHGFDSAZXCVBNM", numbers = "0123456789",
    special = "!@#$%^&*()_-+=\|/.,:;[]{}", check_s, check_c,
    check_n, check_sp, st_use, pass_ch, repeated = 0;
addEventListener('keydown', function checkpass(){
    pass = document.getElementById('password').value;
    strength = 100;
    length_of = pass.length;
    check_s = false; check_c = false;
    check_n = false; check_sp = false; st_use = false;
    if (pass.length < 8) {
        strength -= 90;
    }
    else
    if  (pass.length >= 8 && pass.length < 12)
        strength += pass.length;
    else
        strength += pass.length * 5;
    pass = pass.split('');
    for (let i = 0; i < pass.length; i++) {
        if (!check_s && s_letters.indexOf(pass[i]) !== -1) {
            check_s = true;
            strength += 50;
```

```
        }
        else if (!check_c && c_letters.indexOf(pass[i]) !== -1){
            check_c = true;
            strength += 50;
        }
        else if (!check_n && numbers.indexOf(pass[i]) !== -1){
            check_n = true;
            strength += 50;
        }
        else if (!check_sp && special.indexOf(pass[i]) !== -1){
            check_sp = true;
            strength += 50;
        }
        if (pass[i]===pass[i-1]){
            repeated++;
        }
        else
            repeated=0;
        if (repeated >= 3){
            strength-=30;
        }
    }
        for(let j = 0; j < passes.length; j++)
        if (levenshtein(pass,passes[j].split('')) < pass.length - 3) {
            st_use = true;
            strength = -60;
            break;
    }
    console.log(st_use);
});
</script>
```

Для перевірки схожості пароля з паролями з бази було реалізовано функцію алгоритму відстані Левенштейна [1; 2]. За допомогою цього алгоритму пароль порівнюється із паролями з бази.

Після рефакторингу коду було отримано скрипт, який повністю підходить для перевірки паролів на складність. Переваги даного скрипту над скриптами, які використовуються для тестування паролів на інших вебплатформах:

точність;

можливість тонкої настройки;

ефективність роботи;

швидкодія (порівняно з методом Монте-Карло).

Розробка інтерфейсу

Після завершення роботи над алгоритмом було створено простий односторінковий сайт для демонстрації його роботи. Першим етапом було створення HTML-документа та його наповнення.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>PassCheck</title>
    <link rel="stylesheet" href="css/index.css">
```

```
    <link rel="script" href="js/checker.js">
    <link rel="preconnect" href="https://fonts.gstatic.com">
    <link href="https://fonts.googleapis.com/css2?family=Mukta&display=swap" rel="stylesheet">
</head>
<body>
    <h1 class="header">Перевірте Ваш пароль</h1>
    <label for="password"></label><input id="password" type="password" placeholder="Введіть пароль" value=""><br>

    <script type="text/javascript" src="js/checker.js"></script><br>
    <div id="pi" class="progressbar" hidden>
      <div id="bard" class="bar">
        <br>
      </div>
    </div>
    <p id ="Funny"></p>

</body>
</html>
```

В результаті було отримано ось таку сторінку (рис. 1):

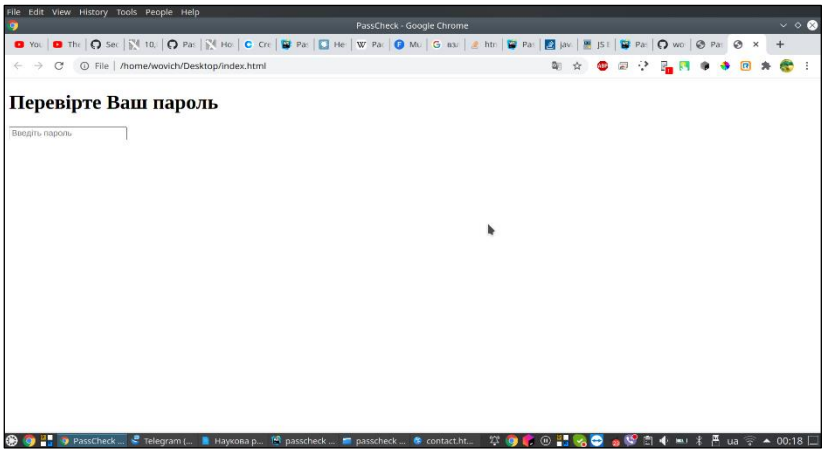


Рис. 1. Загальний вигляд сторінки

Після створення HTML-документа та написання коду сторінки було створено CSS-документ.

```
body{
    background-color: #093824;
    text-align: center;
    margin: 0;
    font-family: Mukta,Serif;
}

.header {
    color: #78FECF;
    margin: 35px 0 45px 0;
    padding: 30px 0px 10px 0px;
    font-size: 55px;
}
#Funny{
```

```
    color: #78FECF;
    font-size: 16px;
}

#password{
    background-color: #78FECF;
    text-align: center;
    font-size: 45px;
    width: 100%;
    padding: 50px 0px 60px 0px;
    outline: none;
    border: none;
}

#password::placeholder{
    color: #093824;
    caret-color : #78FECF;
}
#password:active, #password :hover,#password :focus {
    outline: none;
    border: none;
    caret-color : #093824;
    color: #093824;

}
.progressbar{
    background-color: #C6CCB2;
    padding: 5px 10px;
    width:480px;
    margin: auto;
    border-radius: 15px;
}

#bard{
    background-color: #BF4E30;
    max-width: 480px;
    border-radius: 15px;
}
```

В результаті сайт набув презентабельного вигляду (рис. 2).

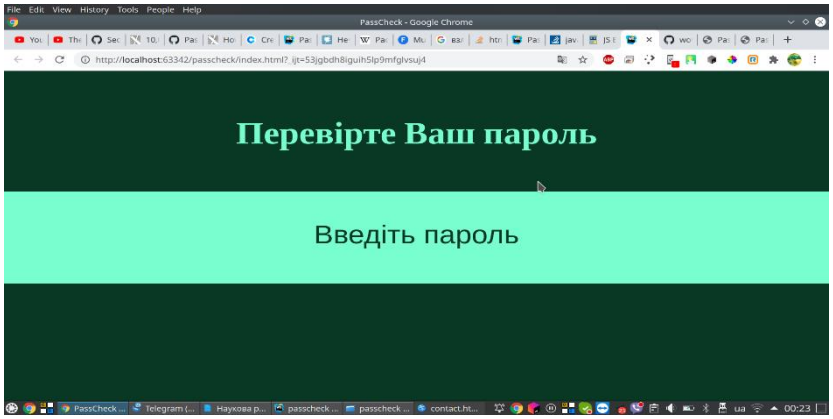


Рис. 2. Вигляд сторінки тестування

Наприкінці роботи до вебсайту було підключено алгоритм перевірки паролів на складність. Після завершення роботи над вебсайтом було виконано повний цикл тестування (рис. 3, 4).

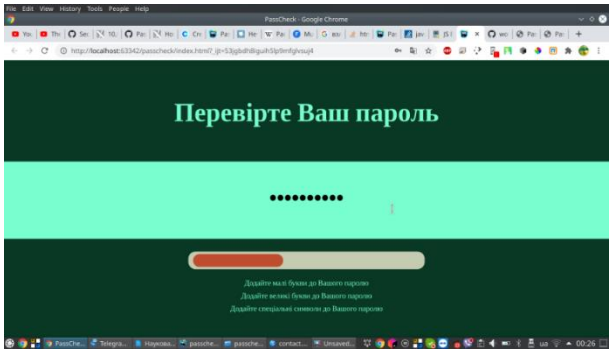


Рис. 3. Перевірка пароля

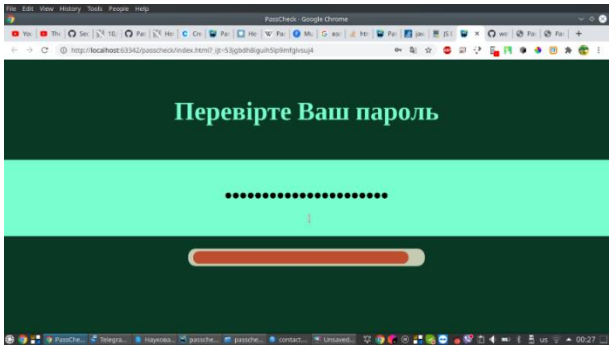


Рис. 4. Результат перевірки пароля

Висновки. Після аналізу проблем, пошуку та опрацювання інформації було отримано надійний алгоритм перевірки паролів на надійність та створено вебсайт, на якому можна отримати інформацію про надійність свого пароля та поради щодо його покращення. Алгоритм, що є результатом даного дослідження, має такі переваги над іншими:

вища точність;

можливість тонкої настройки за допомогою зміни коефіцієнтів;

швидкість роботи (порівняно з методом Монте-Карло) та легкість підключення до існуючого сайту;

перевірка пароля на схожість із паролями з підключеної бази.

Завдяки цьому можливо збільшити рівень безпеки користуванням мережею Інтернет та знизити ризик втрати даних чи крадіжки особистої інформації. Також через можливість доповнення чи заміни бази паролів та корегування коефіцієнтів даний алгоритм більш зручний і ефективний, ніж алгоритми інших сайтів чи вебплатформ.

Подальші напрямки досліджень даної тематики слід сконцентрувати на розробках інноваційних методів створення паролів, зокрема вивченні нових підходів до створення паролів, які були б інтуїтивно зрозумілі, легкі для запам’ятовування та міцні з точки зору криптографічних вимог. Важливим аспектом в будь-яких сучасних дослідженнях є використання машинного навчання та штучного інтелекту, зокрема використання алгоритмів машинного навчання для аналізу та класифікації паролів з метою виявлення слабких та вразливих варіантів.

Не менш важливим напрямком є дослідження поведінкової аналітики користувачів, зокрема аналіз звичок користувачів та їхніх підходів до створення паролів для виявлення шаблонів та слабких місць, які можуть бути використані зловмисниками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wagner R. A., Fischer M. J. The string-to-string correction problem // Journal of the ACM. Volume 21. Issue 1. Pp. 168–173. January 01, 1974. URL: https://doi.org/10.1145/321796.321811.

2. Левенштейн В. И. Двоичные коды с исправлением выпадений, вставок и замещений символов // Докл. АН СССР. 1965. Т. 163. № 4. С. 845–848.

3. Bruce Schneier. Snakeoil: Warning Sign #5: Ridiculous key lengths» // Schneier on Security. February 15, 1999. URL: https://www.schneier.com/crypto-gram/archives/1999/0215.html.

4. Burnett Mark. 10,000 Top Passwords // Medium. URL: https://xato.net/10-000-top-passwords-6d6380716fe0.

5. Справочник по HTML // HTMLBOOK: веб-сайт. URL: http://htmlbook.ru/html.

DOI: 10.58254/viti.3.2023.04.31

УДК.621.39

канд. техн. наук Коваленко І. Г. ORCID: 0000-0002-6827-5196 (ВІТІ ім. Героїв Крут)
канд. техн. наук Масесов М. О. ORCID: 0000-0003-4537-4295 (ВІТІ ім. Героїв Крут)
Драглюк О. В. ORCID: 0000-0001-8572-7257 (ВІТІ ім. Героїв Крут)
канд. техн. наук Ткаченко А. Л. ORCID: 0000-0002-9789-8536 (ВІТІ ім. Героїв Крут)

МЕТОДИКА ПОБУДОВИ РАДІОРЕЛЕЙНИХ ЛІНІЙ НА ОСНОВІ ВИКОРИСТАННЯ ГЕОПРОСТОРОВОЇ ІНФОРМАЦІЇ

При плануванні та організації зв'язку з використанням сучасних військових цифрових радіозасобів важливим та актуальним завданням є забезпечення максимально можливої дальності зв'язку при забезпеченні необхідної швидкості передачі інформації із заданою якістю. З-поміж основних чинників, які визначають можливу дальність зв'язку сучасних військових цифрових радіозасобів, крім їхніх характеристик, є рельєф місцевості, забудова та рослинність. Крім того, для організації радіорелейного зв'язку можуть використовуватися існуючі висотні об'єкти на місцевості (зокрема вежі операторів зв'язку).

Проведений аналіз показав, що існуючі методики та спеціалізоване програмне забезпечення може використовуватись для окремих розрахунків рівнів сигналів, що розповсюджуються, проте не завжди дозволяють врахувати всі необхідні технічні параметри радіозасобів та додаткову вихідну геопросторову інформацію. А головне існуюче програмне забезпечення не призначено для побудови багатоінтервальних радіорелейних ліній з урахуванням додаткових геопросторових даних. При побудові радіорелейних ліній часто складується ситуація, коли один інтервал не може забезпечити зв'язок із заданою якістю. Тоді постає задача планування радіорелейної лінії з використанням станцій-ретрансляторів. Вибір місця розташування ретрансляторів залежить від багатьох чинників: можливості встановлення зв'язку, мінімізації кількості ретрансляцій, геопросторової інформації щодо рельєфу місцевості та наявності в місті встановлення відповідної інфраструктури (забудов, електроживлення, точок прив'язки, веж тощо).

У статті запропонована методика побудови радіорелейних ліній зв'язку на основі розрахунків рівнів сигналів з урахуванням геопросторових даних, яка дозволяє аналізувати окремі радіорелейні інтервали для побудови багатоінтервальних радіорелейних ліній. Програмна реалізація розробленої методики дозволяє створити програмне забезпечення розрахунку радіорелейних ліній з урахуванням необхідних вихідних даних та геопросторової інформації щодо місцевості.

Ключові слова: *рівняння радіолінії, умови здійснення радіозв'язку, втрати у вільному просторі, енергетичний запас, технічні характеристики радіозасобів.*

I. Kovalenko, M. Masesov, O. Draglyuk, A. Tkachenko Methodology for building radio relay lines based on the use of geospatial information.

When planning and organizing communication using modern military digital radios, a crucial and relevant task is to ensure the maximum possible communication range while providing the necessary speed and quality of information transmission. The main factors determining the possible communication range of modern military digital radios, in addition to their characteristics, are the terrain relief, buildings, and vegetation. Additionally, existing height objects in the area, such as communication operator towers, can be used to organize radio relay communication.

An analysis showed that existing methods and specialized software can be used for certain calculations of signal levels, but they do not always take into account all necessary technical parameters of radio equipment and additional geospatial information. Moreover, the existing software is not designed to construct multi-interval radio relay lines while considering additional geospatial data. In constructing radio relay lines, there is often a situation where one interval cannot provide communication with the required quality. This situation calls for planning a radio relay line using relay stations. The choice of the location of relay stations depends on many factors, including the possibility of establishing communication, minimizing the number of relays, geospatial information regarding the terrain relief, and the presence of the necessary infrastructure (buildings, power supply, anchor points, towers, etc.) in the area.

The article proposes a methodology for constructing radio relay communication lines based on calculations of signal levels while considering geospatial data. This methodology allows analyzing individual radio relay intervals for constructing multi-interval radio relay lines. The software implementation of the developed methodology allows creating software for calculating radio relay lines with the necessary input data and geospatial information regarding the terrain.

Keywords: *radio line equation, conditions of radio communication, losses in free space, energy reserve, technical characteristics of radio equipment.*

Постановка завдання. На сьогодні для організації радіорелейного зв’язку та широкосмугових ліній прив’язки використовуються як прийняті на озброєння засоби військового призначення (Р-414МУ, Р-425, Р-402), так і комерційні вироби широкосмугового радіодоступу (виробництва компаній Ubiquiti, MikroTik, D-Link, TP-Link тощо) з направленими антенами. Також країнами-партнерами надаються окремі засоби радіорелейного та тропосферного зв’язку.

При плануванні та організації зв’язку з використанням сучасних військових цифрових радіозасобів важливим та актуальним завданням є забезпечення максимально можливої дальності зв’язку при забезпеченні необхідної швидкості передачі інформації із заданою якістю. Сучасні засоби – радіорелейні станції (РРС) та засоби широкосмугового радіодоступу – підтримують декілька режимів роботи, які можуть відрізнятися шириною смуги каналу, видом модуляції, схемою завадостійкого кодування, потужністю передавача, чутливістю приймача та іншими параметрами. Крім цього, можуть використовуватися антени з різними значеннями коефіцієнта підсилення; висота підвісу антен також може бути різною. Залежно від необхідної швидкості передачі та, відповідно, інших параметрів радіолінії, дальність зв’язку може коливатися у широких межах. З-поміж основних чинників, які визначають можливу дальність зв’язку, крім характеристик радіозасобів, є рельєф місцевості, забудова та рослинність. Також суттєво впливають інші чинники: опади, атмосферні явища тощо. Крім того, для організації радіорелейного зв’язку може використовуватися додаткова геопросторова інформація, зокрема щодо висотних об’єктів на місцевості (споруди, вежі Концерну радіомовлення, радіозв’язку та телебачення (КРРТ) та інших операторів зв’язку).

Очевидно, що розрахунок рівнів сигналів, що передаються, з урахуванням вказаних вище чинників, в умовах обмеження кількості і якості вихідних даних (рельєфу місцевості, забудови, рослинності, погодних умов тощо) розв’язати можна, як правило, тільки наближено. Проте навіть приблизний розрахунок є доцільним на етапі планування ліній та мереж зв’язку.

Для вирішення задач планування радіорелейних ліній (РРЛ) доцільно використовувати відповідне програмне забезпечення (ПЗ) на основі розроблених методик розрахунків та додаткових геопросторових даних (розташування веж КРРТ, операторів зв’язку та інших висотних об’єктів).

Існуюче спеціалізоване ПЗ, що призначене для розрахунку напруженості поля в точці прийому для окремих радіорелейних інтервалів, зокрема „Radio Mobile”, „Radio Works”, „Radio Planner”, „CRC-COVWEB” та ін., може використовуватись для окремих розрахунків рівнів сигналів, що розповсюджуються, проте його використання не регламентоване керівними документами з організації зв’язку, не завжди дозволяє врахувати всі необхідні технічні параметри радіозасобів та додаткової вихідної геопросторової інформації [1]. А головне існуюче ПЗ орієнтовано на розрахунки рівнів сигналів для окремих радіоелектронних засобів (радіорелейних інтервалів) і не призначено для побудови багатоінтервальних РРЛ.

Тому постає задача розробки методик та алгоритмів побудови й розрахунку РРЛ з використанням геопросторової інформації, що дозволить розробити відповідне ПЗ для їх планування.

Аналіз публікацій за темою дослідження. Проведений аналіз показав, що існуючі методики та ПЗ для визначення можливості забезпечення зв’язку між кореспондентами із заданими координатами вирішують задачу з розрахунку рівня сигналу на вході приймача P_2, що являє собою рівняння радіолінії (1) [1–3]:

$$P_2, \text{дБ} = P_1 + G_1 + G_2 - L_{ф1} - L_{ф2} - L_0 - L_{сер} - W_з, \quad (1)$$

де P_1 – потужність сигналу на виході передавача;

G_1, G_2 – коефіцієнти підсилення передавальної та приймальної антен відповідно;

$L_{ф1}$, $L_{ф2}$ – втрати у антенно-фідерних трактах на передачі та прийомі відповідно;

L_0 – основні втрати радіолінії (втрати у вільному просторі);

$L_{сер}$ – втрати, які визначають вплив реального середовища на розповсюдження радіохвиль (так званий множник ослаблення);

$W_з$ – енергетичний запас, який необхідний для компенсації втрат сигналу на прийомі через низку несприятливих факторів, які призводять до зменшення дальності зв’язку (температурний дрейф чутливості приймача і вихідної потужності передавача, атмосферні явища (туман, сніг, дощ), неузгодженість антени, приймача, передавача з антенно-фідерним трактом та ін.). При проведенні розрахунків енергетичний запас ($W_з$) у системах радіозв’язку зазвичай приймається рівним 10–15 дБ [4].

Втрати у вільному просторі визначаються з виразу (2):

$$L_0 = 10\lg\left(\frac{4\pi R}{\lambda}\right)^2, \quad (2)$$

де R – відстань між радіостанціями;

λ – довжина хвилі.

На підставі виразу (1) можуть бути розраховані радіолінії всіх видів. Відмінність полягає у методиці розрахунку множника ослаблення радіосигналів $L_{сер}$ для різних типів радіоліній.

Умови здійснення радіозв’язку. Для здійснення радіозв’язку необхідне дотримання наступних умов [2; 3]:

1) розраховане за формулою (1) значення P_2 повинне перевищувати чутливість приймача $P_ч$:

$$P_2, \text{ дБ} \geq P_ч; \quad (3)$$

2) має бути забезпечене певне перевищення потужності сигналу над потужністю різного роду завад $P_з$ на вході приймача (відношення сигнал/шум (SNR)), що залежить від виду роботи, достовірності і надійності прийому (4):

$$P_2, \text{ дБ} \geq SNR + P_з; \quad (4)$$

3) спотворення сигналу в процесі розповсюдження не повинні перевищувати допустимих норм. Ця умова обмежує смугу частот неспотвореної передачі, тобто швидкість передачі інформації.

З ряду причин потужність завад, а в ряді випадків і потужність сигналу на вході приймача, зазнають безперервних і безладних змін (флуктуацій). Тому у виразах (3), (4) доводиться оперувати середніми значеннями потужностей сигналу і завад (P_2 і $P_з$) і враховувати закони їх статистичного розподілу.

Порядок розрахунку радіорелейних інтервалів без урахування рельєфу місцевості наведено в [1]. При розрахунку втрат, обумовлених загасанням електромагнітного поля за рахунок рельєфу місцевості, а саме дифракції на перешкодах, необхідно використовувати методики, викладені у Рекомендації ITU-R P.526 [5].

Проведений аналіз показав, що існуючі методики та спеціалізоване ПЗ можуть використовуватись для окремих розрахунків рівнів сигналів, що розповсюджуються, проте не завжди дозволяють врахувати всі необхідні технічні параметри радіозасобів та додаткову вихідну геопросторову інформацію. А головне існуюче ПЗ не призначено для побудови багатоінтервальних РРЛ з урахуванням додаткових геопросторових даних. При побудові РРЛ часто складується ситуація, коли один інтервал не може забезпечити зв’язок із заданою якістю. Тоді постає задача планування РРЛ з використанням станцій-ретрансляторів. Вибір місця розташування ретрансляторів залежить від багатьох чинників: можливості встановлення зв’язку, мінімізації кількості ретрансляцій, геопросторової інформації щодо рельєфу місцевості та наявності в місті встановлення відповідної інфраструктури (забудов, електроживлення, точок прив’язки, веж тощо).

Мета статті. Провести аналіз методик розрахунку РРЛ та запропонувати методику побудови радіорелейних ліній зв’язку з використанням геопросторової інформації.

Вихідні дані.

У запропонованій Методиці використовуються такі вихідні дані.

1. РРС з відповідними технічними характеристиками:
– потужність передачі P, дБВт;
– коефіцієнт підсилення антени G, її тип, поляризація випромінювання і втрати в антенно-фідерному тракті η;
– чутливість приймача, дБВт, мВ/м (коефіцієнт шуму, дБ);
– швидкість цифрового потоку, біт/с;
– припустимий рівень помилок і величина захисного відношення для заданого % часу.
2. Смуги частот, які використовуються, f_1-f_n.
3. Характеристики місць розташування початкової та кінцевої РРС:
– географічні координати розташування початкової та кінцевої РРС, широта/довгота;
– висота основи РРС над рівнем моря, м;
– висота підвісу антени над рівнем Землі, м.
4. Характеристики місцевості навколо РРС: висота над рівнем моря (м) та покриття (забудова, вода, рослинність), погодні умови тощо.
5. Додаткова геопросторова інформація щодо забудови, висотних об'єктів на місцевості: розташування/межі (координати), висота (м), додаткові характеристики.

1. Розрахунок радіорелейної лінії зв'язку. Нехай необхідно забезпечити РРЛ між двома пунктами управління з пропускною спроможністю не менше заданої.

При плануванні радіорелейного зв'язку проводиться побудова профілю місцевості з визначенням типу інтервалу (відкритий, напіввідкритий або закритий) та подальший енергетичний розрахунок, кінцевим підсумком якого є визначення надійності зв'язку H [%] (коефіцієнта готовності) [6; 7]. При цьому H [%] = 100 % T [%], де T [%] – *коефіцієнт неготовності*, який визначає відсоток часу (за добу), протягом якого можуть не виконуватися вимоги щодо забезпечення заданої якості зв'язку на інтервалі РРЛ. Вимоги до якості зв'язку для цифрових РРС задаються припустимим значенням ймовірності помилкового прийому інформаційних символів ($P_{пом} = N_{пом}/N_{пер}$, де $N_{пом}$ – кількість помилково прийнятих інформаційних символів; $N_{пер}$ – загальна кількість переданих інформаційних символів).

Для всієї РРЛ T*[%] визначають як суму значень втрат надійності усіх інтервалів, з яких складається РРЛ (5):

$$T^*[\%] = \sum_{i=1}^{M} T_i\ [\%], \qquad (5)$$

де T_i [%] – величина втрат надійності на i-му інтервалі РРЛ;
M – кількість інтервалів РРЛ.

Відповідно до цього надійність зв'язку (коефіцієнт готовності) всієї РРЛ визначається як H* [%] =100 % T*[%].

Методика розрахунку військових польових РРЛ наведена у [6: 7]. Розрахунок стаціонарних РРЛ проводиться на основі рекомендації ITU-R P.530 [8]. Для радіорелейних інтервалів сумарні втрати у середовищі передачі L_Σ визначаються втратами рівня сигналів за рахунок розповсюдження радіохвиль у вільному просторі (L_0), рельєфом місцевості ($L_р$) та рефракційними завмираннями ($L_з$):

$$L_\Sigma = L_0 + L_{сер} = L_0 + L_р + L_з,$$

де L_0 та $L_р$ мають фіксовані значення, а $L_з$ постійно змінюється протягом доби, а його максимально можлива величина враховується у енергетичному запасі $W_з$.

Розрахунок $L_р$ залежить від типу інтервалу. На відкритих інтервалах враховується інтерференція за рахунок відбитого від поверхні землі променю, на напіввідкритих величина втрат залежить від розміру перешкоди, яка потрапляє у зону, суттєву для розповсюдження радіохвиль [6; 7].

Величина надійності зв'язку (коефіцієнта готовності) інтервалу $T_і$ залежить від величини енергетичного запасу $W_з$, який забезпечує необхідну якість зв'язку за заданий відсоток часу роботи РРЛ. Відповідно, для визначення можливості зв'язку необхідно вирішити зворотну (5) задачу – визначення значення необхідного $W_з$ відповідно заданому $T_і = T_\Sigma/n_і$ ($n_і$ – кількість інтервалів) за графіками розподілення завмирань на інтервалах РРЛ

(рис. 1), які отримані шляхом статистичного усереднення експериментальних даних. Графіки на рисунку 1 приведені для найгірших погодних умов протягом року відповідно до метеорологічної статистики для відповідного регіону [6; 7].

Значення параметрів P_1, $L_{ф1}$, $L_{ф2}$, G_1, G_2, $P_ч$ визначаються з технічної документації на РРС. Тоді за формулою (5) можна визначити граничну дальність зв’язку для кожного з можливих режимів роботи, що визначаються шириною смуги та видом модуляції (сигнально-кодової конструкції).

Гранична дальність зв’язку для сучасних військових РРС без урахування рельєфу місцевості розрахована в [1]. Технічні характеристики, необхідні для енергетичного розрахунку, наведені у таблицях 1–3 [9–10]. Значення граничної чутливості приймача в таблицях 2, 3 наведені для $P_{пом} = 10^{-6}$.

Таким чином, можливість забезпечення зв’язку з необхідною пропускною спроможністю між двома заданими точками оцінюється на основі перевірки умови (3). Для цього здійснюється побудова профілю, розрахунок енергетичного запасу та визначення надійності зв’язку на реальному інтервалі.

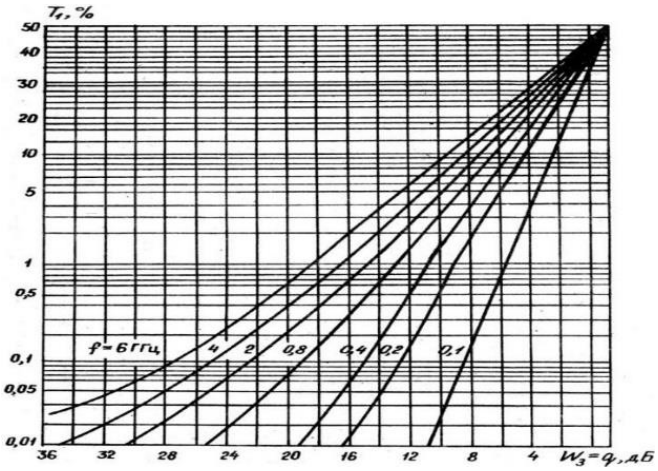


Рис. 1. Графіки залежності коефіцієнта неготовності від енергетичного запасу

Таблиця 1

Значення параметрів РРС, необхідних для енергетичного розрахунку

Характеристика	**Р-425С3**	**Р-402**			
		Р-402.01	**Р-402.02**	**Р-402.03**	**Р-402.04**
Діапазон робочих частот, ГГц	6,43–7,10	4,8–6,75		4,92–6,1	
Потужність передавача, дБм	30	до 29	до 27		
Коефіцієнт підсилення антени, дБі	35	28 направлена, 20 секторна (90°), 16 секторна (120°), 13 всенаправлена			

Таблиця 2

Гранична дальність для різних режимів роботи Р-425С3

Вид модуляції	**Ширина каналу, МГц**								
	7			**14**			**28**		
	***B*, Мбіт/с**	**$P_ч$, дБм**	**$R_{гр}$, км**	***B*, Мбіт/с**	**$P_ч$, дБм**	**$R_{гр}$, км**	***B*, Мбіт/с**	**$P_ч$, дБм**	**$R_{гр}$, км**
QPSK	10	-90 (-89)	192	22	-87 (-86)	136	46	-84 (-83)	96
16QAM	21	-85 (-82)	108	44	-82 (-80)	76	92	-79 (-77)	54
32QAM	26	-82	76	55	-79	54	114	-76	38
64QAM	32	-79 (-76)	54	66	-76	38	137	-73	27
128QAM	37	-76 (-73)	38	77	-73 (-71)	27	160	-70 (-68)	19
256QAM	42	-73	24	87	-70	17	183	-67	12

Примітка: в дужках наведені значення чутливості для режиму адаптивної модуляції.

Таблиця 3

Гранична дальність для різних режимів роботи Р-402

MCS	Вид СКК	Ширина каналу, МГц											
		5			10			20			20–40		
		B, Мбіт/с	$P_ч$, дБм	$R_{гр}$, км	***B***, Мбіт/с	$P_ч$, дБм	$R_{гр}$, км	***B***, Мбіт/с	$P_ч$, дБм	$R_{гр}$, км	***B***, Мбіт/с	$P_ч$, дБм	$R_{гр}$, км
MCS0	BPSK-1/2	1,875	-101	141	3,75	-99	112	7,5	-96	79	15	-93	56
MCS1	QPSK-1/2	3,75	-99	112	7,5	-96	79	15	-93	56	30	-90	40
MCS2	QPSK-3/4	5,625	-96	79	11,25	-93	56	22,5	-90	40	45	-87	28
MCS3	16QAM-1/2	7,5	-93	56	15	-90	40	30	-87	28	60	-84	20
MCS4	16QAM-3/4	11,25	-90	40	22,5	-87	28	45	-84	20	90	-81	14
MCS5	64QAM-2/3	15	-87	28	30	-84	20	60	-81	14	120	-79	11
MCS6	64QAM-3/4	16,875	-84	18	33,75	-81	13	67,5	-79	10	135	-76	7
MCS7	64QAM-5/6	18,75	-83	16	37,5	-80	11	75	-77	8	150	-74	6

Для перевірки виконання умови (4) необхідно, по-перше, знати величину відношення сигнал/шум (ВСШ), необхідного для забезпечення заданої ймовірності помилкового приймання, по-друге, виміряти значення рівнів сигналу та завад на вході приймача.

Необхідні значення ВСШ для багатопозиційних сигналів, що використовуються в РРС Р-425С3, наведено в таблиці 4 [11].

Таблиця 4

Необхідні значення ВСШ для Р-425С3

Вид модуляції	**QPSK**	**16QAM**	**32QAM**	**64QAM**	**128QAM**	**256QAM**
ВСШ, дБ ($P_{пом} = 10^{-5}$)	9,6	14	16,1	18,5	20,9	23,5

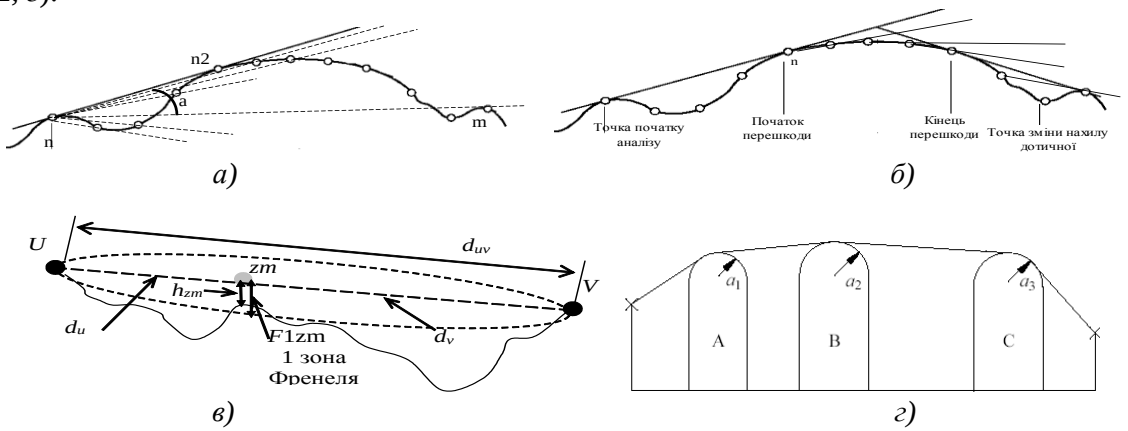
2. Розрахунок послаблень радіосигналів за рахунок розповсюдження радіохвиль з використанням геопросторової інформації щодо рельєфу місцевості. Відповідно до рекомендацій ITU-R P.530, ITU-R P.526 з урахуванням ITU-R P.525 [12], ITU-R P.676 [13], ITU-R P.452 [14] були розроблені алгоритми розрахунків послаблення за рахунок розповсюдження радіохвиль з урахуванням рельєфу місцевості, які включають в себе:

аналіз профілю траси на наявність перешкод (рис. 2, *а*);

аналіз характеристик перешкод (рис. 2, *б*);

розрахунок послаблення на окремому інтервалі розповсюдження радіохвиль з урахуванням перешкод (рис. 2, *в*);

розрахунок загального послаблення на трасі як суми послаблень на перешкодах (рис. 2, *г*).



а) *б)* *в)* *г)*

Рис. 2. Приклади розрахунків послаблення розповсюдження радіохвиль за рахунок наявності перешкод:

а – аналіз профілю траси на наявність перешкод; *б* – аналіз характеристик перешкод; *в* – розрахунок послаблення на окремому інтервалі розповсюдження радіохвиль з урахуванням перешкод; *г* – розрахунок загального послаблення на трасі як суми послаблень на перешкодах

На основі розроблених алгоритмів була розроблена програмна реалізація розрахунку радіорелейних інтервалів (рис. 3), яка дозволяє розрахувати можливість встановлення зв’язку для окремого інтервалу для обраних характеристик РРС та заданої якості зв’язку (чутливість відповідно до режимів роботи та захисне відношення) (рис. 4).

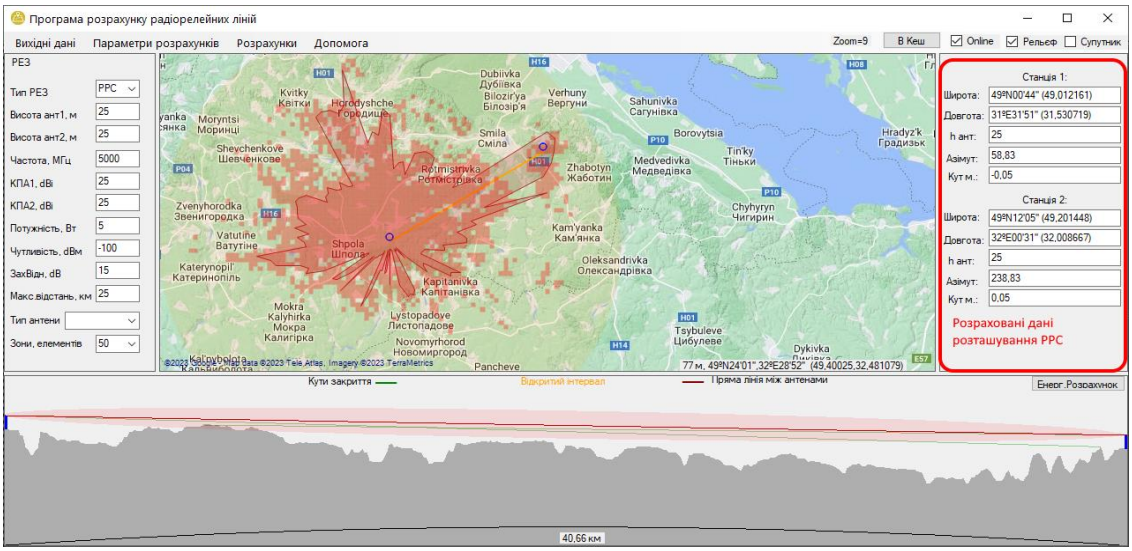


Рис. 3. Приклад розрахунку радіорелейного інтервалу

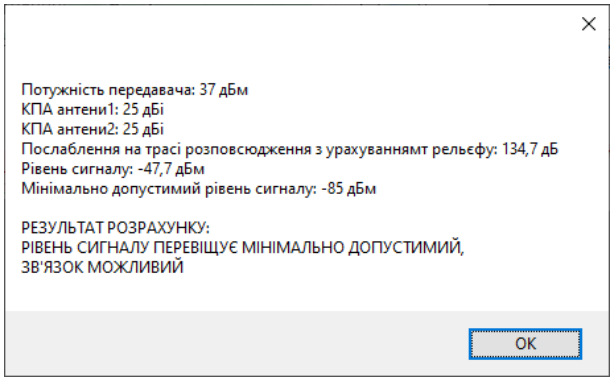


Рис. 4. Результат енергетичного розрахунку радіорелейного інтервалу

3. Методика побудови РРЛ з використанням геопросторової інформації.

При побудові РРЛ часто виникає ситуація, коли один інтервал не може забезпечити зв’язок із заданою якістю. Тоді постає задача планування РРЛ з використанням станцій-ретрансляторів. Вибір місця розташування ретрансляторів залежить від багатьох чинників: можливості встановлення зв’язку, мінімізації кількості ретрансляцій, геопросторової інформації щодо рельєфу місцевості та наявності в місті встановлення відповідної інфраструктури (забудов, електроживлення, точок прив’язки, веж тощо). Тому для побудови РРЛ пропонується наступна методика та відповідний алгоритм (рис. 5).

Суть методики – послідовна побудова зон можливого розташування взаємодіючих станцій (інтервалу) та пошук близького до оптимального розташування антен РРС для побудови багатоінтервальної РРЛ з використанням геопросторових даних.

Етапи методики:

1. Визначення місця розташування антени початкової РРС . При визначенні початкової точки аналізується додаткова геопросторова інформація щодо рельєфу, наявності забудов, веж та інших висотних об’єктів в зоні досяжності проводових засобів зв’язку для максимального підняття антени.

2. В межах граничного радіусу можливої дальності зв’язку (табл. 2, 3) проводиться розрахунок зони можливого розташування взаємодіючої станції із вказаними

характеристиками та максимальні дальності прямої видимості (рис. 6) з урахуванням рельєфу місцевості відповідно до (1) та (4).

3. Якщо кінцева РРС знаходиться в межах зони можливого розташування взаємодіючої станції – перехід до п. 8.

4. Вибір найвіддаленішого від поточної точки (найближчого до кінцевої) місця розташування станції-ретранслятора в напрямку кінцевої станції з урахуванням можливості забезпечення якості зв’язку в розрахованій зоні можливого розташування та з використанням геопросторової інформації щодо наявності відповідної інфраструктури (веж, забудов, електроживлення, точок прив’язки тощо) в зоні граничної дальності зв’язку (табл. 2, 3) для обраного режиму роботи.

5. Розрахунок обраного радіорелейного інтервалу з урахуванням додаткової геопросторової інформації (забудови, вежі) відповідно до (1) з відповідними даними щодо додаткової висоти підвісу антени.

6.Якщо інтервал не забезпечує необхідну якість зв’язку відповідно до (4) – виключення останньої обраної точки та перехід до п. 4

7. Збереження даних розташування станції-ретранслятора, визначення її як поточної та перехід до п. 2.

8. Вивід результатів.

9. Кінець.

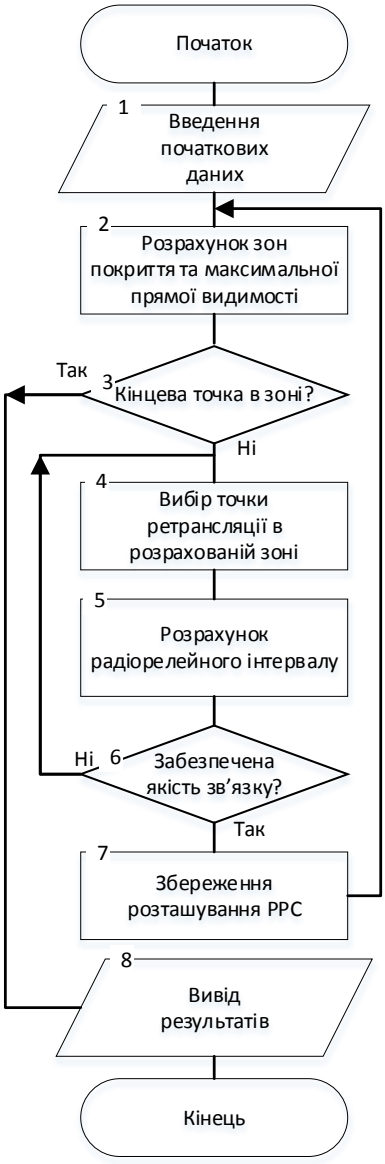


Рис. 5. Блок-схема алгоритму побудови РРЛ

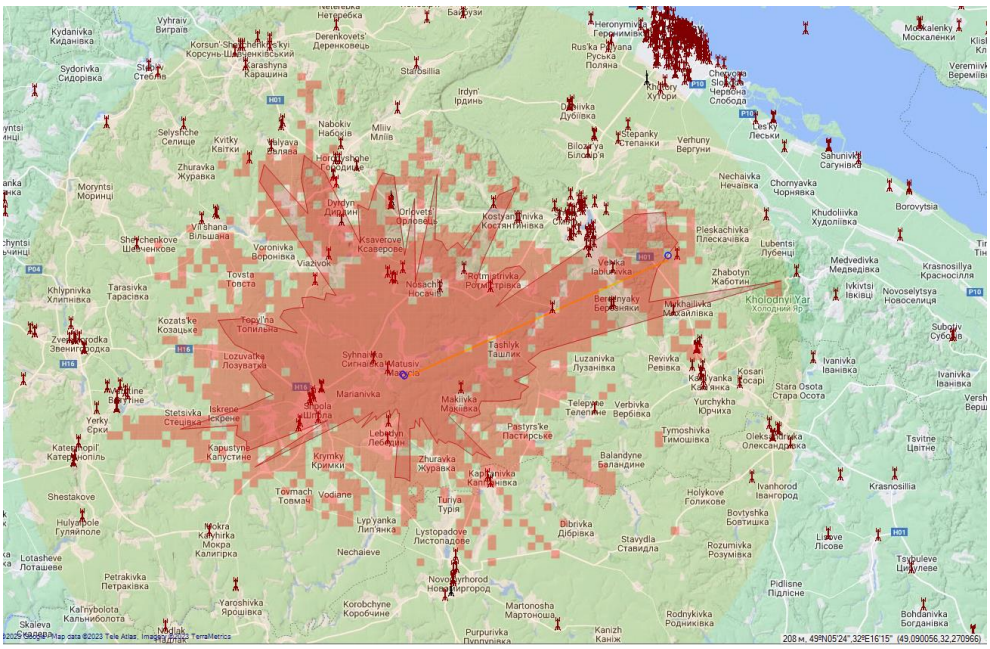


Рис. 6. Розрахунок зони можливого розташування взаємодіючої станції

Результатом застосування методики є отримання параметрів розгортання РРС (з відповідними технічним характеристикам та режимам роботи) для побудови РРЛ, а саме: координати, висоти підвісу антен, азимути, кути місць.

Оцінка ефективності. Програмна реалізація методики дозволяє оператору проводити розрахунки для побудови РРЛ в близькому до реального масштабі часу. Залежно від заданої точності (кроку) розрахунків зон можливого розташування РРС час розрахунку складає одиниці – десятки секунд на ПЕОМ з двоядерним процесором з тактовою частотою 2 ГГц та 4 Гб оперативної пам’яті.

Висновок. У статті представлена методика побудови РРЛ зв’язку з використанням геопросторової інформації, відповідні алгоритми та їх програмна реалізація. Особливістю запропонованої методики є можливість будувати багатоінтервальні радіорелейні лінії зв’язку на основі розрахунків рівнів сигналів з урахуванням рельєфу місцевості та іншої геопросторової інформації (споруди, вежі та інші висотні об’єкти). Також особливістю є побудова зон досяжності (можливості встановлення зв’язку) та зон максимальної прямої видимості для визначення місць розташування станцій-ретрансляторів. Програмна реалізація розроблених алгоритмів дозволяє створити ПЗ планування та розрахунку РРЛ, яке на відміну від існуючого ПЗ, орієнтованого на розрахунки рівнів сигналів між окремими радіорелейними засобами, призначено для побудови багатоінтервальних РРЛ на основі наявних вихідних даних.

Подальші дослідження. У подальшому пропонується розширити розрахунки для тропосферних ліній зв’язку та доопрацювати алгоритми та ПЗ для підвищення ефективності (зменшення часу) планування мереж зв’язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гурський Т. Г., Степаненко Є. О., Шишацький А. В. Оцінка граничної дальності зв’язку на сучасних радіо- та радіорелейних лініях // Збірник наукових праць ВІТІ. 2019. № 1. С. 6–17.

2. Лінії радіозв’язку та антенні пристрої: навч. посіб. / М. Д. Ільїнов, Т. Г. Гурський, І. В. Борисов, К. М. Гриценок. К.: ВІТІ, 2018. 268 с.

3. Гряник М. В. Распространение радиоволн: учеб. пособ. / М. В. Гряник, В. И. Ломан. К.: КВВИУС, 1989. 382 с.

4. Тарасюк О. М. Исследование и разработка энергоэффективных беспроводных сетей: практикум / Тарасюк О. М., Горбенко А. В.; под ред. Харченко В. С. НАУ им. Н. Е. Жуковского „ХАИ”, 2016. 96 с.

5. ITU-R. Recommendation P.526: Propagation by diffraction. URL: https://www.itu.int/rec/R-REC-P.526/.

6. Волков Е. А. Военные системы радиорелейной и тропосферной связи / Е. А. Волков. Л.: ВАС, 1982. 403 с.

7. Наритник Т. М. Радіорелейні та тропосферні системи передачі: навч. посіб. / Т. М. Наритник, В. М. Почерняєв, Ю. В. Уткін. Міністерство науки та освіти, 2007. 312 с. (Серія «Системи передачі»).

8. ITU-R. Recommendation P.530: Propagation data and prediction methods required for the design of terrestrial line-of-sight systems. URL: https://www.itu.int/rec/R-REC-P.530/.

9. Радіорелейна станція Р-425С3. Посібник з експлуатування ААМВ.464412.003 РЭ. 68 с.

10. Mini-Link TN ETSI Release 5.3FP. Product Spec. Ericsson AB, 2014. 152 p.

11. Банкет В. Л. Сигнально-кодовые конструкции в телекоммуникационных системах / В. Л. Банкет. Одесса: Фенікс, 2009. 180 с.

12. ITU-R. Recommendation P.525: Calculation of free-space attenuation. URL: https://www.itu.int/rec/R-REC-P.525/.

13. ITU-R. Recommendation P.676: Attenuation by atmospheric gases and related effects. URL: https://www.itu.int/rec/R-REC-P.676/.

14. ITU-R. Recommendation P.452: Prediction procedure for the evaluation of interference between stations on the surface of the Earth at frequencies above about 0.1 GHz. URL: https://www.itu.int/rec/R-REC-P.452/.

DOI: 10.58254/viti.3.2023.05.41

УДК 378.046

Кондрусь А. В. ORCID: 0000-0001-8815-6517 (ВІТІ ім. Героїв Крут)
Балан Д. Д. ORCID: 0000-0002-6714-8718 (ВІТІ ім. Героїв Крут)
Олексенко В. П. ORCID: 0000-0003-2757-498X (ГУЗтаКБ ГШ ЗСУ)
канд. техн. наук Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ «BIG DATA» ДЛЯ ЗБЕРЕЖЕННЯ, ОБРОБКИ ТА АНАЛІЗУ ДАНИХ У ПРОЦЕСІ УПРАВЛІННЯ ВІЙСЬКАМИ

У сучасному світі збільшення обсягу та різноманітності даних, що використовуються в процесі управління військами, призводить до зростання вимог та їх зберігання і обробки.

Для ефективного управління військовими операціями необхідно володіти інформацією про різні аспекти військової діяльності, такі як розташування військових підрозділів, наявність ресурсів, оцінка потенційних загроз та багато іншого.

Сучасна військова діяльність потребує обробки та аналізу великої кількості даних, які генеруються в режимі реального часу. Дані, зібрані з датчиків, супутників, зондів, сенсорів та інших джерел, можуть бути величезними за обсягом та різноманітними за структурою.

Збільшення обсягу та різнорідність даних, які використовуються в процесі управління військами, призводять до зростання вимог до їх зберігання та обробки. Це ставить перед військовими організаціями завдання створення ефективних та надійних систем зберігання та обробки даних.

Стаття розглядає можливості використання технології «Big Data», які дозволяють збирати, зберігати, обробляти та аналізувати великі обсяги різноманітних даних у режимі реального часу.

Використання сучасних технологій управління даними може допомогти підвищити ефективність військової діяльності та забезпечити швидке та точне прийняття рішень на різних рівнях управління. Це може бути досягнуто завдяки використанню технологій штучного інтелекту, машинного навчання та аналізу даних, які можуть допомогти військовим структурам виконувати розрахунки та прогнозування, оптимізувати використання ресурсів та підвищувати ефективність вирішення різних завдань. Також важливою складовою ефективного використання технологій «Big Data» у військовій сфері є забезпечення захисту даних від несанкціонованого доступу, а також забезпечення надійності та стійкості систем зберігання та обробки даних в умовах можливих кібератак.

У статті проаналізовано систему Hadoop, яка може бути використана для збереження, обробки та аналізу «Big Data» у військовій сфері.

Ключові слова: *структуровані дані, неструктуровані дані, великі обсяги даних, «Big Data».*

A. Kondrus, D. Balan, V. Oleksenko, O. Symonenko Application of «Big Data» technologies for storage, processing and analysis of data in the process of army management.

In today's world, the increase in the volume and variety of data used in the process of military management leads to an increase in the requirements for their storage and processing.

To effectively manage military operations, it is necessary to have information about various aspects of military activity, such as the location of military units, the availability of resources, the assessment of potential threats, and much more.

Modern military operations require the processing and analysis of a large amount of data generated in real time. Data collected from sensors, satellites, probes, sensors, and other sources can be vast in volume and diverse in structure. The increase in the volume and heterogeneity of data used in the process of military management leads to an increase in the requirements for their storage and processing. This presents military organizations with the task of creating effective and reliable data storage and processing systems.

The article considers the possibilities of using «Big Data» technology, which allow collecting, storing, processing and analyzing large volumes of various data in real time.

The use of modern data management technologies can help increase the efficiency of military activities and ensure fast and accurate decision-making at various levels of management. This can be achieved through the use of artificial intelligence, machine learning and data analysis technologies that can help military structures perform calculations and forecasts, optimize the use of resources and increase the efficiency of solving various tasks. Also, an important component of the effective use of «Big Data» technologies in the military sphere is ensuring the protection of data from unauthorized access, as well as ensuring the reliability and stability of data storage and processing systems in the face of possible cyberattacks.

The article analyzes the Hadoop system, which can be used to store, process and analyze «Big Data» in the military sphere.

Keywords: *structured data, unstructured data, large volumes of data, «Big Data».*

Постановка завдання. З урахуванням зростання кількості даних, їх важливості та ризику втрати, стає все більш важливим розробка системи зберігання даних для управління військами, яка відповідала б найвищим вимогам щодо надійності, безпеки та ефективності. Така система може забезпечити більш ефективне та точне управління військами, зменшення ризиків та безпеку.

Створення системи зберігання даних для управління військами зможе покращити процеси планування та прийняття рішень, що, в свою чергу, покращить виконання завдань військовими підрозділами та забезпечить взаємодію між ними в реальному часі.

На сьогодні існуючі системи зберігання даних не завжди можуть задовольнити вимоги автоматизованих систем управління військами. Наприклад, деякі з них можуть бути застарілими, не забезпечують достатню надійність або ефективність, недостатньо адаптовані до вимог сучасного військового управління. Збільшення кількості даних та їхня складність можуть зробити існуючі системи зберігання непридатними для використання в управлінні військами.

Аналіз останніх публікацій. Нині виникає проблема щодо великих обсягів даних, які сформувалися у процесі діяльності Збройних сил України та Міністерства оборони України за роки незалежності і потребують зберігання, відповідно до чинного законодавства [1]. У сучасному світі «Big Data» в інформаційних технологіях використовуються для покращення операцій, забезпечення кращого обслуговування клієнтів, розробки налаштованих маркетингових кампаній та виконання інших дій для покращення різних аспектів бізнесу, науки та техніки [2]. У спеціальній науковій літературі розглядаються технології аналізу, обробки та зберігання «Big Data» [3–6], які можна застосувати і у військовій сфері.

Мета статті: аналіз можливості застосування технологій «Big Data» для збереження, обробки та аналізу даних у процесі управління військами.

Викладення основного матеріалу. Збройні сили будь-якої країни світу можуть зазнати поразки в ході бойових дій через недостатню кількість або відсутність необхідної оперативної інформації. У ході бою великий обсяг інформації надходить від особового складу, командирів, техніки, засобів розвідки, яка потребує швидкої обробки. Актуальна інформація потрібна збройним силам на кожному рівні, для прийняття обґрунтованих рішень.

Велику кількість даних надає розвідка, яка є важливою складовою для підготовки та успіху бою.

Починаючи з етапу передачі інформації до етапу прийняття рішення і видачі наказу, дуже важливу роль відіграє система зберігання даних. Чим більш доступною, організованою, цілісною вона буде, тим швидше буде працювати вся система.

Проблема зберігання та обробки інформації є актуальною на сьогодні. На сучасному етапі розвитку інформаційних систем на всіх рівнях управління Збройних сил України виникають проблеми, пов’язані з великим обсягом даних, який сформувався за роки існування незалежної України, особливо під час військових дій російсько-української війни. Багато інформації, починаючи з 1992 року і дотепер, досі зберігається в письмовому і оцифрованому вигляді. Керівні документи, застарілі накази та розпорядження, описи майна військових частин, – вся ця інформація може бути застарілою, але повинна зберігатися певний визначений термін, згідно з чинним законодавством України [1].

Окремо необхідно зазначити широке використання технології «Інтернету речей» (IoT) великої кількості датчиків на військових об’єктах або об’єктах відповідальності Міністерства оборони України та Збройних сил України. Такі технології передбачають використання датчиків, виконавчих пристроїв, мікроконтролерів, які можуть виконувати різні дії. У процесі роботи виконується постійний збір даних, великі масиви інформації надходять у режимі реального часу та зберігаються для подальшого використання.

Під великими даними розуміється широке розмаїття масивів даних, які не можуть бути належним чином оброблені традиційними додатками через свій величезний обсяг або різний тип.

«Big Data» – це поєднання структурованих, напівструктурованих та неструктурованих даних, які можуть бути видобуті для отримання інформації та використані в різних сферах.

Системи, які обробляють і зберігають «Big Data», стали загальним компонентом архітектур управління даними в великих організаціях.

«Big Data» часто характеризуються за наступними характеристиками «6V»:

– **обсяг** (volume) – об'єм даних, які можна зберігати та обробляти за допомогою технологій «Big Data»;

– **швидкість** (velocity) – швидкість, з якою дані надходять та обробляються в системах «Big Data»;

– **правдивість** (veracity) – якість даних, яка зазвичай включає точність, повноту та достовірність;

– **різноманітність** (variety) – різноманітність форматів і типів даних, які можуть бути збережені та оброблені за допомогою технологій «Big Data»;

– **цінність** (value) – важливість та цінність даних, які можна отримати з використанням технологій «Big Data»;

– **мінливість** (variability) – непередбачуваність та змінність даних, які можуть бути збережені та оброблені за допомогою технологій «Big Data».

У таблиці 1 наведено порівняння найпопулярніших технологій «Big Data» за характеристиками «6V».

Таблиця 1

Порівняння найпопулярніших технологій «Big Data» за характеристиками «6V»

Технологія	Обсяг	Швидкість	Правдивість	Різноманітність	Цінність	Мінливість
Hadoop	+++	++	++	+++	+++	+++
Kafka	++	+++	++	++	+++	++
Cassandra	++	++	+++	+++	++	++
MongoDB	++	++	+++	+++	++	++

«+++» – висока ефективність відносно даної характеристики;

«++» – помірна ефективність відносно даної характеристики.

Складність аналізу «Big Data» полягає в специфіці їх збору, керування, поділу, зберігання, передачі та візуалізації.

Під аналізом «Big Data» часто розуміється застосування прогнозної аналітики або інших передових методів з метою вилучення з безлічі даних певної корисної інформації. Точність при аналізі «Big Data» допомагає приймати більш раціональні рішення. У свою чергу, прийняття найкращих рішень дозволяє збільшити виробничу ефективність, скоротити витрати і знизити ризики.

Аналітика в реальному часі даних різних форматів та будь-якого обсягу даних є кінцевою метою аналітики «Big Data». Програмні рішення повинні проводити аналіз різноманітних даних, поки дані все ще перебувають у русі. Щоб полегшити це, архітектурна структура вимагає інтегрування даних. Цього найкраще досягти за допомогою повної апаратної та програмної інтегрованої системи обробки «Big Data».

Доцільно розглянути процес розгортання відповідно до трьох основних фаз (збір даних, організація даних та аналіз даних) інфраструктури «Big Data». Розгортання – це складний процес, у якому необхідно враховувати дрібниці, задіяні на етапах придбання, організації та аналізу. Зазвичай, організації беруть участь у фазі аналізу попередньої розробки, щоб визначити архітектурні вимоги на основі характеру даних, очікуваного часу обробки, вимог конфіденційності отриманих результатів та доступності для конкретного проєкту.

Основними обмеженнями, які слід врахувати в процесі розгортання, є неоднорідність даних, вимога до своєчасної обробки, проблеми безпеки, масштаб з точки зору обсягу, складність даних, очікувана точність результатів та, що більш важливо, спосіб забезпечення взаємодії особи з даними. Відповідно до п'ятифазної моделі процесу [2], обробка в режимі реального часу охоплює дистиляцію даних, розробку моделі, перевірку та розгортання, оцінку роботи в реальному часі та оновлення моделі.

Конвеєр розгортання великих даних може починатися з отримання та запису даних, а потім переходити до аналізу архітектури; вилучення даних; формування даних; їх інтеграції, агрегування, аналізу та моделювання; представництва і нарешті їх інтерпретації. Всі ці процеси є складними, оскільки безліч варіантів та методів оптимізації доступні на кожній фазі конвеєру розгортання. Вибір та обробка відповідних методів для кожної фази залежить від природи даних та очікуваних результатів. Для зручності розуміння ці підпроцеси згруповані за трьома основними фазами інфраструктури (таблиця 2).

Жодна окрема технологія не може сформувати повну платформу великих даних. Саме інтеграція багатьох основних технологій створює платформу «Big Data», більш широку модель «Big Data» для організації. Проте замість того, щоб розглядати рішення для «Big Data» як цілком нову технологію, доцільно розглядати платформу «Big Data» як інтегроване розширення існуючих інструментів бізнес-аналітики, наприклад: Hadoop – система надійного загального зберігання та аналізу даних, основними складовими якої є розподілена файлова система *Hadoop Distributed File System* (HDFS), яка забезпечує зберігання та високошвидкісний доступ до даних, а також MapReduce – програмна модель проведення розподіленої паралельної обробки та аналізу великих масивів даних з використанням кластерів звичайних недорогих комп'ютерів [3].

Таблиця 2

Підпроцеси та їх відповідні цілі, пов'язані з конвеєром розгортання

Назва фази	**Субпроцес**	**Призначення**
Отримання даних	– збір даних і їх запис; – архітектурний аналіз	– збирання даних з різних інформаційних джерел та завантаження їх у *NoSQL* бази даних; – базується на отриманих даних. Проводиться аналіз вимог до архітектури, необхідної для обробки
Організація даних	– вилучення та формування даних; – інтегрування; – агрегація та репрезентація	– уточнення вихідних даних для отримання зразку; – ідентифікація відносин між під'єднаними точками даних; – встановлення представлення під'єднаних даних
Аналіз даних	– аналіз та моделювання; – інтерпретація	– виконання необхідного аналізу; – завантаження даних в форматі *user-friendly* в базу даних

Робота MapReduce заснована на розбитті обробки даних на дві фази: фазу відображення MAP та фазу згортки REDUCE. Кожна фаза використовує в якості вхідних і вихідних даних пару «ключ-значення», типи яких вибирає програміст. Програміст також визначає дві функції: функцію відображення map() та функцію згортки reduce().

Розглянемо на прикладі аналізу метеорологічних даних Національного центру кліматичних даних (NCDC) засобами MapReduce [3].

Вхідними даними для фази MAP у нашому прикладі є вихідні дані NCDC. Ми вибираємо текстовий формат вхідних даних, у якому кожен рядок набору даних інтерпретується як текстове значення. Ключем є зміщення початку рядка від початку файла, але оскільки ця інформація нам не потрібна, ми її просто ігноруємо.

Функцію map() влаштовано просто. Ми отримуємо рік та температуру повітря, бо нас цікавлять лише ці поля. У цьому випадку функція map() лише готує дані до використання так, щоб функція reduce() могла виконати свою роботу, а саме – визначення максимальної

температури за кожен рік. Функція map() також підходить для виключення небажаних записів: тут відфільтровуються відсутні, сумнівні або помилкові значення температури.

Щоб уявити, як працює функція map(), розглянемо кілька рядків вхідних даних.

```
0067011990999991950051507004...9999999N9+00001+99999999999...;
0043011990999991950051512004...9999999N9+00221+99999999999...;
0043011990999991950051518004...9999999N9-00111+99999999999...;
0043012650999991949032412004...0500001N9+01111+99999999999...;
0043012650999991949032418004...0500001N9+00781+99999999999... .
```

Ці рядки передаються функції map() у вигляді пар «ключ-значення»:

(0, 0067011990999991**950**051507004...9999999N9+**00001**+99999999999...);
(106, 0043011990999991**950**051512004...9999999N9+**00221**+99999999999...);
(212, 0043011990999991**950**051518004...9999999N9-**00111**+99999999999...);
(318, 0043012650999991**949**032412004...0500001N9+**01111**+99999999999...);
(424, 0043012650999991**949**032418004...0500001N9+**00781**+99999999999...).

Ключі (зміщення рядків у файлі) функції map() ігноруються. Функція відображення просто отримує рік і температуру повітря (виділені жирним шрифтом) і передає їх як вихідні дані (значення температури інтерпретуються як цілі числа):

(1950, 0);
(1950, 22);
(1950, −11);
(1949, 111);
(1949, 78).

Вихідні дані функції map() обробляються інфраструктурою MapReduce перед тим, як вони передані функції reduce(). Під час цієї обробки пари «ключ-значення» сортуються та групуються за ключом. Таким чином, у нашому прикладі функція reduce() отримає такі вхідні дані:

(1949, [111, 78]);
(1950, [0, 22, −11]).

Кожен рік супроводжується переліком його значень температури. Тепер функції reduce() залишається лише перебрати елементи списку та знайти максимум:

(1949, 111);
(1950, 22).

Схема потоку даних зображена на рисунку 1.

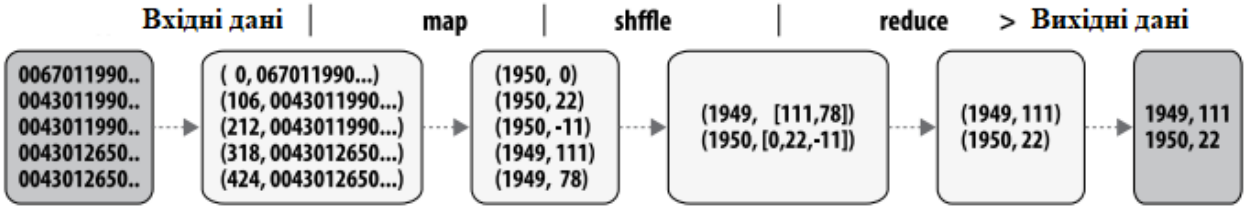


Рис. 1. Схема потоку даних

Розподілена файлова система Hadoop (HDFS) – варіант зберігання даних платформи Hadoop, який використовується для збору, зберігання та отримання даних для подальшого аналізу. HDFS зазвичай конфігурується як безпосередньо приєднане сховище (DAS) до Hadoop і полегшує переміщення блоків даних на різні розподілені сервери для обробки. HDFS орієнтований на бази даних NoSQL, здатні фіксувати та зберігати всі формати даних без
будь-якої категоризації. Вихідні дані, що генеруються платформою Hadoop, зазвичай записуються на HDFS, який працює у архітектурі master-slave, із двома типами вузлів, вузлом імен (NameNode) та вузлом даних (DataNode). Він використовує один NameNode на кластер, який виконує роль master, і ряд вузлів DataNode, що виконують запити читання та запису клієнтів.

Вузли DataNode зберігають блоки даних у HDFS, тоді як вузол NameNode містить метадані з переліком блоків та списком вузлів даних у кластері HDFS. На рисунку 2 показано логічне представлення компонентів HDFS [4].

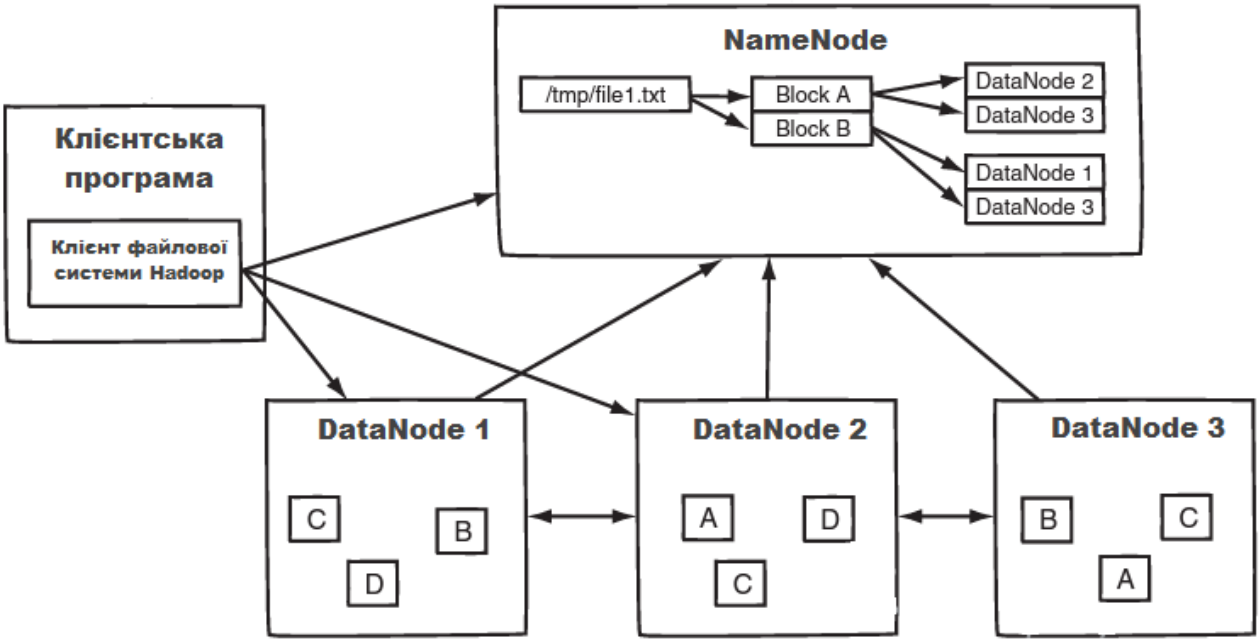


Рис. 2. Логічне представлення компонентів HDFS

HDFS має можливість зберігати дані всіх форматів та великих розмірів. Таким чином, вони перевершують можливості традиційних СУБД, які обмежуються лише структурованими даними.

Аналітика «Big Data» ілюструє значну та вагому цінність нової технології, але вона також демонструє складність платформи аналітики на кожному етапі. Успіх концепції великих даних полягає в потенційній інтеграції допоміжних технологій, які можуть полегшити збір, зберігання та аналіз даних. Реалізація «Big Data» вимагає розширення або навіть заміни традиційних систем обробки даних. Розуміючи значення «Big Data» для розвитку у найближчі роки, організації і відповідні структурні підрозділи почали частіше застосовувати рішення для використання «Big Data». З іншого боку, розміри наборів даних постійно зростають, і тому необхідно впроваджувати нові технології та нові стратегії для роботи з цими даними. Хмарні обчислення лежать в основі реалізації «Big Data». В цілому, надійність «Big Data» вимагає включення, інтеграції та узгодження відповідних методів і технологій, щоб забезпечити перспективи та потенціал рішень для великих даних.

Висновок. Використання технологій «Big Data» має значний потенціал для покращення управління військовими операціями. Завдяки цим технологіям збирається більша кількість даних, що може бути оброблено та проаналізовано для отримання більш точної та повної інформації про військові операції. Це дозволяє керівникам ухвалювати більш обґрунтовані та

ефективні рішення щодо використання ресурсів, що підвищує ефективність військових операцій та допомагає досягти поставлених цілей.

Напрямки подальших досліджень: пошук ефективної моделі впровадження кластера Hadoop для збереження, обробки та аналізу даних у процесі управління військами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Перелік типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів: Наказ Міністерства юстиції України від 12 квітня 2012 року № 578/5.

2. Barlow, M., 2013. Real-Time Big Data Analytics: Emerging Architecture.

3. Tom White Hadoop: The Definitive Guide 4th Edition Revised & Updated, 2015.

4. Alex Holmes Hadoop in Practice, 2012.

5. Chuck Lam Hadoop in Action, 2013 // URL: https://www.manning.com/books/hadoop-in-action (дата звернення: 23.03.2023).

6. Dong, X., Srivatsava, D., 2013. Big Data integration. In: 29th International Conference on Data Engineering (ICDE). IEEE, Brisbane, pp. 1245–1248.

7. IBM Developer / M. Tim Jones. Process your data with Apache Pig, 2012 // URL: https://event.cwi.nl/lsde/papers/apachepigdataquery.pdf (дата звернення: 23.03.2023).

DOI: 10.58254/viti.3.2023.06.48

УДК 621.317.08

д-р техн. наук Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ)
Погребняк С. В. ORCID: 0000-0002-7902-9847 (ВІТІ)
Михайлюк С. С. ORCID: 0009-0001-5665-8866 (ВІТІ)

ВАРІАНТ ВИЗНАЧЕННЯ ТЕХНІЧНОГО СТАНУ ЕЛЕКТРОЛІТИЧНОГО КОНДЕНСАТОРА МЕТОДОМ БЕЗКОНТАКТНОЇ ДІАГНОСТИКИ

Під час повномасштабної війни в Україні сили оборони почали отримувати засоби радіоелектронного озброєння від країн-партнерів. Зразки озброєння, які надаються, здебільшого не нові та мають певний ресурс напрацювання та (або) терміни зберігання. Внаслідок цього загострилось питання діагностування технічного стану таких зразків. У статті наведено варіант визначення технічних характеристик одного з низьконадійних радіоелектронних компонентів (електролітичного конденсатора) сучасних імпульсних блоків живлення радіоелектронного устаткування. Розглядаються практичні способи та вимірювальні прилади для діагностування та типові проблеми, з якими доводиться зіткнутися під час проведення робіт з визначення технічного стану об'єкта контролю. Описано основні фізичні властивості, які покладено в основу запропонованого методу визначення технічного стану та представленої еквівалентної схеми датчика діагностичного сигналу.

Представлений метод базується на використанні безконтактного індукційного датчика. Визначення технічного стану радіоелектронного компоненту здійснюється на основі аналізу вихідних сигналів функціональних вузлів, які містять даний компонент. Використання запропонованого методу вимагає наявності еталонного сигналу (відповіді на тестовий сигнал), з яким порівнюється сигнал, отриманий під час перевірки. Запропоновано можливий варіант використання спеціального програмного забезпечення, яке надає можливість наочної презентації отриманої діагностичної інформації та її візуалізації в різних видах. Описано основні технічні характеристики обладнання, що використовується.

Спираючись на потенційну ефективність, інформативність та безпечність запропонованого способу, обґрунтовано доцільність непринципової зміни конструктиву об'єкта контролю з метою застосування запропонованого методу як безпосередньо в блоках монтованих плат та схем, так і на випробувальних стендах.

Ключові слова: *безконтактний індукційний метод, датчик діагностичного сигналу, гістограма, низьконадійний елемент, діагностичний параметр.*

V. Kuzavkov, S. Pohrebniak, S. Mykhailiuk Variant of determining the technical condition of an electrolytic capacitor by contactless method.

In the course of the full-scale war in Ukraine, the defense forces began to receive radio-electronic weapons from partner countries. The samples of weapons that are provided are mostly not new and have a certain service life and (or) shelf life. As a result, the issue of diagnosing the technical condition of such samples became more acute.

The article provides a variant of determining the technical characteristics of one of the low-reliability radio electronic components (electrolytic capacitor) of modern pulsed power supply units of radio electronic equipment. Practical methods and measuring devices for diagnosis and typical problems that have to be faced during work on determining the technical condition of the control object are considered.

The main physical properties are described, which are the basis of the proposed method of determining the technical condition and the presented equivalent circuit of the diagnostic signal sensor. Calculations of empirical studies and assumptions expressed in previous works of the authors have been mathematically confirmed.

The presented method is based on the use of a non-contact induction method. The determination of the technical condition of the radio-electronic component is carried out on the basis of the analysis of the output signals of the functional nodes that contain this component. The use of the proposed method requires the availability of a reference signal (response to the test signal) with which the signal obtained during the test is compared.

Based on the potential effectiveness, informativeness and safety of the proposed method, the expediency of a non-fundamental change in the design of the control object is substantiated, in order to effectively apply the proposed method both directly in the blocks of mounted boards and circuits and on test stands.

Keywords: *non-contact induction method, diagnostic signal sensor, histogram, low-reliability element, diagnostic parameter.*

Постановка завдання в загальному вигляді. Збройна агресія Росії проти України спричинила новий виток модернізації та переоснащення Збройних сил України та інших військових формувань на новітні зразки озброєння та військової техніки. До сил оборони України надходить все більша кількість радіоелектронної апаратури. Значна кількість цих зразків перебувала на базах та складах тривалого зберігання. Поставки західного озброєння

від країн-партнерів обумовили загострення питання технічного діагностування зразків радіоелектронного озброєння. Виконання завдань за призначенням підрозділів та частин значною мірою залежить від якості та надійності зразків радіоелектронного озброєння, яким вони укомплектовані. Враховуючи специфіку та масштабність театру бойових дій, значна увага приділяється надійності та захищеності системи зв’язку та координації дій підрозділів. Абсолютно всі підрозділи використовують засоби радіоелектронної апаратури (засоби зв’язку, планшети, ноутбуки, системи відеоспостереження, комплекси керування БпЛА і т. ін.). Всі ці засоби мають блоки живлення в тому чи іншому варіанті виконання. Однак термін експлуатації таких блоків живлення в рази перевищує «терміни життя» низьконадійних радіоелектронних компонентів (РЕК). Процеси «старіння» та «зношування» РЕК мають різну природу та інтенсивність. Це обумовлено, перш за все, різними початковими фізичними властивостями РЕК та умовами експлуатації. Отже, важливим є моніторинг стану РЕК як фундаментальної процедури оцінки працездатності радіоелектронного озброєння, що забезпечує прогностичний ремонт для гарантування стабільної роботи.

Аналіз публікацій за темою дослідження. Проблемі визначення технічного стану РЕК присвячено велика кількість робіт як вітчизняних, так і закордонних вчених [1–6; 21–24]. Існуюча система технічного діагностування, яка використовується в Збройних силах України, застаріла і не повною мірою відповідає вимогам сьогодення [7]. Як відомо, причиною переважної більшості відмов радіоелектронної апаратури є несправність низьконадійних елементів, до яких відносять і електролітичні конденсатори [8; 9; 21–27]. Різноманітні методи визначення технічного стану РЕК стали об’єктами досліджень багатьох наукових шкіл, які працюють в галузі технічної діагностики [10–12; 20–24; 30–32]. Роботи, опубліковані за останній час, зосереджені на підвищенні надійності електролітичних конденсаторів в ланцюгах постійного струму та пошуку методів підвищення часу життя електролітичних конденсаторів [25; 26]. Однак пошук «неінвазивного» варіанта визначення технічного стану РЕК є актуальним з огляду на формфактор та специфіку апаратури подвійного призначення, що використовується в Збройних силах України. Існуючі методи визначення технічного стану передбачають втручання в об’єкт контролю та необхідність вилучення (випаювання) електролітичного конденсатора для правильного (коректного) визначення його технічного стану. Це вимагає великої витрати часу, наявності спеціальних інструментів та пристроїв, а також специфічної навченості персоналу. Саме тому все більшу увагу міжнародна наукова спільнота приділяє безконтактним онлайн методам визначення технічного стану електролітичних конденсаторів [27–30]. Автори цих робіт намагаються обґрунтувати можливість визначення технічного стану електролітичних конденсаторів в ланцюгах постійного струму безконтактними методами та пропонують варіанти різних схемотехнічних рішень вбудованих систем контролю для вирішення поставлених задач. При чому запропоновані системи контролю передбачають наявність того чи іншого периферійного устаткування (осцилографи, мікроконтролери, ESR-вимірювачі, LCR-вимірювачі та мікрокомп’ютери зі спеціалізованим програмним забезпеченням).

Метою статті є обґрунтування можливості визначення технічного стану електролітичних конденсаторів безконтактним індукційним методом в імпульсних блоках живлення радіоелектронного обладнання без необхідності випаювання конденсаторів та використання спеціалізованого периферійного устаткування.

Виклад основного матеріалу. Як відомо, близько 30 % всіх несправностей електронної апаратури викликана відмовами електролітичних конденсаторів [31]. Пошук несправних низьконадійних елементів за допомогою тестера чи вимірювального пристрою ємності має ряд недоліків та обмежень. Це обумовлюється необхідністю випаювання «підозрюваного» конденсатора та вимірювання його ємності. Ємність несправного конденсатора може відрізнятися від номінальної на незначну величину, а значення такої характеристики як ESR (Equivalent Series Resistance – еквівалентного послідовного опору) може бути досить великим. Саме ESR є важливішим параметром для вимірювання під час пошуку несправного конденсатора. У більшості випадків це конденсатори імпульсних блоків

живлення в апаратурі подвійного призначення, імпульсних блоків живлення комп'ютерів, імпульсних перетворювачах на материнських платах, драйвери двигунів, малі розгортки та ін. У цих місцях конденсатори піддаються значному нагріванню і швидше виходять з ладу – «висихають».

Існуючі методики діагностування електролітичних конденсаторів використовують різноманітні мультиметри, або спеціалізовані цифрові тестери. Наприклад, пристрій для вимірювання ESR та ємності конденсаторів Mega328 LCR-T4. Відповідно до характеристик, пристрій налаштований на формування синусоїдального струмі частотою 62,5 кГц. Незважаючи на те, що частоти імпульсних блоків живлення та перетворювачів лежать у діапазоні 20–100 кГц, форма перевірного сигналу не відповідає формі сигналу у ланцюгах реальних схем живлення.

Окрім того, вимірювання проводяться без демонтажу конденсатора з штампованої плати шляхом контактного підключення вимірювального пристрою. Для імпульсних блоків живлення напруга у окремих частинах схеми досягає рівня 400 В і конструктивно передбачаються відповідні обмеження до елементів схеми. Тому, для отримання доступу до певних радіокомпонентів іноді необхідно виконати повну розборку пристрою.

Слід зазначити також, що алгоритм розрахунку ESR на базі виміряної напруги не може повністю враховувати нелінійності, пов'язані з ненульовим вихідним опором генератору тестового сигналу, а також пропорції зміни напруги на низькоомних дільниках. Отже, неможливо забезпечити необхідну точність та лінійність вимірювань у всьому діапазоні.

Тому в статті пропонується використовувати метод безконтактного діагностування. Цей пристрій діагностування складеться з індукційного датчика [14; 15] (роботу якого наведено нижче), аналого-цифрового перетворювача (АЦП) та спеціалізованого програмного забезпечення. Рішення про технічний стан приймається за результатами порівняння зразкового (еталонного) сигналу схеми з отриманими під час перевірки за детермінованим підходом розпізнання [19]. Використовуючи метод статистичних рішень при відомих граничних значеннях x_0 параметра x об'єкта контролю, приймається рішення про працездатний або непрацездатний стан. Параметром x може виступати як ємність конденсатора (С), так і його еквівалентний послідовний опір (ESR).

Граничними значеннями для ємності прийнято вважати її зменшення більш ніж на 20 %, а граничним значенням ESR є його збільшення більш ніж у 2 рази від номінальних значень [32]. У такому випадку правило прийняття рішення матиме вигляд (1) [19]:

$$\text{при } x < x_0 \;\; x \in D_1;\; x > x_0 \;\; x \in D_2\,. \tag{1}$$

Для значень, які можуть набувати параметри x в нашому випадку, вираз (1) матиме вигляд (2), (3):

$$x < 2x \;\; x \in D_1; \quad x > 2x \;\; x \in D_2, \tag{2}$$

де x – параметр ESR;
D_1 – справний стан;
D_2 – дефектний стан.

$$x > 0{,}2x \;\; x \in D_1;\; x < 0{,}2x \;\; x \in D_2, \tag{3}$$

де x – параметр С;
D_1 – справний стан;
D_2 – дефектний стан.

З метою мінімізації кількості помилкових рішень при оцінці стану ОК виконання нерівностей (2) та (3) одночасно дає максимальну щільність ймовірнісного розподілу.

Розглянемо конструкцію та принцип функціонування датчика [16], який використовується для зняття діагностичної інформації (рис. 1). Довкола кожного з активних провідників виникає магнітне поле. Щоб отримати параметри поля і перетворити їх в електричний сигнал, необхідно провід пропустити крізь магнітний сердечник з обмоткою. Як наслідок, цей провід виконує роль первинної обмотки (з одного витка), вторинна обмотка може мати більшу кількість витків. Наведена конструкція є струмовим трансформатором, напруга та форма сигналу у вторинній обмотці якого пропорційна зміні струму первинної обмотки [17].

Як відомо, всі трансформатори складаються з кількох котушок індуктивності, пов’язаних загальним магнітним полем.

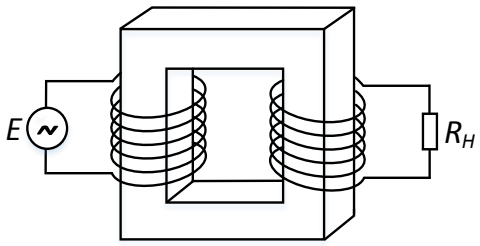


Рис. 1. Датчик діагностичної інформації

Котушка, до якої прикладається джерело змінної напруги E, називається первинною обмоткою. Інші називаються вторинними, до них підключається навантаження $R_н$.

Принцип роботи трансформатора виходить із закону електромагнітної індукції (закону Фарадея). Напруга первинної обмотки E_1 (напруга підключеного джерела) пов’язана з магнітним потоком $Ф$, який проходить через кожен виток первинної обмотки, співвідношенням:

$$E_1 = w_1 \frac{d\Phi}{dt},$$

де w_1 – число витків первинної обмотки.

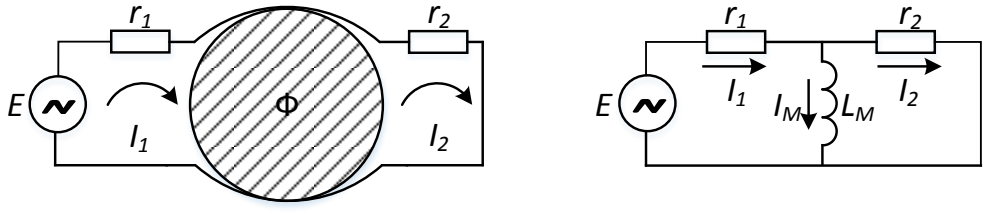
Аналогічно, ЕРС, наведена у вторинній обмотці з числом витків w_2, має вигляд:

$$E_2 = w_2 \frac{d\Phi}{dt}.$$

Звідси витікає, що коефіцієнт передачі напруги або коефіцієнт трансформації n визначається лише відношенням витків:

$$n = \frac{E_2}{E_1} = \frac{w_2}{w_1}.$$

Розглянемо процеси, які відбуваються в трансформаторі струму (рис. 2).



а) *б)*

Рис. 2. Трансформатор:
а – з перекриттям обмоток; *б* – його еквівалентна схема

Нехай кожна обмотка має індуктивність L. Розташуємо їх так, щоб магнітний потік $Ф$, який створюється первинною обмоткою, повністю охоплювався вторинною обмоткою.

У цьому випадку коефіцієнт зв'язку обмоток дорівнює одиниці. Як відомо, падіння напруги на індуктивності пов'язане з магнітним потоком наступним співвідношенням:

$$U_1 = \frac{d\Phi}{dt} = L\frac{dI}{dt},$$

де I – струм, який протікає через індуктивність.

Відповідно до 2-го закону Кірхгофа:

$$E = I_1 r_1 + L\frac{dI_1}{dt} - M\frac{dI_2}{dt} = I_1 r_1 + L\left(\frac{dI_1}{dt} - \frac{dI_2}{dt}\right) \text{ для } M = L,$$

$$E_0 = I_2 r_2 + L\frac{dI_2}{dt} - M\frac{dI_1}{dt} = I_2 r_2 + L\left(\frac{dI_2}{dt} - \frac{dI_1}{dt}\right) \text{ для } M = L,$$

де M – це взаємна індуктивність, тобто індуктивність вторинної обмотки, «видима» з боку первинної і навпаки; $M\frac{dI_2}{dt}$ – напруга, яка наводиться вторинною обмоткою в первинному контурі.

Взаємна індуктивність M визначається через коефіцієнт зв'язку k (при k=1 і L_1=L_2=L_3 отримуємо M=L):

$$k = \frac{M}{\sqrt{L_1 L_2}}.$$

Таким чином, отримаємо еквівалентну схему датчика діагностичного сигналу. До r_1 входить внутрішній опір джерела, опір проводу обмотки й т. ін., а до r_2 – опір навантаження разом з опором проводів та іншими втратами. Якщо нехтувати величиною r_1, то видно, що напруга джерела повністю виявляється прикладеною до навантаження і збігається за величиною (в разі $w_1 = w_2$) і фазою.

Трансформатор як індуктивний елемент присутній на схемі у вигляді паралельної індуктивності $L_м$, яка називається індуктивністю намагнічування і в нашому випадку дорівнює L. Напруга джерела, прикладена до трансформатора, викликає струм намагнічування, який змінюється, а зміна струму, у свою чергу, створює напругу на вторинній обмотці. Таким чином, головна умова роботи трансформатора – наявність струму, який змінюється. Швидкість зміни струму пропорційна величині миттєвої напруги на обмотках.

Датчик діагностичної інформації можливо виконати на броньованому, або кільцевому феритовому сердечнику з високою магнітною проникністю, який розмикається. Таке виконання діагностичного датчика дозволяє переносити його від одної точки виміру до іншої, не втручаючись в роботу самого об'єкта контролю (ОК), яким є імпульсний блок живлення .

Сутність вимірювань [14; 17] полягає у дослідженні параметрів сигналу, отриманого безконтактним методом з перемички між функціональними вузлами об'єкта контролю в умовах реального функціонування ОК.

Розглянемо принцип функціонування пристрою визначення технічного стану конденсаторів безконтактним індукційним методом на прикладі простих радіоелектронних чотириполюсників. До таких пристроїв відносимо широко розповсюджені диференціюючий (рис. 3) та інтегруючий (рис. 4) [18] ланцюги елементів цифрової схемотехніки.

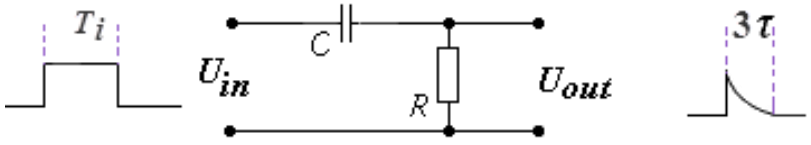


Рис. 3. Диференціюючий ланцюг

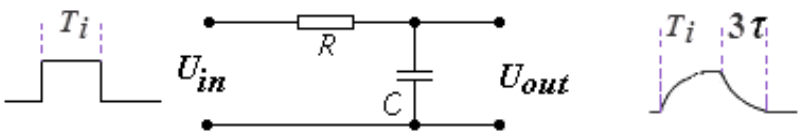


Рис. 4. Інтегруючий ланцюг

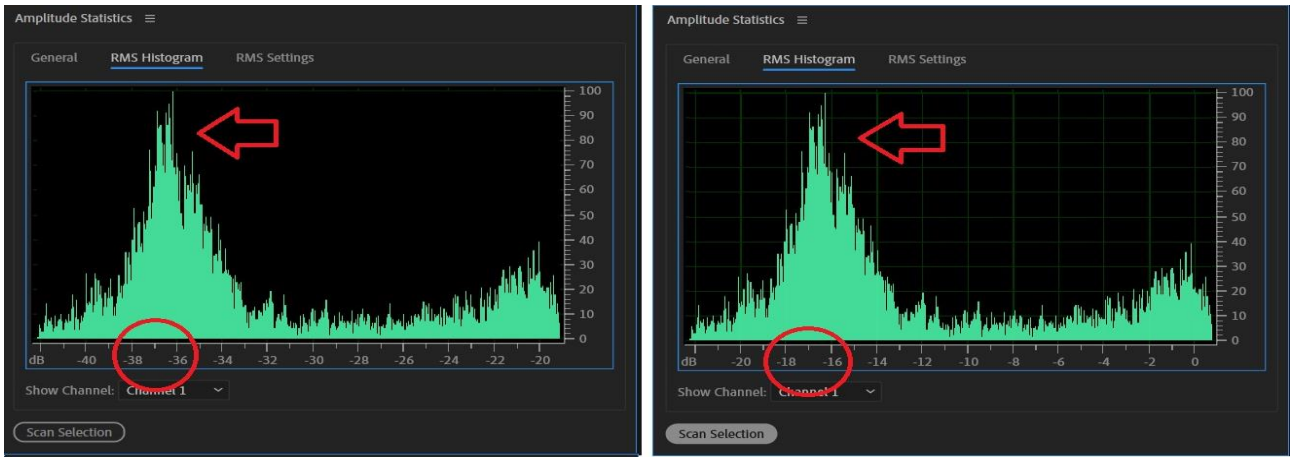
На рисунках 3, 4 зображено вхідний сигнал (у вигляді прямокутного імпульсу) та реакція ланцюгів на нього. В обох випадках форма та часові параметри вихідного сигналу залежать від чисельних значень складових радіоелектронних компонентів (*R, C*). Вважаємо, що величина *R* (в Ом) є незмінною в часі, а часові характеристики перехідних процесів залежать виключно від значення ємності *C* (в Ф). У такому випадку справедливо стверджувати, що зміна форми вихідного сигналу залежить від зміни ємкості конденсатора.

Наведені графіки добре відомі і зазвичай спостерігаються за допомогою осцилографа. У запропонованому методі безконтактного індукційного діагностування сигнал, отриманий за допомогою датчика діагностичних сигналів (ДДС), надходить на АЦП. Аналого-цифрове перетворення здійснює 16-розрядний (65536 кодових позицій) АЦП з частотою квантування 44 кГЦ. Кількість вимірювань за секунду становіть біля 3×10^9, отже при амплітуді вхідного аналогового сигналу 100 мВ зазначені кількісні показники є достатніми для вирішення основних завдань технічного діагностування.

Подальша обробка сигналу виконується спеціальним програмним забезпеченням. Як спеціалізоване програмне забезпечення (СПЗ) використано ліцензійний програмний пакет Adobe Audition (Cool Edit Pro, Wave Lab Pro). Особливістю зазначеного СПЗ є можливість не лише візуалізувати процеси, які відбуваються в об’єкті контролю, а й накопичувати відповідну інформацію з подальшою статистичною обробкою. Внаслідок обробки інформації отримуємо впорядкований розподіл енергії дискретних відліків у вихідному сигналі.

Вказане СПЗ дозволяє виконати декілька способів аналізу отриманої цифрової інформації – фазовий (Phase Meter), частотний (Frequency Analysis) та амплітудний (Amplitude Statistics), кожен з яких має відповідний спосіб візуалізації. Наявність інформативного способу представлення діагностичної інформації дозволяє значно спростити та прискорити її обробку, агрегацію та прийняття відповідних рішень.

На рисунку 5 представлено результати статистично опрацьованої інформації з ДДС для різного стану конденсатора в об’єкті контролю.



а) *б)*

Рис. 5. Гістограма (опрацьований сигнал ДДС):
а – еталонний сигнал; *б* – сигнал, отриманий під час контролю

Обидві гістограми не лише візуалізують зміну стану об’єкта контролю, а й містять кількісну інформацію про енергетичну наповненість сигналу з ДДС. На осі абсцис відкладено значення енергетичного рівня в dB, а по осі ординат – кількість таких відділків. Результати, отримані з еталонного ОК (рис. 5, *а*), відображають максимальне значення вибірки, яке припадає на діапазон -38…-36 dB. При визначенні стану об’єкта контролю енергетичний максимум вибірки припадає значення -18…-16 dB (рис. 5, *б*). Що свідчить про відмінність у 20 dB. Зростання енергії обумовлено деградацією якості параметрів електролітичного конденсатора (параметри резистора вважатимемо незмінними в часі).

Для радіоелектронних компонентів особливо важливих зразків обладнання процедура прийняття рішення про технічний стан об’єкта контролю відбувається незалежно від оператора засобами автоматизованої системи діагностування (АСД), як запропоновано в [28–30], при цьому база даних АСД при кожному запуску процедури контролю поповнюється додатковими сигнатурами стану конденсатору, відповідність яких очікуваним результатам свідчить про належний (або неналежний) технічний стан об’єкта контролю з точки зору апаратної складової, а стрибкоподібні відхилення в сигнатурі відгуку свідчитимуть про високу імовірність виходу устаткування з ладу найближчим часом.

Висновки. У роботі представлено фізичні основи функціонування діагностичного датчика, описано його властивості, які дозволяють використовувати його для вирішення завдань контролю технічного стану конденсатора.

Представлений метод позбавлений недоліків існуючих систем контролю та має ряд переваг, до яких можна віднести:

– практична цінність запропонованого способу полягає в тому, що в реальному часі швидко та без втручання в схемотехнічні рішення об’єкта контролю безпосередньо на місці експлуатації можливо визначати фактичний технічний стан;

– економічна доцільність використання даного методу не потребує розробки СПЗ. Запропоновані в цій статті ліцензійні пакети СПЗ володіють необхідними характеристиками для обробки знятої з ДДС інформації, її візуалізації та зберігання. Для побудови автоматичної системи діагностування можна використовувати існуючі нейронні мережі, розроблені для схожих схемотехнічних рішень;

– простота використання, що не потребує спеціального навчання оператора для проведення технічного діагностування та можливість визначення технічного стану за даними лише одного діагностичного параметра.

Напрямком подальших досліджень пропонується розробка еталонних значень граничних параметрів ємності та послідовного еквівалентного опору для різних номіналів ємності електролітичних конденсаторів. Шляхом проведення форсованих випробувань статистично повної вибірки планується отримати набір значень ємності з відповідними значеннями енергетичних рівнів, для різних часових відрізків експлуатації електролітичних конденсаторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жердєв М. К., Вишнівський В. В., Сазонов Ю. І., Жиров Г. Б. Удосконалення системи ремонту пристроїв, які містять цифрові елементи // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. Випуск № 1. Київ: ВІКНУ, 2005. С. 51–57.

2. Тюрин С. Ф., Громов О. А. Разработка контрольных и диагностических тестов для КМОП элементов с избыточным базисом // Приволжский научный вестник. Ижевск: ИЦНП, 2013. Вип. 1 (17). С. 13–21.

3. Шевченко В. В. Визначення технічного стану цифрових типових елементів заміни за допомогою електромагнітного методу діагностування // Сучасні інформаційні технології у сфері безпеки та оборони. 2015. № 1. С. 136–139.

4. Волков Ю. В. Системы технического диагностирования, автоматического управления и защиты: учеб. пособ. Ч. 1. Спб: ВШТЭ СПбГУПТД, 2016. 115 с.

5. Кравчук Р. В., Стецюк О. І., Чешун В. М. Функціональний підхід в діагностуванні цифрових процесів і елементів пам’яті // Вимірювальна та обчислювальна техніка в технологічних процесах. Хмельницький національний університет. 2018. Вип. 2. С. 106–110.

6. H. Czichos, ed., Handbook of Technical Diagnostics, Springer Heidelberg, New York, 2013 // URL: https://doi.org/10.1007/978-3-642-25850-3 (дата звернення: 28.03.2023).

7. Глухов С. І. Аналіз існуючих методів діагностування типових елементів заміни радіоелектронних засобів озброєння та обґрунтування необхідності використання інформаційних технологій при їх застосуванні // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. 2016. Вип. 52. С. 12–19.

8. Погребняк С. В. Аналіз основних несправностей новітньої радіоелектронної зброї // Збірник тез доповідей науково-практичної конференції НАНУ. Львів. 2020. С. 164.

9. Ленков С. Особливості моделювання відмов відновлюваного складного технічного об’єкта з ієрархічною конструкцією структури / С. Ленков та ін. // Східноєвропейський журнал передових технологій. 2017. Вип. 4. С. 34–42.

10. Жиров Г. Б. Методика контролю технічного стану цифрових пристроїв енергостатичним методом на місці дислокації об’єктів РЕЗО // Збірник наукових праць Одеського ордена Леніна ін-ту Сухопутних військ. 2005. Вип. 11. С. 55–61.

11. Жердєв М. К., Вишнівський В. В., Жиров Г. Б. Контроль технічного стану цифрових пристроїв енергостатичним методом // Зб. наук. пр. ВІТІ НТУУ «КПІ». 2005. № 1. С. 51–57.

12. Вишнівський В. В., Гахович С. В., Катін П. Ю., Круценко В. В. Пристрій для діагностування цифрових ТЕЗ з використанням енергодинамічного процесу // Вісник Військового інституту Київського національного університету ім. Т. Шевченка. 2003. Вип. № 6. С. 70–74.

13. Про затвердження Положення про технічне забезпечення зв’язку в Національній гвардії України: наказ МВС від 06.11.2015 № 1384 // Верховна Рада України: офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/z1499-15#n12 (дата звернення: 28.03.2023).

14. Вишнівський В. В., Жердєв М. К., Креденцер Б. П., Кузавков В. В., Редзюк Є. В. Безконтактний індукційний метод діагностики радіоелектронних блоків // Збірник наукових праць Військового інституту КНУ ім. Т. Шевченка. 2013. Вип. 43. С. 17–23 // Національна бібліотека ім. В І. Вернадського. URL: http://nbuv.gov.ua/UJRN/Znpviknu_2013_43_5 (дата звернення: 28.03.2023).

15. Погребняк С. В. Індуктивний метод як перспективний спосіб діагностики технічного стану вторинних джерел живлення // Modern Scientific research Achievements innovation and development prospects: VIII International scientific and practical conference, Berlin, Germany, 23–25.01.2022. P. 258–260.

16. Кузавков В. В., Гайдур Г. І., Сєрих С. А., Редзюк Є. В. Безконтактний індукційний метод визначення технічного стану цифрового блоку: розрахунок потужності випромінювання провідника // Зв’язок. Державний університет зв’язку. Київ, 2016. Вип. 1. С. 32–39.

17. Сегеда М. С., Мазур Т. А. Математичне моделювання вільних коливань в обмотці трансформатора при різних формах імпульсу напруги // Інтелектуальні енергетичні системи (ESS13): матеріали 3 Міжнародної науково-технічна конференції, м. Мукачеве, 10–14 червня 2013 р. 235 с.

18. Бабаєв М. М., Давиденко М. Г., Загарій Г. І., Соболєв Ю. В. Лінійні електричні схеми пристроїв автоматики та зв’язку: навч. пос. Харків: УкрДАЗТ, 2007. 285 с.

19. Аврутов В. В., Бурау Н. И. Надежность и диагностика приборов и систем НТУУ «КПІ». Киев, 2014. 158 с.

20. Yu Tack Kim, Simulation study on the lifetime of electrochemical capacitors using the accelerated degradation test under temperature and voltage stresses / Yu Tack Kim, Kwang-Bum Kim, Yoo Eo Hyun, Ick-Jun Kim, Sunhye Yang // Microelectronics Reliability, Volume 55, Issue 12, Part B, 2015, pp. 2712–2720.

21. Чжао, З., Даварі, П., Лу, В., Ван, Х., Блайберг Ф. Огляд методів моніторингу стану конденсаторів у програмах ланцюгів постійного струму. IEEE Trans. Силовий Електрон. 2021. № 36. 3692–3716.

22. Ву, Ю., Ду, Х. Метод моніторингу стану VEN конденсаторів ланцюгів постійного струму для перетворювачів енергії. IEEE Trans. Пром Електрон. 2019, 66, 1296–1306.

23. Мяо, В., Лю, Х., Лам, КН, Понг, PWT Моніторинг стану електролітичних конденсаторів у підвищуючих перетворювачах за допомогою магнітних датчиків. IEEE Sens. J. 2019, 19, 10393–10402.

24. Ю, Ю., Чжоу, Т., Чжу, М., Ху Д. Діагностика несправностей і прогнозування терміну служби алюмінієвих електролітичних конденсаторів постійного струму, які використовуються в трифазних перетворювачах змінного/постійного/змінного струму // Матеріали Другої Міжнародної конференції 2012 року з приладобудування, вимірювань, комп’ютерів, зв’язку та управління, Харбін, Китай, 8–10 грудня 2012 р. С. 825–830.

25. H. Wang і F. Blaabjerg, «Надійність конденсаторів для програм постійного струму в силових електронних перетворювачах – огляд», IEEE Trans. Інд. При., Вип. 50, № 5, 2014. С. 3569–3578,

26. H. Wang, P. Davari, H. Wang, D. Kumar, F. Zare, and F. Blaabjerg “Lifetime estimation of dc-link capacitors in adjustable speed drives under grid voltage unbalances,” IEEE Trans. Power Electron., vol. 34, № 5. 2019, pp. 4064–4078.

27. W. Miao, X. Liu, K. H. Lam, and P. W. T. Pong, “Condition monitoring of electrolytic capacitors in boost converters by magnetic sensors,” IEEE Sens. J., vol. 19, № 22. 2019, pp. 10393–10402.

28. L. Ren and C. Gong, “Online estimation scheme of output capacitor’s ESR and tanδ for Buck converter”, IET Power Electron., vol. 12, № 11. 2019, pp. 2978–2986.

29. A. M. R. Amaral and A. J. M. Cardoso, “On-line fault detection of aluminum electrolytic capacitors, in step-down dc-dc converters, using input current and output voltage ripple,” IET Power Electron., vol. 5, № 3. 2012, pp. 315–322.

30. H. Givi, E. Farjah, and T. Ghanbari, “A comprehensive monitoring system for online fault diagnosis and aging detection of non-isolated dc–dc converters’ components,” IEEE Trans. Power Electron., vol. 34, № 7. 2019, pp. 6858–6875.

31. H. Wang, M. Liserre, and F. Blaabjerg, “Toward reliable power electronics: Challenges, design tools, and opportunities,” IEEE Ind. Electron. Mag., vol. 7, № 2. 2013, pp. 17–26.

32. Hoanglong Dang, Hyejin Park, Sangshin Kwak, Seungdeog Choi DC-Link Electrolytic Capacitors Monitoring Techniques Based on Advanced Learning Intelligence Techniques for Three-Phase Inverters MDPI. Machines. 2022, 10, 1174. URL: https://www.researchgate.net/publication/366115422 (дата звернення: 14.04.2023).

DOI: 10.58254/viti.3.2023.07.56

УДК 621.391.372

Лазута Р. Р. ORCID: 0000-0003-3254-9690 (ВІТІ ім. Героїв Крут)
Бондаренко Л. О. ORCID: 0000-0003-1850-0508 (ВІТІ ім. Героїв Крут)
Макарчук В. І. ORCID: 0000-0002-3997-4684 (ВІТІ ім. Героїв Крут)
Руденко В. І. ORCID: 0000-0003-3563-5482 (ВІТІ ім. Героїв Крут)

МЕТОД ОЦІНКИ ЖИВУЧОСТІ РОЗПОДІЛЕНИХ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З ПОЗИЦІЙ ТЕОРІЇ РИЗИК-МЕНЕДЖМЕНТУ

Різноманітність мереж електронних комунікацій спеціального призначення, процесів їхнього руйнування та відновлення роблять проблему розроблення методологічних засад оцінювання їхніх ключових характеристик вкрай затребуваною під час проведення оперативних розрахунків посадовими особами органів управління зв'язком.

Залишається так само актуальною і проблема раціонального та оптимального задіяння ресурсів, що збереглися в системі, спрямованих на виконання критично важливих функцій системи після інтенсивного впливу на неї зовнішніх дестабілізаційних впливів. Розв'язання цієї проблеми вимагає від системи нових якостей, яких вона може і не мати, якщо спроєктована для роботи тільки в певних умовах експлуатації.

З огляду на вищевикладені проблеми до властивості живучості та їхніх особливостей, які широко застосовують у створенні складних систем різного призначення, висувають низку особливих вимог, які стосуються як структурної, так і функціональної частини складних систем.

Одним із природних показників кількісного вимірювання ефективності мереж електронних комунікацій спеціального призначення є показник живучості, що зберігся у системи після фіксованої сукупності дестабілізуючих впливів. Показник ефективності є мірою (метричною або у вигляді шкали балів у відповідних модифікаціях) ступеня відповідності необхідному реального результату виконання встановлених функціональних завдань після впливу дестабілізуючих впливів.

Для того щоб показник ефективності, визначений на безлічі стратегій, міг розглядатися як характеристики функціонування системи, він повинен задовольняти наступним вимогам: змістовності та інтерпретованості, вимірності, відповідності системі переваг особи, що приймає рішення.

Оскільки рішення особи, що приймає рішення щодо побудови та бойового застосування мереж електронних комунікацій спеціального призначення, є визначальним, то розрахунки показника ефективності мереж доцільно проводити з позиції моделі управління ризиками (ризик-менеджменту).

Ключові слова: *живучість, ефективність функціонування системи, ризик-менеджмент.*

R. Lazuta, L. Bondarenko, V. Makarchuk, V. Rudenko A method for assessing the resistance of distributed networks of electronic communications for special purpose from the position of the theory of risk management.

The diversity of special-purpose electronic communications networks, their destruction and restoration processes make the problem of developing methodological bases for evaluating their key characteristics highly demanded during operational calculations by officials of communication management bodies.

The problem of rational and optimal use of the resources preserved in the system aimed at performing critically important functions of the system after the intense impact of external destabilizing influences on it remains just as relevant. Solving this problem requires new qualities from the system, which it may not have if it is designed to work only in certain operating conditions.

In view of the above-mentioned problems with the properties of survivability and their features, which are widely used in the creation of complex systems of various purposes, a number of special requirements are put forward that relate to both the structural and functional parts of complex systems. One of the natural indicators of the quantitative measurement of the effectiveness of special purpose electronic communications networks is the survivability index that has remained in the system after a fixed set of destabilizing influences.The efficiency indicator is a measure (metric or in the form of a scale of points in the appropriate modifications) of the degree of compliance with the required real result of the performance of the established functional tasks, after the impact of destabilizing influences.

In order for the performance indicator, determined on the basis of many strategies, to be considered as a characteristic of the functioning of the system, it must satisfy the following requirements: content and interpretability, measurement, compliance with the system of preferences of the decision-maker.

Since the decision of the person making the decision on the construction and combat use of special-purpose electronic communications networks is decisive, it is advisable to calculate the network efficiency indicator from the standpoint of the risk management model.

Keywords: *survivability, efficiency system operation, risk management.*

Постановка завдання. Поняття живучості з часом еволюціонує і набуває нового змісту, що тягне за собою не завжди своєчасне закріплення цього поняття у нормативних документах.

У зв’язку з цим у наукових публікаціях та в практиці планування бойового застосування мереж електронних комунікацій спеціального призначення (далі – МЕК СП) спостерігається відсутність єдиного підходу до аналізу та оцінки можливих варіантів побудови оптимальної технічної основи системи управління військами та зброєю.

Відсутність єдиних моделей живучості породжує велику різноманітність запропонованих методів дослідження, а отже, і показників живучості. Таке положення дозволяє зробити висновок про те, що точні визначення та поняття в теорії живучості не сформовані належним чином. Водночас є різні методики з питань оцінки живучості різних технічних систем, що оперують різною термінологією та критеріями, що викликає труднощі або неможливість їх застосування при плануванні МЕК СП.

У цій публікації досліджується сутність питання живучості МЕК СП, що дозволить уточнити стандартизовані визначення та систематизувати підходи до розробки методів аналізу мереж за показником живучості з позицій моделі управління ризиками (ризик-менеджменту).

Актуальність викладеного матеріалу полягає в тому, що відсутність єдиних підходів, а відтак і єдиних методів аналізу ефективності побудови МЕК СП, ускладнює ухвалення рішень особою, що приймає рішення (далі – ОПР), щодо розгортання оптимальної за складом та ефективної за функціональним призначенням технічної основи управління військами та зброєю. Розмаїття телекомунікаційних мереж, процесів їх руйнування та відновлення роблять проблему розробки методологічних засад оцінки живучості ієрархічних МЕК СП вкрай затребуваною під час проведення оперативних розрахунків органів управління зв’язком (далі – ОУЗ). Вирішення зазначеної проблеми полягає в подальшому вивченні глибинної суті проблеми, її опису та пропозиції нових методів вирішення цього актуального завдання.

Аналіз останніх досліджень і публікацій. У публікації [2] представлені методики, що застосовуються для аналізу структурованих мереж, в яких враховується їх зв’язність. Однак пріоритетам важливості (вагомості) діючих у системі функціональних взаємозв’язків належного значення не надається.

У публікації [3] цей недолік усунений, але в ній не передбачається оцінка ступеня здатності мережі в цілому функціонувати після шкідливих впливів на її елементи.

Методика, запропонована в [4], спрямована на оцінку живучості мереж з погляду їх функціональності з урахуванням ієрархічних взаємозв’язків. Але в цій роботі структурний аспект живучості представлений лише одним видом взаємозв’язків і до того ж без урахування їхньої значущості.

У публікації [5] розроблено методику оцінки живучості складних систем військового призначення, що дозволяє отримувати комплексну оцінку живучості системи з точки зору її структурної вразливості та функціональності. Однак застосовуваний математичний апарат для моделювання поширення зовнішніх впливів по структурі системи не повністю враховує всі можливі наслідки небажаних впливів.

У деяких роботах, наприклад, [6; 7], подана досить змістовна класифікація властивостей та показників живучості. Однак методики визначення показників у наведених роботах не повною мірою враховують вплив на живучість МЕК СП умов застосування об’єкта дослідження. Саме цим і пояснюється велика кількість показників живучості та відсутність будь-якого взаємозв’язку між ними.

У публікації [8] розроблено методику порівняльної оцінки розподілених інформаційно-телекомунікаційних мереж на предмет їхньої здатності забезпечувати інформаційний обмін між кореспондентами в умовах випадкових та навмисних (комп’ютерні атаки, використання недекларованих можливостей програмного забезпечення) програмних перешкод (деструктивних програмних впливів).

Таким чином можна вважати, що на даний момент у теорії живучості МЕК СП не позначений усталений методологічний підхід, що дозволяє вирішувати задачу комплексної оцінки живучості складної системи з точки зору її структурної вразливості та функціональності з урахуванням значущості взаємозв’язків, що існують в системі.

Метою статті в умовах відсутності єдиних підходів та методів аналізу живучості МЕК СП є:

встановлення залежностей між сформованими науковими та класифікаційними поняттями живучості МЕК СП, що оперують різною термінологією;

встановлення взаємозв’язку між термінами та їхніми визначеннями;

визначення шляхів вирішення проблеми оцінки живучості МЕК СП та пропозиція методів її вирішення.

Виклад основного матеріалу. Розглянемо загальнотехнічні визначення живучості, наведені у [9–12].

У [9] під живучістю розуміється «здатність системи військового зв’язку забезпечувати управління військами [силами] в умовах дії зброї противника».

Це визначення близьке за змістом до визначення [10], де «живучість – здатність системи військового зв’язку і автоматизації виконувати завдання за призначенням в умовах дії зброї противника».

У [11] під живучістю розуміється здатність систем до збереження своїх основних функцій (хоча б із допустимою втратою якості їх виконання) при впливі факторів зовнішнього середовища катастрофічного характеру – несприятливих умов експлуатації.

В [12] живучість визначена як властивість об’єкта, що полягає в його здатності виконувати задане призначення в процесі несприятливих впливів на весь об’єкт або окремі його компоненти, підтримуючи в допустимих межах свої експлуатаційні показники.

У цих визначеннях слід звернути увагу на таке:

по-перше, живучість слід розглядати як внутрішню властивість системи, якою вона володіє незалежно від умов функціонування, що виникають в даний момент часу. Вона володіє ним завжди і певною мірою може проявлятися за нормальних умов функціонування, коли виникають відмови елементів, які викликані виробничими дефектами, старінням, відхиленням параметрів тощо. Але повною мірою живучість проявляється при великих зовнішніх впливах, не передбачених умовами нормальної експлуатації, і тому важко прогнозувати, оскільки вони створюють у системі екстремальні умови функціонування;

по-друге, живучість проявляється у тому, що система зберігає не всі функції, які вона має виконувати при нормальній роботі, а лише основні функції, та й то з можливим зниженням якості виконання. Це означає, що можлива зміна стратегії функціонування системи зі збільшенням тяжкості несприятливих впливів;

по-третє, система повинна мати властивість поступової деградації в міру збільшення тяжкості несприятливих наслідків і для кожного рівня таких наслідків вміти оперативно і максимально ефективно використовувати ресурси, що збереглися, для виконання основних функцій з урахуванням зміни стратегії функціонування (цільової функції), а надалі реалізувати оптимальну стратегію відновлення з урахуванням обмежень.

Спираючись на аналіз визначень властивості живучості МЕК СП, наведених вище, представляється можливим уявити визначення живучості з погляду класичної «теорії ризику» як «можлива подія, яка може завдати шкоди чи втрати, або впливати на досягнення цілей». Ризик визначається ймовірністю загрози, вразливістю активу стосовно цієї загрози та впливом, якщо ця подія станеться. Ризик також може бути визначений як невизначеність кінцевого результату та використовуватись у контексті вимірювання ймовірності як негативних, так і позитивних результатів [13].

Нормативними документами, що визначають загальний підхід до управління будь-якими ризиками, є стандарти Міжнародної організації зі стандартизації (англ. *International Organization for Standardization, ISO*) [14] та Державний стандарт України [15]. Зазначені стандарти не є вузькоспеціальними чи галузевими, а порядок застосування цих рекомендацій

може бути адаптований для будь-якої організації та її контексту, включаючи прийняття рішень на всіх рівнях протягом усього життєвого циклу системи [14; 15].

У [15] ризик визначено як «вплив невизначеності на цілі». Ризик зазвичай визначається у термінах джерел ризику, потенційних подій, наслідків цих подій та його ймовірності. «Вплив» розглядається як відхилення від очікуваного і може бути позитивним та/або негативним, а також може сприяти реалізації можливостей та усунення загроз, створювати чи призводити до виникнення можливостей та загроз. Цілі можуть мати різні аспекти і категорії та можуть застосовуватися на різних рівнях.

Ризик-менеджмент (risk-management) – це скоординовані дії управління організацією (процесом) з урахуванням ризику [14; 15].

Процес функціонування системи передбачає систематичне застосування політик, процедур та практик для забезпечення обміну інформацією та консультування, визначення контексту (середовища, в якому МЕК СП повинні виконувати свої функціональні завдання з найбільшою ефективністю), а також оцінки ризиків, впливу на ризики, моніторингу, аналізу та документування ризиків, а також ведення звітності щодо ризиків. Процес ризик-менеджменту показаний на рисунку 1.

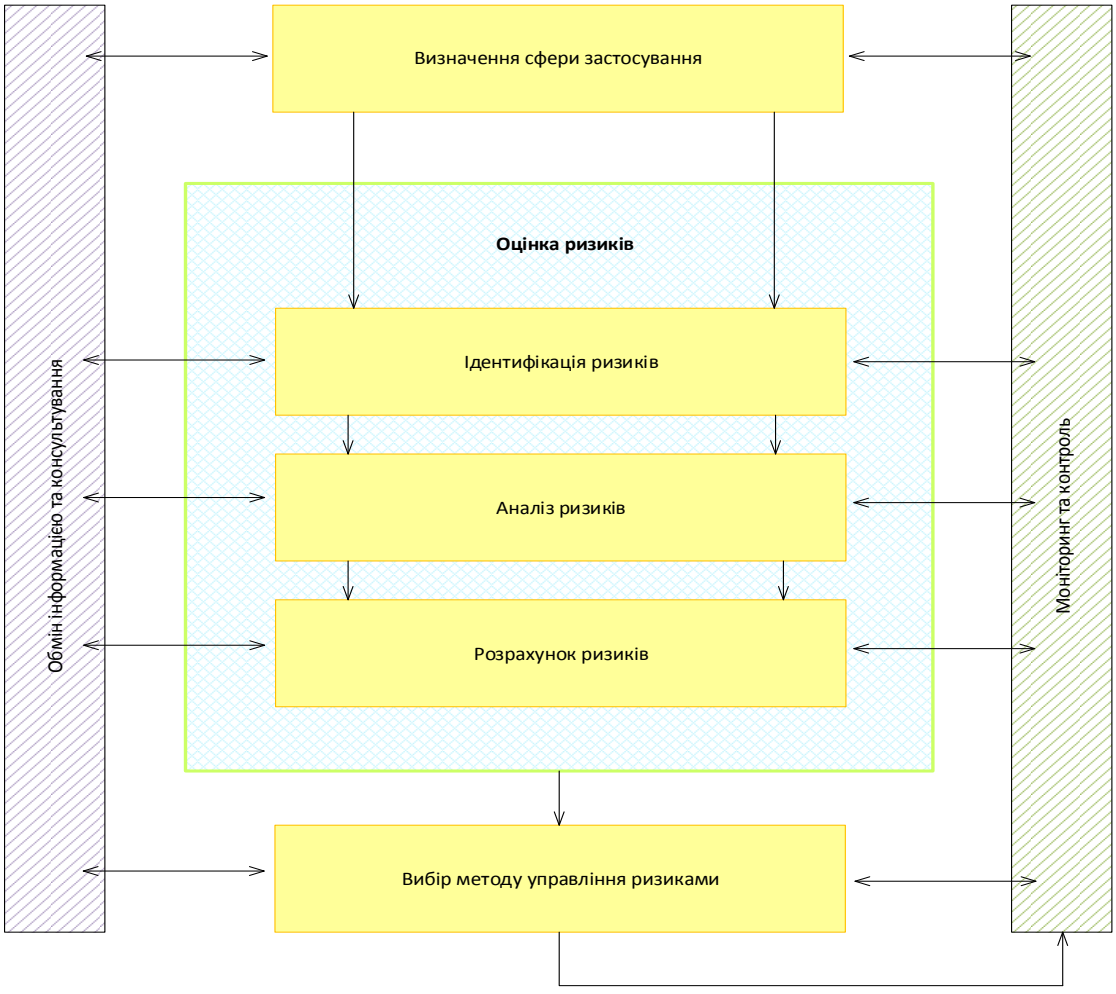


Рис. 1. Процес ризик-менеджменту

Процес ризик-менеджменту має бути невід’ємною частиною процесів управління та прийняття рішень та має бути інтегрований у структуру, діяльність та процеси функціонування ОУЗ. Він повинен застосовуватись на всіх етапах життєвого циклу МЕК СП.

У рамках ОУЗ процес ризик-менеджменту може мати безліч варіантів застосування, адаптованих з урахуванням необхідності досягнення цілей, а також зовнішнього та внутрішнього контексту.

Протягом усього процесу ризик-менеджменту слід враховувати динамічний та мінливий характер поведінки МЕК СП та посадових осіб ОУЗ.

Обмін інформацією та консультування проводяться з метою:

– зведення різних галузей експертних знань воєдино на кожному етапі процесу ризик-менеджменту;

– забезпечення належного обліку різних поглядів щодо критеріїв ризику та їхньої оцінки;

– надання достатньої інформації для полегшення контролю за ризиками та прийняття рішень.

Обмін інформацією спрямований на підвищення обізнаності та забезпечення розуміння ризику, тоді як консультування включає отримання зворотного зв’язку та інформації для обґрунтування прийнятих рішень.

Мета ідентифікації ризиків полягає в пошуку, визначенні та описі ризиків, які можуть допомогти або завадити досягненню цілей. Для ідентифікації ризиків важливо використовувати належну, відповідну та актуальну інформацію. ОУЗ слід ідентифікувати ризики незалежно від того, чи знаходяться джерела цих ризиків під її контролем.

Аналіз ризику може проводитися з різним ступенем деталізації та складності, залежно від мети аналізу, доступності та достовірності інформації та наявних ресурсів. Методи аналізу можуть бути якісними, кількісними або їх комбінаціями, залежно від конкретних обставин та передбачуваного використання результатів.

Аналіз ризику слід проводити з урахуванням таких факторів, як:

– ймовірність подій та наслідків;

– характер та масштаби наслідків;

– складність і пов’язаність компонентів;

– фактори, пов’язані з часом;

– ефективність існуючих засобів контролю;

– чутливість та достовірність.

На аналіз ризиків може впливати будь-яка розбіжність думок, упередженість, сприйняття ризику та судження.

Метою оцінювання ризику є сприяння ухваленню рішень. Оцінювання ризику включає порівняння результатів аналізу ризику зі встановленими критеріями ризику визначення необхідності додаткових дій. Цей процес може призвести до вирішення:

– більше нічого не робити;

– розглянути можливі варіанти впливу на ризик;

– провести подальший аналіз, щоб краще зрозуміти ризик;

– підтримувати наявні засоби контролю;

– переглянути цілі.

Розрахунки ризиків проводяться із застосуванням відповідного математичного апарату та обчислювальних систем.

Мета впливу на ризик полягає у виборі та застосуванні варіантів реагування на ризик у процесі функціонування МЕК СП.

Вибір методу та управління ризиками (вплив на ризик) є ітеративним процесом, що включає:

– вибір варіантів впливу на ризик;

– підготовку та реалізацію планів впливу на ризик.

Моніторинг і контроль охоплюють планування, збір та аналіз інформації, документування результатів і надання зворотного зв’язку. Результати моніторингу та контролю мають бути частиною діяльності ОУЗ із загального управління МЕК СП, оцінки її ефективності, а також складання звітності.

Процеси ризик-менеджменту добре узгоджується з принципами системного аналізу, головним завданням якого є вивчення проблемної ситуації, з’ясуванням її причин,

виробленням варіантів її усунення, прийняттям рішення та організацією подальшого функціонування системи, що вирішує проблемну ситуацію [16].

Метою застосування системного аналізу, як і ризик-менеджменту, є підвищення ступеня обґрунтованості прийнятого рішення, розширення безлічі варіантів, серед яких проводиться обґрунтований вибір.

Методи та процедури системного аналізу спрямовані на виявлення цілей, висування альтернативних варіантів вирішення проблем, виявлення масштабів невизначеності по кожному з варіантів та зіставлення варіантів за тими чи іншими критеріями ефективності, а також пов’язаних організаційних завдань, що також стосується процесів ризик-менеджменту.

Окрему групу завдань системного аналізу складають завдання дослідження комплексу взаємодій аналізованих об’єктів із зовнішнім середовищем та альтернатив розвитку системи у часі та у просторі.

У системному аналізі використовується сучасний математичний апарат та обчислювальні системи, а також об’єднання формальних та неформальних методів аналізу та синтезу з використанням імітаційних моделей.

Виявлення та вирішення проблем управління в ієрархічних системах, вибір їх оптимальної структури, режимів функціонування та організації взаємодії між підсистемами будується на спільній роботі системних аналітиків, побудованої на принципах [16]:

– *принцип кінцевої мети* (абсолютний пріоритет кінцевої (глобальної) мети);

– *принцип єдності* (спільний розгляд системи як цілого сукупності елементів);

– *принцип функціональності* (спільний розгляд структури та функції з пріоритетом функції над структурою);

– *принцип розвитку, адаптації* (облік змінності системи, її здатність до розвитку, адаптації, розширення, заміни частин, нарощування, удосконалення, накопичення інформації);

– *принцип ієрархії* (введення частин та їх ранжування з метою встановлення порядку їх розгляду);

– *принцип зв’язності* (виявлення зв’язків між елементами системи та виявлення зв’язків із зовнішнім середовищем (облік зовнішнього середовища);

– *принцип невизначеності* (облік невизначеностей та випадковостей у системі);

– *принцип еквіфінальності* (досягнення системою необхідного кінцевого стану виключно власними характеристиками);

– *принцип модульної побудови* (виділення модулів у системі та розгляд її як сукупності модулів).

Перелічені принципи системного аналізу мають високий ступінь спільності з процесами ризик-менеджменту як за цілями, так і засобами їх реалізації.

Універсальним засобом дослідження різних властивостей складних організаційно-технічних систем довільної природи є методи теорії графів, оскільки вони дозволяють адекватно відображати їх склад, структуру, функціонування різних рівнів декомпозиції.

Для аналізу та наближеної оцінки живучості МЕК СП може бути застосована математична модель у вигляді ймовірності зваженого графа, вершинам якого відповідають вузли та комплекси засобів зв’язку, а ребрам – канали зв’язку, що їх з’єднують [17].

Центральною ідеєю дослідження складних організаційно-технічних систем методом моделювання за допомогою графів є те, що на кожному кроці моделювання, зокрема імітаційного, граф будь-якої природи із довільними властивостями стає детермінованим із фіксованими значеннями параметрів властивостей [17].

Так, якщо структура графа є ймовірністю виваженою, то шляхом розіграшу ймовірностей існування вершин та ребер фіксується конкретна реалізація структури, тобто з вихідного графа виключається частина вершин та ребер. Якщо значення параметрів властивостей залежить від часу, то фіксується момент часу, з якого обчислюється значення параметрів властивостей. У якості вагових коефіцієнтів вершин використовуються

ймовірності збереження вузлів при заданій моделі завдання ударів, а як вагові коефіцієнти каналів зв'язку – ймовірності їх збереження при заданій моделі постановки перешкод. Можливість одночасного обліку у моделі впливу противника зброєю на вузли (центри зв'язку) та перешкодами на канали зв'язку розширює можливості моделі на оцінку стійкості МЕК СП. Як показник живучості використовується ймовірність збереження шляху передачі інформації між довільними вузлами зв'язку і та сама ймовірність, але за умови, що кількість транзитів може обмежуватися.

З урахуванням викладеного методику аналізу критичності окремих елементів МЕК СП пропонується будувати на вимогах щодо проведення аналізу критичності відмов елементів складних систем, викладених у [18]. Для МЕК СП можливі три основні види відмов їх елементів множини *C(a,b)*:

1) відмови, які впливають на виконання критичної функції ($F_{\text{кр}}$) МЕК СП загалом;

2) відмови, що призводять до погіршення якісних та/або часових характеристик виконання функціональних завдань, але які не призводять до критичного стану саму МЕК СП або призводять до частково працездатного її стану;

3) відмови, що призводять до критичного стану МЕК СП (при цьому неминучий значний збиток для системи в цілому при виконанні функціональних завдань).

На першому етапі проводиться аналіз критичності безлічі функцій F, що виконуються системою, з паралельним розкладанням графа МЕК СП на приватні підграфи окремих підсистем, що виконують критичні функції $F_{\text{кр}}$.

На другому етапі кожна з даних $F_{\text{кр}}$ розкладається на безліч простих завдань (процесів), виконання яких обумовлює нормальне функціонування відповідної підсистеми МЕК СП.

Третій етап аналізу полягає у визначенні кратності використання окремих елементів підсистем МЕК СП у вирішенні критичних завдань, що забезпечують виконання $F_{\text{кр}}$.

На четвертому етапі проводять розрахунок нормованого показника кратності критичності кожного з елементів підсистем МЕК СП.

Як було зазначено, на першому етапі аналізу критичності елементів МЕК СП з безлічі функцій F, покладених на неї у нормальних умовах експлуатації, виділяють групу $F_{\text{кр}} - F^*$, порушення виконання яких може призвести до критичних станів системи. Таким чином, формується група з i функцій для даної МЕК СП, виконання яких повинно забезпечуватися навіть в екстремальних умовах експлуатації. Якісні характеристики виконання цих $F_{\text{кр}}$ будуть визначальними для якості живучості системи.

Далі з кожної $F_{\text{кр}}$ f_n^* (n=1,....i) формується власний підграф $G(a,b)$, що містить всі елементи, які беруть участь (можуть брати участь) у її реалізації, шляхом розбиття графа $G(a,b)$ на підграфи $G(a,b)$. Підграфи мають, як правило, ієрархічну структуру, що відображає взаємозв'язок керуючого та керованих елементів підсистеми. Для кожного з підграфів G формуються масиви $M_n(c_k)$ з елементів, що входять до них і одновимірні масиви $M_{\text{Ж}_b}(p_c)$ відповідних їм показників живучості.

Другим етапом є процедура формування множин Z_nприватних завдань z_{nj} (j=1,...,e) щодо прийому, зберігання, обробки та видачі інформаційних та керуючих повідомлень (команд, сигналів), що виконуються групами елементів та/або окремими елементами, які входять до підграфа G даної $F_{\text{кр}}$. Таким чином на другому етапі формується i груп критичних завдань, що полегшують подальше визначення безлічі критичних елементів МЕК СП. Результати визначення безлічі критичних завдань заносяться до i одновимірних масивів M_{Z_n}.

На третьому етапі проводиться аналіз критичності окремих елементів c_k ($k = 1, \dots g$) кожної з функціональних підсистем МЕК СП. При цьому для кожного з i-підграфа G формуються матриці критичності $M_{F_{\text{крп}}}(z_{nj}, c_k)$ з елементів c_k що входять до їх складу. Елементи даних матриць m_{jk} на перетині рядків, відповідних певним критичним завданням z_{nj}, зі стовпцями, відповідними елементам c_k аналізованого підграфа, заповнюються числовими значеннями відповідно до правил:

1) якщо відмова елемента c_k для даної критичної задачі z_{nj} відноситься до виду 1 – значення елемента m_{jk} матриці $M_{F_{\text{крп}}}(z_{nj}, c_k)$ дорівнює 0;

2) якщо відмова елемента c_k для даної критичної задачі z_{nj} відноситься до виду 2 – значення елемента m_{jk} матриці $M_{F_{\text{крп}}}(z_{nj}, c_k)$ дорівнює 0,5;

3) якщо відмова елемента c_k для даної критичної задачі z_{nj} відноситься до виду 3 – значення елемента m_{jk} матриці $M_{F_{\text{крп}}}(z_{nj}, c_k)$ набуває значення 1;

4) якщо для виконання критичної задачі z_{nj} використовуються d паралельно включених однотипних структурних елементів c_k, що входять в аналізований підграф Gn, то відповідний елемент m матриці $M_{F_{\text{крп}}}(z_{nj}, c_k)$ прийме значення в d разів менше значення, що визначається за правилами 1–3.

Четвертим етапом аналізу є визначення кількісного значення показника кратності критичності – v_k всіх структурних елементів c_k кожної з i функціональних підсистем МЕК СП.

Визначення кількісного значення v_k проводиться у чотири дії:

1) визначення абсолютного значення величини критичності $m_{\sum k}$ елемента c_k n-ї підсистеми МЕК СП шляхом підсумовування значень всіх елементів m_{jk} k-го стовпця матриці критичності $M_{F_{\text{крп}}}(z_{nj}, c_k)$;

2) визначення сумарного значення критичності $m_{\sum k}$ всіх елементів c_k n-ї підсистеми МЕК СП шляхом підсумовування значень $m_{\sum k}$ всіх елементів c_k, що утворюють цю підсистему;

3) визначення нормованого значення величини критичності $\{m_{\sum k}\}$ для кожного елемента c_k n-ї підсистеми МЕК СП згідно з виразом (1):

$$\{m_{\sum k}\} = \frac{m_{\sum k}}{m_{\sum n}}; \tag{1}$$

4) розрахунок значення показника v_k проводити за формулою (2):

$$v_k = \frac{1}{m_{\sum k}}. \tag{2}$$

Результатом проведення аналізу критичних відмов елементів МЕК СП відповідно до запропонованої методики буде i одновимірних масивів $V_n(c_k)$, що містять значення показника кратності критичності v_k всіх g елементів критичних підсистем МЕК СП [19; 20].

Для оцінки живучості МЕК СП загалом необхідно провести оцінку живучості множини i критичних підсистем з урахуванням критичності їх окремих елементів.

Як було зазначено, практично всі підсистеми МЕК СП матимуть ієрархічну структуру. Тому при оцінці їх живучості в запропонованому методі пропонується використовувати як відомі підходи (детерміновану оцінку та імітаційну модель оцінки структурної живучості ієрархічних систем), так і математичний апарат, що враховує показник кратності критичності елементів, що забезпечують функціональну живучість визначальних підсистем.

Для подальшого проведення обчислень приймемо дві умови:

1) система має живучість, якщо всі i критичних підсистем мають мінімально-допустимий рівень живучості;

2) система залишається частково працездатною в екстремальних умовах експлуатації, якщо у кожній підсистемі залишається хоча б один шлях комунікації між різними рівнями ієрархії.

Для кількісної оцінки живучості n-ї критичної підсистеми МЕК СП пропонується використовувати мінімальне та середнє значення комплексного показника S_n, що визначається як показник живучості, який враховує її структуру та кратність критичності окремих елементів, що входять до підсистеми.

Для розрахунку мінімального значення комплексного показника живучості S_{nMIN} n-ї підсистеми МЕК СП при кратності впливів факторів, що дестабілізують l, використовується вираз (3) [19; 20]:

$$S_{nMIN}^{l} = min_Y \left\{ \prod_{k-1}^{g} \left[p_B \left[M_{B_y}(c_k) \right] \right] \times \left(1 - p_B[M_n(c_k)] - M_{B_y}(c_k) \right) \right] \times K_y \times \sum_{M_{B_y}(c_k)} v_k \right\}, \quad (3)$$

де Y – безліч можливих станів підсистеми з елементів g при l впливах дестабілізуючих факторах, як вказано у виразі (4):

$$Y = C_l^g = \frac{g!}{l!(g-l)!}\ ; \quad (4)$$

K_y – показник якості функціонування підсистеми в y-му стані, що визначається з виразу (5):

$$K_y = \frac{u_y}{U}, \quad (5)$$

де u_y – кількість нормально функціонуючих вузлів нижнього рівня ієрархічної структури підсистеми МЕК СП мають можливість обміну інформацією з керуючим вузлом верхнього рівня в y-му стані;

U – загальна кількість вузлів нижнього рівня ієрархічної структури даної підсистеми МЕК СП;

$p_B[M_n(c_k)]$ – ймовірність виживання елемента c_k множини $M_{B_y}(c_k)$ – елементів, що вижили в стані y підсистеми;

$p_B[M_n(c_k)] - M_{B_y}(c_k)]$ – ймовірність виживання елемента c_k з безлічі елементів $[M_n(c_k)]$ даної n-ї підсистеми загиблих у аналізованому y-му стані (не увійшли до $M_{B_y}(c_k)$);

v_k – кратність критичності елемента c_k даної підсистеми МЕК СП.

Для розрахунку середнього значення комплексного показника живучості S_n n-ї підсистеми МЕК СП при кратності l впливів дестабілізуючих факторів використовується вираз (6):

$$\overline{S_n^l} = \frac{\sum_{y=1}^{Y} \left\{ \prod_{k=1}^{g} \left[p_B \left[M_{B_y}(c_k) \right] \right] \times \left(1 - p_B[M_n(c_k)] - M_{B_y}(c_k) \right) \right] \times K_y \times \sum_{M_{B_y}(c_k)} v_k \right\}}{Y}. \quad (6)$$

Фізичний зміст запропонованого показника близький до функції живучості F, оскільки за його допомогою можна простежити зміни живучості кількості впливів дестабілізуючих чинників.

Для аналізу живучості МЕК СП загалом доцільно використовувати безліч найменших значень показника S_{nMIN}, i усереднених значень показників S_n, що визначаються для безлічі критичних підсистем при заданих значеннях кратності l впливу дестабілізуючих факторів.

Висновки. У роботі проведено аналіз різних за змістом термінів, що визначають поняття живучості МЕК СП та встановлені залежності між сформованими науковими та класифікаційними поняттями. Встановлені взаємозв'язки між термінами та їхніми визначеннями.

Проведено аналіз визначень властивості живучості МЕК СП з погляду класичної «теорії ризику». Проведено аналіз процесів ризик-менеджменту щодо їх узгодження з принципами системного аналізу, головним завданням якого є вивчення проблемної ситуації, з'ясуванням її причин, виробленням варіантів її усунення, прийняттям рішення та організацією подальшого функціонування системи, що вирішує проблемну ситуацію.

Розглянута та запропонована математична модель наближеної оцінки живучості МЕК СП у вигляді ймовірності зваженого графа, вершинам якого відповідають вузли та комплекси засобів зв'язку, а ребрам – канали зв'язку, що їх з'єднують. Визначені шляхи вирішення проблеми оцінки живучості МЕК СП та надана пропозиція щодо методів її вирішення .

Запропоновано оцінку живучості МЕК СП, заснованої на безлічі показників, що дозволяє проводити аналіз живучості та обґрунтований вибір найкращого архітектурно-структурного варіанта побудови (реконфігурації) мереж та їх критичних підсистем.

Подальші шляхи досліджень пов'язані з пошуком шляхів підвищення живучості МЕК СП в умовах масованого застосування противником безпілотних літальних апаратів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Надежность и эффективность в технике. Справочник: в 10 т. / Ред. совет: В. С. Авдуевский (пред.) и др. М.: Машиностроение, 1988. Т. 3. Эффективность технических систем / Под общ. ред. В. Ф. Уткина, Ю. В. Крючкова. С. 328.

2. Стекольников Ю. И. Живучесть систем. СПб.: «Политехника», 2002. С. 152. URL: https://www.google.com/search?client=firefox-b (дата звернення: лютий 2023 р.).

3. Кочкаров А. А., Малинецкий Г. Г. Обеспечение стойкости сложных систем. Структурные аспекты. М., 2005. URL: https://www.google.com/search?client=firefox-b-d&q= (дата звернення: лютий 2023 р.).

4. Горшков В. В. Логико-вероятностный метод расчета живучести сложных систем // Кибернетика АН УОТ. 1982. № 1. С. 104–107.

5. Сафонов Р. А. Методика оценки живучести сложных систем военного назначения. 2003. С. 1. УДК 519.876.

6. Черкесов Г. Н. Методы и модели оценки живучести сложных систем. М.: Знание, 1987. 55 с.

7. Попков В. К. Математические модели живучести сетей связи. Новосибирск: СО АН СССР. 1990. 235 с.

8. Искольный Б. Б., Максимов Р. В., Шарифуллин С. Р. Оценка живучести распределенных информационно-телекоммуникационных сетей // Вопросы кибербезопасности. 2017. № 5 (24). URL: https://cyberleninka.ru/article/n/otsenka-zhivuchesti-raspredelennyh-informatsionno-telekommunikatsionnyh-setey (дата звернення: лютий 2023 р.).

9. ДСТУ В3265 – 95. Зв’язок військовий. Терміни та визначення. [Чинний від 1997–01–01]. К.: УкрНДІССІ, 1995. 23 с.

10. Військовий стандарт 01.112.001. Військова система стандартизації. Військовий зв’язок. Терміни та визначення. Міністерство оборони України, Київ, 2006. Реєстраційний номер А2187/000020.

11. Глушков В. М. Словарь по кибернетике. К.: Гл. ред. УСЭ, 1979. С. 87.

12. Горшков В. В. Логико-вероятностный метод расчета живучести сложных систем // Кибернетика АН УОТ. 1982. № 1. С. 104–107.

13. Словарь терминов и определений ITIL. Словарь терминов ITIL® на русском языке, версия 2.0, 29 июля 2011 г. на основе английской версии 1.0, 29 июля 2011. С. 114. Crown Copyright 2011].

14. International standard ISO 31000. Second edition 2018-02 Risk management - Guidelines.

15. ДСТУ ISO 31000:2018 Менеджмент рисков. Принципы и руководства (ISO 31000:2018, IDT).

16. Згуровский М. Г., Панкратова Н. Д. Системный анализ. Проблемы. Методология. Приложения. Киев: Наукова думка, 2005. С. 304.

17. Омельченко А. В. Теория графов. М.: МЦНМО, 2018. 416 с.

18. ГОСТ 27.310-95. Анализ видов, последствий и критичности отказов. Основные положения: [введен 1997-01-01]. М.: Издательство стандартов, 1996. 12 с. [Межгосударственный стандарт].

19. Харыбин А. В. Метод оценки живучести распределенных информационно-управляющих систем // Радіоелектронні і комп’ютерні системи. Харків: «ХАІ», 2007. № 8 (27). URL: http://nti.khai.edu:57772/csp/nauchportal/Arhiv/REKS/2007/REKS807/Titul.htm (дата звернення: лютий 2023 р.).

20. Надежность и эффективность в технике. Справочник: в 10 т. / Ред. совет: В. С. Авдуевский (пред.) и др. М.: Машиностроение, 1987. Т. 2: Математические методы в теории надежности и эффективности / Под ред. Б. В. Гнеденко. 280 с.

DOI: 10.58254/viti.3.2023.08.66

УДК.62-23

Поляк І. Є. ORCID: 0000-0002-5469-3215 (ВІТІ ім. Героїв Крут)
канд. техн. наук Борисов О. В. ORCID: 0000-0002-9460-2605 (ВІТІ ім. Героїв Крут)
канд. техн. наук Мацаєнко А. М. ORCID: 0000-0003-1149-7318 (ВІТІ ім. Героїв Крут)

МОДЕЛЮВАННЯ ПІДРЕСОРЕНОЇ ЧАСТИНИ МОБІЛЬНОГО ТРАНСПОРТНОГО ЗАСОБУ

Під час повномасштабного вторгнення країна агресор змінила тактику застосування мобільних вогневих засобів. Ці зміни призвели до створення високомобільних систем на базі колісного транспорту з нетиповим вогневим засобом. Як колісний транспортний засіб найчастіше використовують автомобіль типу «Пікап», оскільки в його конструктивних властивостях існує місце у кузові для встановлення додаткових систем з подальшим маскуванням обраного засобу. Такі колісні транспортні бази з нетиповим вогневим засобом вже використовуються в Збройних силах України, як на лінії зіткнення з ворогом, так і в цивільних містах для захисту повітряного простору залежно від характеристик нетипового вогневого засобу. Аналіз створення та використання згаданих систем виявив їхні певні недоліки та відповідні напрямки вдосконалення.

У роботі розглянуто питання формування коливального ефекту в підресореній частині колісного транспортного засобу при застосуванні поздовжнього збурення від використання вогневого засобу. В основу роботи покладено аналіз вимог до поздовжньої та поперечної стабілізації кузова колісного транспортного засобу. Для цього проведено аналіз характеристик існуючих видів та схем підвіски автомобіля типу «Пікап». Отримані результати використовуються для розрахунку коливального ефекту колісного транспортного засобу, який виникає внаслідок використання вогневого засобу.

Кінцевою метою роботи є створення моделі жорсткості системи «транспортний засіб – вогневий засіб» та використання цієї моделі для формування керуючого впливу системою автоматичного управління стабілізації вогневого засобу. Наявність системи автоматичного управління дозволить збільшити ефективності встановленого вогневого засобу.

Ключові слова: *пікап, підвіска, поперечний важіль, демпфер, амортизатор, тросіон, нетиповий вогневий засіб.*

I. Polyak, O. Borysov, A. Matsayenko Modeling of the springed part of a mobile vehicle.

During a full-scale invasion, the aggressor country changed the tactics of using mobile fire equipment. These changes led to the creation of highly mobile systems based on wheeled vehicles with an atypical firearm. As a wheeled vehicle, a "Pickup" type car is most often used, since its structural properties have room in the body for installing additional systems with subsequent masking of the selected vehicle. Such wheeled transport bases with an atypical firearm are already used in the Armed Forces of Ukraine both on the line of contact with the enemy and in civilian cities to protect the airspace, depending on the characteristics of the atypical firearm. Analysis of the creation and use of the mentioned systems revealed their certain shortcomings and the corresponding areas of improvement.

The article considers the issue of the formation of an oscillating effect in the spring-loaded part of a wheeled vehicle when longitudinal disturbance from the use of a firearm is applied. The work is based on the analysis of requirements for longitudinal and transverse stabilization of the body of a wheeled vehicle. For this, an analysis of the characteristics of the existing types and schemes of the suspension of the "Pickup" type car was carried out. The obtained results are used to calculate the oscillating effect of a wheeled vehicle that occurs as a result of the use of an incendiary agent.

The final goal of the work is to create a model of the rigidity of the "vehicle - firearm" system and to use this model to form a control effect of the automatic control system of the stabilization of the firearm. The presence of an automatic control system will increase the efficiency of the installed fire means.

Keywords: *pickup truck, suspension, transverse lever, damper, shock absorber, trosion, atypical firearm.*

Постановка завдання в загальному вигляді. Повномасштабне вторгнення Росії на територію України спричинило модернізацію та переоснащення військової техніки, що використовується, та отримання новітнього озброєння від країн-партнерів. Вторгнення розпочалось зі знищення авіаційної техніки ЗСУ та зумовило створення високомобільних систем вогневого ураження на базі ТЗ з різними системами вогневого ураження, в тому числі й авіаційними. Аналіз створених високомобільних систем виявив певні недоліки при використанні ЗСУ. Відсутність технологічного процесу створення згаданих систем призвів до виникнення негативного коливального ефекту під час використання вогневого засобу та зниження ефективності встановленого нетипового вогневого засобу.

Аналіз публікацій за темою дослідження. На сьогодні коливальний ефект кузова залишається актуальною проблемою для автомобільної індустрії. Цей ефект може виникати при русі автомобіля на нерівному дорожньому покритті або при створенні збурного діяння від встановленої вогневої системи. Під впливом коливального ефекту кузова автомобіль може рухатися непередбачувано, що може стати причиною аварій.

Визначенню коливальних здібностей надресорних мас автомобіля присвячена велика кількість робіт вчених країни [1; 3; 4]. За результатами аналізу доступних літературних джерел та публікацій проаналізовано методики розрахунку жорсткості підресорених мас на основних видах підвіски. Існуючі методи розрахунку коливання надресорних мас ТЗ не враховують знаходження автомобіля в статичному стані. Здійснено аналіз змін у конструкції сучасних автомобілів, випущених як в Україні, так і за кордоном [7; 8]. Проаналізовано зміну центру тяжіння залежно від ТТХ встановленого нетипового вогневого засобу [2; 6].

Усі ці статті демонструють актуальність проблеми коливального ефекту кузова і наголошують на необхідності пошуку рішень для зменшення впливу цього ефекту на рух автомобіля. Також вони підтверджують важливість досліджень для розробки нових технологій підвищення безпеки автомобілів і забезпечення комфортного використання встановлених вогневих систем.

Одним з можливих рішень для зменшення коливального ефекту кузова є використання активних систем підвіски, які можуть реагувати на зміни в дорожніх умовах і компенсувати коливання кузова, але вони не обраховані щодо збурного діяння від встановленої вогневої системи. Також можливими рішеннями є підбір оптимальних параметрів системи підвіски або використання спеціальних матеріалів для зменшення маси кузова.

Проблема коливального ефекту кузова залишається актуальною для дослідження і розробки нових технологій, які дозволять зменшити вплив цього ефекту на рух автомобіля. Для цього потрібні подальші дослідження і вивчення впливу різних факторів на коливальний ефект кузова, а також розробка нових методів і технологій для зменшення впливу цього ефекту на рух автомобіля.

Метою статті є розрахунок жорсткості підвіски високомобільної системи вогневого ураження на базі колісного транспортного засобу з врахуванням змінних показників основних видів підвіски. Дані розрахунки є елементом моделі жорсткості системи «транспортний засіб – вогневий засіб», що і буде напрямком подальших наукових досліджень.

Виклад основного матеріалу. Схема підвіски транспортного засобу обирається залежно від умов експлуатації цього засобу, його цільового призначення та навантаження (вантажопідйомність, типи доріг, інтенсивність використання транспортного засобу тощо). Основні види підвіски, які використовуються в автомобілях, можливо поділити на суто механічні системи та на комбіновані (електромеханічні, пневмомеханічні і т. ін.). Кожна з існуючих схем має свої переваги та недоліки. Відсутність уніфікованого варіанта обумовлена наявністю протиріччя між комфортом користувача та керованістю транспортного засобу. Отже, існує декілька основних видів підвіски:

листова підвіска. Складається з низки сталевих листів, які розташовані на рівні диференціала та з’єднують його з каркасом (рамою) ТЗ. Такий вид підвіски здатний витримувати велике навантаження;

незалежна підвіска. Має окремі пружини та амортизатори для кожного колеса та забезпечує більш точне керування й комфортний рух пікапа, але є менш міцною, ніж листова підвіска;

пневматична (гідропневматична електрична) підвіска. Використовує повітряні міхури (гідропневматичні або електричні приводи) замість сталевих листів та забезпечує більш гладкий та комфортний рух, дозволяє змінювати жорсткість та висоту центру ваги залежно від навантаження. Може бути налаштована на автоматичний режим регулювання жорсткості пружин у режимі реального часу. Є більш складною та дорожчою в обслуговуванні;

ригельна підвіска. Це спеціальний тип підвіски, який використовується в пікапах з великою вантажопідйомністю. Вона складається з ригелів, які з’єднують задню ось пікапа з рамою транспортного засобу. Ригельна підвіска забезпечує велику міцність та стійкість, але не забезпечує гладкого рухання.

Кожна з описаних схем має свій математичний опис для визначення основних характеристик та опису коливальних властивостей. Комбінація схем підвіски в конструкції одного транспортного засобу призводить до виникнення різних моделей реакції системи на зовнішній вплив.

На відміну від існуючих підходів, під зовнішнім впливом розуміємо вплив від використання за призначенням нетипового вогневого засобу. При цьому відомо:

вогневий засіб при встановленні змінює центр ваги ТЗ в вертикальній та горизонтальній площинах;

сила впливу залежить від технічних характеристик вогневого засобу та напрямку застосування зброї відносно вісі ТЗ;

вплив ВЗ збуджує коливальні процеси підресореної частини ТЗ та спричиняє зміну статичного стану ТЗ;

параметри коливального процесу залежать від конструкції підресореної частини та її характеристик, зокрема параметрів жорсткості.

Метою дослідження є побудова моделі жорсткості системи ТЗ + ВЗ у двох площинах.

Отже, при використанні нетипового вогневого засобу на транспортній базі (ТБ) під час пострілу виникає збурене діяння на підресорену частину ТБ. Тому після першого застосування точність вогневого засобу зменшується у зв’язку з виникненням коливання підресореної частини ТБ (пов’язаних з частотою власних коливань).

Для нівелювання негативного впливу сьогодні використовують два способи:

1) збільшення часу між пострілами з вогневого засобу;

2) використання домкратів для усунення коливання підресореної частини.

Обидва способи пов’язані з витратами часу, що протирічить тактиці застосування високомобільних вогневих засобів.

У роботі пропонується створення уніфікованої платформи стабілізації під керівництвом автоматичної системи. Керуючий вплив в системі САУ визначатиметься моделлю властивостей підресореної частини ТЗ.

Для розрахунку коливального ефекту потрібно визначити характеристики пружності підвіски, які залежать від вертикального навантаження на колесо F_z та деформацією пружних елементів [5] (рис. 1).

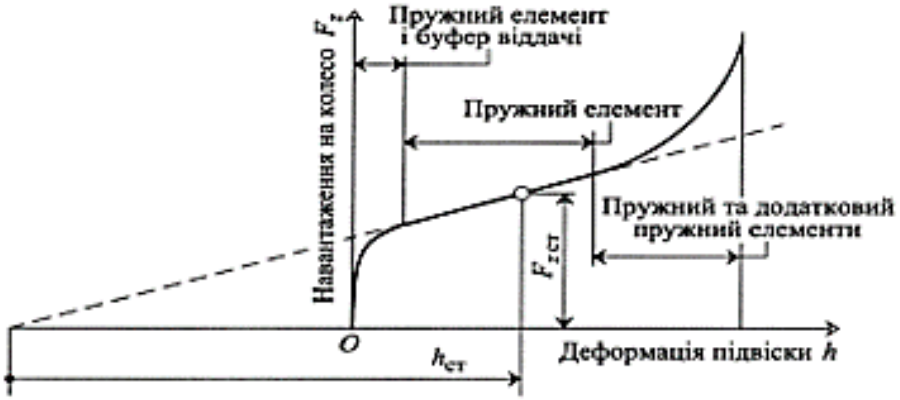


Рис. 1. Характеристика пружності підвіски:
F_z – статичне навантаження на колесо; $h_{\text{ст}}$– статична деформація підвіски

Сучасні підвіски мають буфери віддачі та додаткові пружні елементи, які підвищують жорсткість та обмежують хід стискання.

Частота власних коливань підресореної частини ТБ напряму залежить від статичної деформації підвіски після пострілу $h_{\text{ст}}$ (1):

$$\nu = \frac{1}{2\pi}\sqrt{\frac{g}{h_{cm}}}, \tag{1}$$

де g – прискорення.

Виходячи з рисунку 1, для розрахунку статичної деформації підвіски потрібно визначити її жорсткість.

Аналізу в системи підресорювання підлягають наступні елементи конструкції [1]:

– частина підвіски, яка виконує функцію передачі сил і моментів від коліс до підресореної частини. Ще однією функцією цієї частини є гасіння вібраційної дії на підресорену частину ТЗ у момент руху;

– безпружинні частини. Містять в собі агрегати та вузли, вага яких не передається пружинам;

– шини – елементи автомобіля, які забезпечують взаємодію коліс ТЗ з дорожньою поверхнею;

– до складу підресореної частини віднесено всі агрегати, вага яких передається пружинам.

Вплив нерівностей дорожнього покриття на підресорену частину здійснюється через підвіску ТЗ. Вона розділяється на три основні компоненти: пружний елемент (пружини), гаситель коливань (амортизатор) і направляючий пристрій.

Пружний елемент в підвісці призначений для зменшення впливу від нерівностей дороги через шини та безпружинні частини.

Розробляючи розрахункову модель, зробимо певні спрощення і припущення:

колісний транспортний засіб має симетрію відносно вертикальної осі. Використаємо плоску модель, в якій пружні зв’язки по бортах об’єднуються, а масу розподілимо на безпружинну і підресорену. Підресорена маса складається з агрегатів та вузлів, а непідресорна маса з ваги мостів;

пружні зв’язки між окремими агрегатами автомобіля відсутні. Підресорена маса розглядається як ціле жорстке тіло;

масою для розрахунку будемо вважати експлуатаційну масу ТЗ з додаванням маси вогневого засобу;

навантаження по бортах ТЗ розподілимо рівномірно;

пружні та демпфуючі елементи – безмасова модель, врахуванню підлягає лише піддатливість і коефіцієнт демпфірування;

коефіцієнти демпфірування вважаємо постійними та лінійними;

вважаємо, що ТЗ не рухається, а профіль поверхні синхронний під колесами обох бортів;

вважаємо, що контакт шини з опорною поверхнею точковий;

діє детерміноване збурення.

Розробка математичної моделі для підвіски ґрунтується на постановці диференціальних рівнянь, які описують процеси в підвісці ТЗ, зображеної на рисунках 2, 3.

Для створення математичної моделі коливань представленої системи скористаємося ключовим методом, який базується на рівнянні Лагранжа 2-го роду. Рівняння складаються для кожної маси, яка входить у розрахункову систему, і мають такий вид (2):

$$\frac{d}{dt}\left(\frac{\partial T}{\partial q_i}\right) - \frac{\partial K}{\partial q_i} + \frac{\partial П}{\partial q_i} + \frac{\partial Д}{\partial q_i} = \sum_{i=1}^{I} Q_i, \tag{2}$$

де q_i – узагальнена координата;

K – кінетична енергія;

$П$ – потенціальна енергія;

$Д$ – дисипативна функція Релея;

I – збурення;

Q_i – зовнішнє збурення.

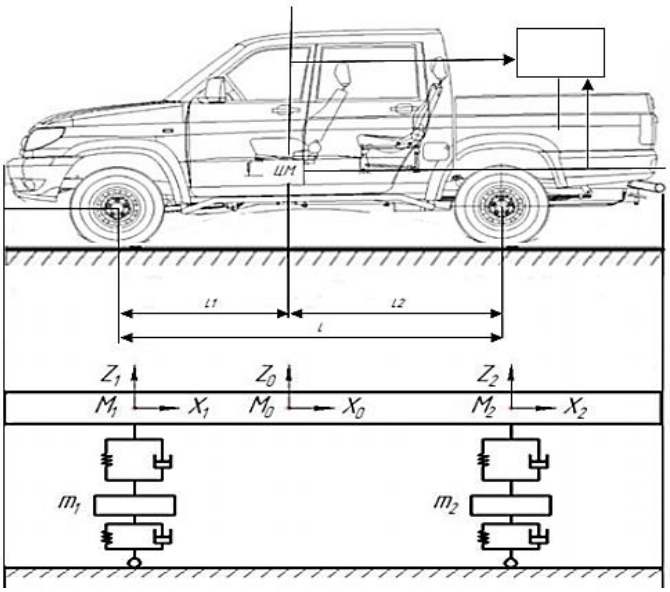


Рис. 2. Коливальна схема автомобіля у статичному стані

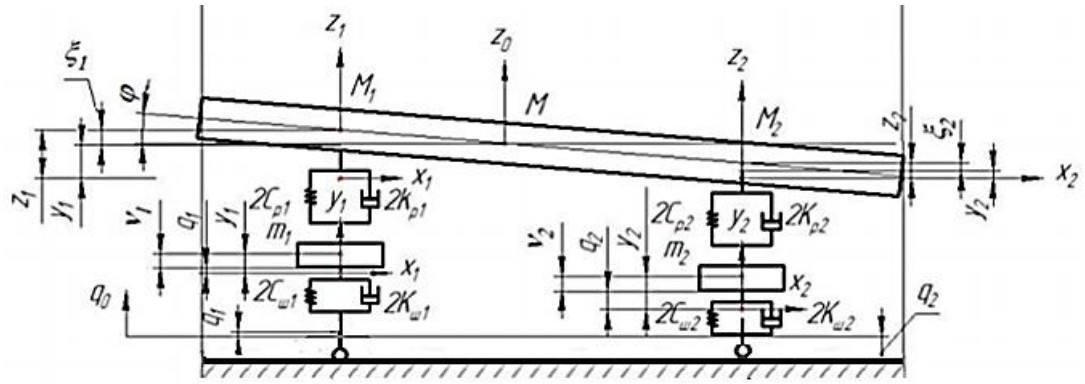


Рис. 3. Зміна кутового положення підресореної частини під дією зовнішнього впливу (поздовжне збурення)

Рівняння енергії матиме вид (3)–(5):

$$K = \frac{1}{2}\left(M_0 z_0^2 + M_0 p^2 \varphi^2 + m_1 y_1^2 + m_2 y_2^2\right); \tag{3}$$

$$П = \frac{1}{2}\left(2C_{p1}\zeta_1^2 + 2C_{p2}\zeta_2^2 + 2C_{ш1}v_1^2 + 2C_{ш2}v_2^2\right); \tag{4}$$

$$Д = \frac{1}{2}\left(2K_{a1}\zeta_1^2 + 2K_{a2}\zeta_2^2 + 2K_{ш1}v_1^2 + 2K_{ш2}v_2^2\right), \tag{5}$$

де M_0 – повна вага авто та вогневого засобу;

z_0 – переміщення центру мас остову;

$\frac{M_0 p^2}{2}$ – момент інерції;

φ – кут нахилу остову;

m_1 та m_2 – маса переднього та заднього мостів;

y_1 та y_2 – переміщення переднього та заднього мостів;

C_{p1} та C_{p2} – жорсткість передньої та задньої підвіски;

ζ_1 та ζ_2 – деформація передньої та задньої підвіски;

$C_{ш1}$ та $C_{ш2}$ – жорсткість шин переднього та заднього мостів;

ν_1 та ν_2 – деформація шин переднього та заднього мостів;

K_{a1} та K_{a2} – коефіцієнт демпфірування амортизаторів;

$K_{ш1}$ та $K_{ш2}$ – коефіцієнт демпфірування шин.

Розглянемо моделі визначення жорсткості для різних схем будови підвіски ТЗ (рис. 4–7).

Для розрахунку жорсткості листової ресори використовують формулу (6):

$$G_в = k_1 k_2 G\,, \tag{6}$$

де k_1 – коефіцієнт, що залежить від конструкції кріплення ресори до осі автомобіля;

k_2 – коефіцієнт, що залежить від конструкції кріплення ресори до рами або кузова автомобіля;

G – жорсткість листової ресори без кріплення.

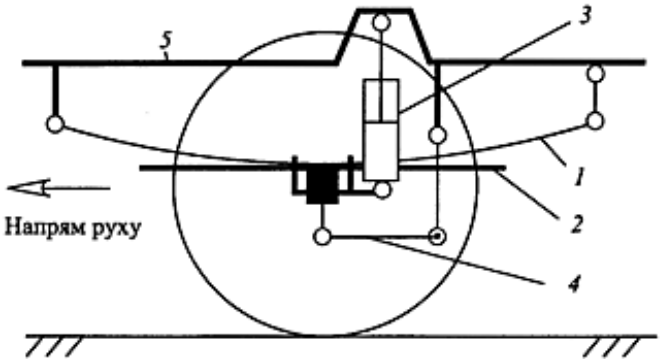


Рис. 4. Схема задньої підвіски легкої вантажівки з однолистовою ресорою:
1 – однолистова ресора; *2* – опорний лист; *3* – амортизатор; *4* – стабілізатор; *5* – рама

Для розрахунку жорсткості важільної торсіонної підвіски, встановленої на ТБ, використаємо формулу (7):

$$G_в = M\frac{d^2\theta}{ds^2} + G\left(\frac{d\theta}{ds}\right)^2, \tag{7}$$

де θ – кут закручення торсіона;

s – переміщення колеса;

M – скручувальний момент;

d – діаметр торсіонну;

G – жорсткість торсіонна без кріплення.

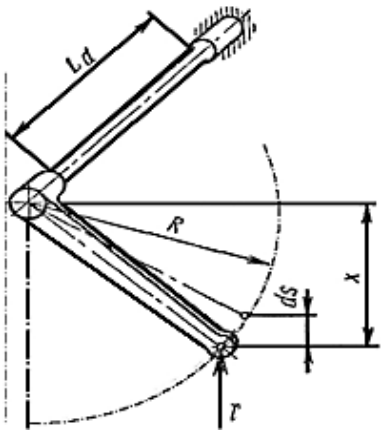


Рис. 5. Схема одноважільної торсіонної підвіски

Для розрахунку жорсткості важільної підвіски зі спіральною пружиною, встановленої на ТБ, використаємо формулу (8):

$$G_в = \frac{4MI_p}{\pi D^3 z_n}, \tag{8}$$

де I_p – полярний момент інерції перерізу дроту пружини;

z_n – число робочих витків пружини;

M – модуль пружності другого роду;

D – середній діаметр пружини.

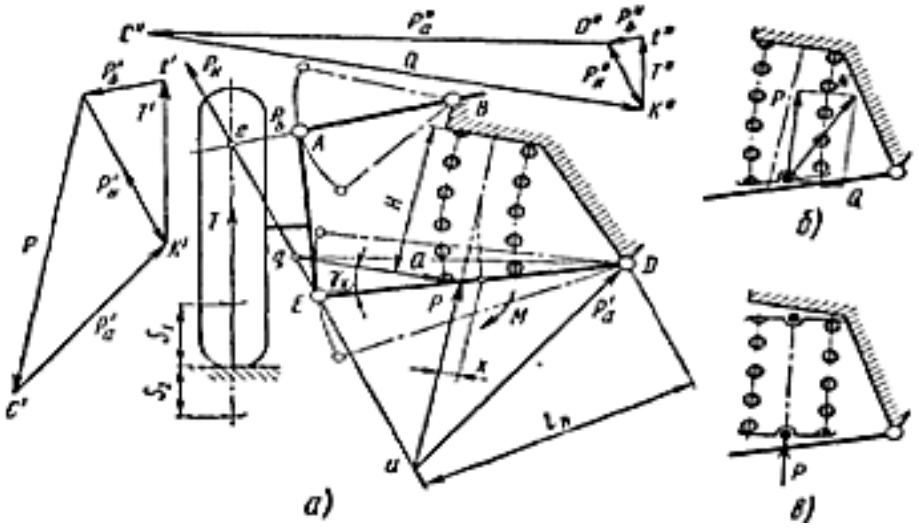


Рис. 6. Схема трапецієподібної підвіски зі спіральною пружиною, опертою на нижній вал:
а – безшарнірне кріплення пружини; *б* – одношарнірне кріплення пружини;
в – двошарнірне кріплення пружини

Для розрахунку жорсткості пневматичної підвіски, встановленої на ТБ, використаємо формулу (9):

$$G_в = \frac{nP_g}{V_g} 4F_б^2 + \left(P_g - P_a\right)\frac{dF_б}{dS}, \tag{9}$$

де n – показник політропи;

P_g – абсолютний тиск газу;

V_g – обсяг газу;

$F_б$ – ефективна площа балона;

P_a – атмосферний тиск;

S – ефективна площа сильфона;

d – діаметр пневмоподушки.

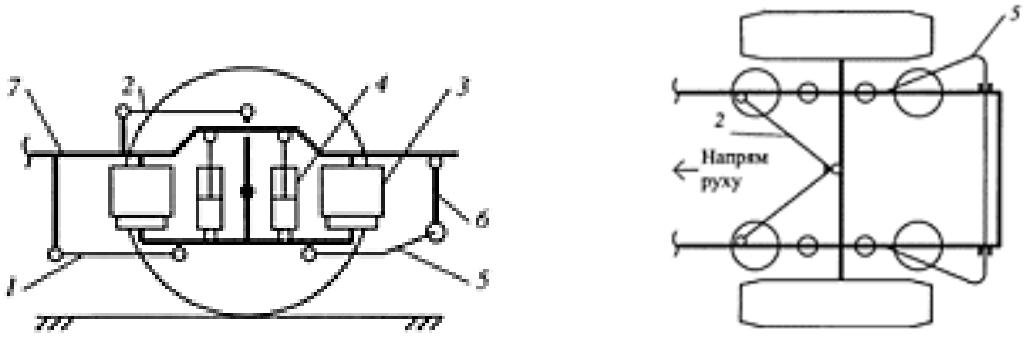


Рис. 7. Схема передньої пневматичної підвіски:
1, 2, 3 – штанги; *4* – тяга Папара; *5* – амортизатор;
6 – рукавний пневмобалон; *7* – стабілізатор; *8* – рама

Висновки. Наявність окремих математичних моделей різних схем підвіски ТЗ дозволяє визначити жорсткість окремої конструкції. Модель всієї системи підресореної частини потрібно визначати з урахуванням відмінностей будови переднього та заднього мостів ТЗ. На відміну від існуючих моделей, в яких досліджується поздовжня та поперечна стійкість (стабілізація) ТЗ, у роботі передбачається створення моделі коливальних властивостей системи в азимутальній та кутомісній площинах, оскільки реакція системи на зовнішній вплив від застосування вогневого засобу різниться залежно від цих кутів. У цілому, наявність двомірної моделі дозволятиме створити ефективну САУ стабілізації вогневого засобу на колісній транспортній базі.

Подальші дослідження створення моделі коливальних властивостей системи транспортного засобу дозволять вивчати характеристики коливань кузова залежно від різних параметрів, таких як вага автомобіля, жорсткість і демпфірування підвіски, рівень навантаження на колеса, тип вогневої системи та ін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шупляков В. С. Колебания и нагруженность трансмиссии автомобиля. М.: Транспорт, 1974. 328 с

2. Кузавков В. В., Поляк І. Є. Аналіз транспортної бази для встановлення стабілізованої платформи нетипової артилерійської системи // Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 50. С. 16–18.

3. S. Kurnikov. Формування ринкової структури автомобільного парку України // Politechnika Rzeszowska. 2017. № 11. P. 35–39.

4. Вертикальні коливання підресореної частини колісних транспортних засобів під дією випадкових збурень / М. Г. Грубель, О. П. Красюк, М. Б. Сокіл, Р. А. Нанівський // Наукові нотатки: Зб. Наук. Пр. Луцьк, 2014. Вип. 46. С. 112–116.

5. Чудаков Е. А. Теория автомобиля. М.: Машгиз, 1950. С. 340–345.

6. Поляк І. Є. Варіант будови системи стабілізації уніфікованої платформи транспортного засобу // Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник доповідей та тез доповідей ІІ Міжнародної науково-технічної конференції, м. Київ, 1 грудня 2022 року. Київ: ВІТІ, 2022. С. 172–174.

7. Современные адаптивные подвески // Автократ. URL: http://avtocrat.at.ua.

8. Сокіл Б. І. Власні вертикальні коливання корпусу автомобіля з урахуванням нелінійних характеристик пружної підвіски / Б. І. Сокіл, Р. А. Нанівський, М. Г. Грубель // Автомобільний транспорт. 2013. № 5 (235). С. 15–18.

DOI: 10.58254/viti.3.2023.09.74

УДК. 621.391

канд. техн. наук Радзівілов Г. Д. ORCID: 0009-0002-6047-1897 (ВІТІ ім. Героїв Крут)
канд. техн. наук Ільїнов М. Д. ORCID: 0009-0008-6945-3354 (ВІТІ ім. Героїв Крут)
Хоменко П. В. ORCID: 0000-0002-8543-1971 (ВІТІ ім. Героїв Крут)

МЕТОД РОЗРАХУНКУ ПАРАМЕТРІВ КОНСТРУКЦІЇ КОЛІНЕАРНОЇ АНТЕНИ ПОСЛІДОВНОГО ТИПУ З ВИКОРИСТАННЯМ ДИСПЕРСІЙНИХ ХАРАКТЕРИСТИК УПОВІЛЬНЮЮЧОЇ СИСТЕМИ

У роботі представлена методика аналізу електричних характеристик колінеарних антен послідовного типу, виконаних за схемою Франкліна, які призначені для використання їх в системах радіозв'язку з рухомими об'єктами в якості базових, або абонентських антенно-фідерних пристроїв.

Колінеарні антени відносяться до антен всенаправленого типу і дозволяють суттєво збільшити коефіцієнт підсилення порівняно із вже існуючими антенами подібного типу, чим і приваблюють на сьогодні розробників антенної техніки.

Рішення електродинамічної задачі про розповсюдження радіохвиль у сповільнюючій системі у вигляді спірального провідника знайшли відображення в багатьох наукових працях, як у строгій постановці задачі (із врахуванням явища дисперсії), так і у наближеній. Однак, громіздкий математичний апарат не зовсім прийнятний в інженерній практиці при розробці колінеарних антен послідовного типу. У роботі запропонована проста інженерна методика розрахунку параметрів індуктивного дроселя як фазозсувного приладу в колінеарній антені, заснована на строгій теорії для сповільнюючих систем, яка дозволяє достатньо легко розрахувати величину фазового зсуву в випромінюючих елементах антени.

Отримані результати моделювання електричних характеристик підтверджують ефективність запропонованої методики. Виявлено значний приріст коефіцієнта підсилення порівняно з існуючими типами антен та відповідність електричних характеристик заданим параметрам. Робота має важливий внесок у розвиток антенної техніки і практичне застосування в системах радіозв'язку з рухомими об'єктами. Запропонована методика розрахунку параметрів індуктивного дроселя може бути використана розробниками антен для підвищення продуктивності та ефективності їхньої системи радіозв'язку.

Ключові слова: *радіолінія, колінеарна антена, антенна решітка, індуктивний дросель, сповільнююча система, фазозсувний пристрій, випромінюючий елемент.*

H. Radzivilov, M. Ilyinov, P. Khomenko The method of calculating the design parameters of a collinear serial antenna using the dispersion characteristics of the retarding system.

The paper presents a technique for analyzing the electrical characteristics of series-type collinear antennas made according to the Franklin scheme, which are intended for use in radio communication systems with moving objects as basic or subscriber antenna-feeder devices. Collinear antennas belong to omnidirectional type antennas and allow to significantly increase the amplification factor in comparison with already existing types of antennas of a similar type, which is what attracts antenna technology developers today.

The main element of a series-type collinear antenna is a phase-shifting device that determines both the performance of the antenna and its electrical characteristics. The most widely used phase-shifting devices were inductive chokes – a section of conductor of a certain length rolled into a spiral.

The proposed engineering method of calculating the parameters of the inductive choke allows you to quickly and accurately adjust its characteristics with the calculation of the necessary phase shift. This approach takes into account the physical parameters of the conductor material and the geometry of the spiral conductor, which greatly simplifies the engineering process of developing collinear antennas. The obtained results of simulation of electrical characteristics confirm the effectiveness of the proposed method.

A significant increase in the amplification factor compared to the existing types of antennas and compliance of the electrical characteristics with the specified parameters was revealed. The work has an important contribution to the development of antenna technology and has practical application in radio communication systems with moving objects. The proposed method of calculating the parameters of the inductive choke can be used by antenna developers to increase the productivity and efficiency of their radio communication system.

Keywords: *radio line, collinear antenna, antenna array, inductive choke, deceleration system, phase-shift device, radiation device.*

Постановка завдання. Одним із важливих елементів функціонування радіоліній систем зв’язку з рухомими об’єктами є антенно-фідерний пристрій, який забезпечує не тільки енергетичний потенціал радіолінії в будь-якому напрямку, але і визначає організаційно-технічну будову всієї системи радіозв’язку, надійність її роботи, розвідзахищеність, електромагнітну сумісність з іншими радіотехнічними пристроями. Тому питання, пов’язані з розробкою нових технічних рішень з компонування антенно-фідерних пристроїв, модернізації існуючих зразків, зменшення матеріальних затрат на їх виготовлення, актуальні і мають практичне значення на цей час при розборці нової техніки для телекомунікаційних систем.

На сьогодні у вказаних системах широко використовуються колінеарні антени. Одним з проблемних питань при розрахунку колінеарних антен є розрахунок індуктивностей, які виконують роль фазозсувного елементу (далі – ФЕ). Зазвичай такий розрахунок проводиться з використанням відомого трансцендентного рівняння. Але цей метод розрахунку є достатньо складним і дозволяє розрахувати ФЕ зі значними похибками. Тому виникає необхідність розрахунку параметрів ФЕ за допомогою дисперсійних характеристик уповільнюючої системи, що дозволить значно зменшити обчислювальне навантаження.

Науковим завданням статті є обґрунтування спрощеного методу розрахунку параметрів ФЕ, необхідних для покращення характеристик антенно-фідерних пристроїв та їх ефективного функціонування в системах зв’язку з рухомими об’єктами.

Аналіз останніх публікацій

У роботі [1] розглянуті шляхи підвищення ефективності функціонування систем радіозв’язку завдяки використанню адаптивних антенних решіток, що є основою подальших розробок та пошуків шляхів покращення характеристик радіоліній систем зв’язку з рухомими об’єктами.

Методика формування діаграми спрямованості кільцевої антенної решітки радіостанції мобільної радіомережі в умовах навмисних завад [2] дозволяє продовжити шлях проєктування нових різновидів антенних решіток в різноманітних умовах, але потребує подальшої розробки методів їх ефективного застосування.

В роботах [3; 4] досліджено шляхи підвищення завадозахищеності мобільних радіомереж з використанням технології адаптивного діаграмоутворення та управління засобами завадозахисту військових систем радіозв’язку, що дозволить авторам шукати можливості підвищення ефективності застосування антен.

Робота [9] обґрунтовує ідею щодо уповільнюючих систем, що дає можливість для розробки нових методів проєктування антен.

Однак ці роботи не враховують завдання щодо оптимізації розрахунку параметрів конструкції колінеарної антени послідовного типу з використанням дисперсійних характеристик уповільнюючої системи.

Метою даної роботи є представлення методу розрахунку конструкції колінеарної антени послідовного типу, виконаної за схемою Франкліна, з використанням дисперсійних характеристик уповільнюючої системи.

Виклад основного матеріалу.

Колінеарна антена послідовного типу являє собою лінійну синфазну антенну решітку, виконану з симетричних вібраторів різної довжини і конструкції. Основним елементом таких антен є ФЕ, який розташований між випромінюючими елементами колінеарної антени і призначений для їхнього синфазного живлення. Фактично ФЕ визначає як зовнішні, так і внутрішні характеристики антени в цілому та її працездатність.

У самому найпростішому варіанті ФЕ виконується у вигляді коротко замкнутого чверть-хвильового відрізка двопроводової лінії, як показано на рисунку 1.

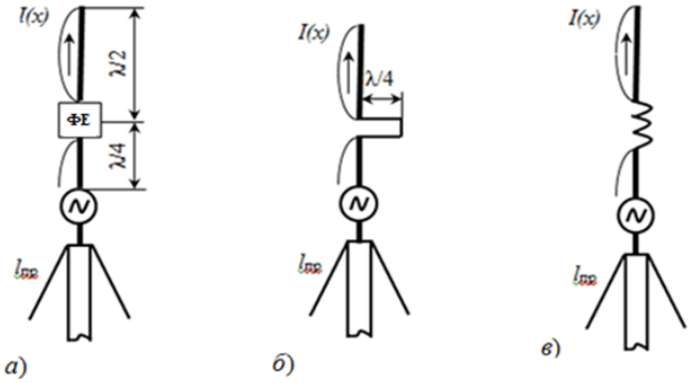


Рис. 1. Колінеарні антени послідовного типу:
а – загальна схема; *б, в* – реалізація ФЕ

Повна довжина короткозамкненого відрізка складає λ/2, де λ – довжина хвилі. Відповідно, фаза струму змінюється на 180°, що забезпечує синфазне збудження другого елемента колінеарної антени. Перевага такого ФЕ – простота конструкції і простота її реалізації. Недолік – збільшення габаритних характеристик, що обмежує застосування таких антен на мобільних об’єктах. Цей недолік можливо деякою мірою усунути, якщо короткозамкнений відрізок двопровідної лінії звернути або розмістити вздовж випромінюючих елементів. На практиці найбільш широке застосування отримали ФЕ, виконані у вигляді індуктивного дроселя (котушки індуктивності). Така реалізація ФЕ в колінеарних антенах послідовного типу забезпечує зменшення її масогабаритних характеристик антен, підвищує її механічну міцність, що особливо важливо при використанні таких антен на мобільних об’єктах. Варіант колінеарної антени з ФЕ у вигляді індуктивного дроселя представлений на рисунку 1, *в*.

Для вивчення принципу роботи ФЕ, виконаного у вигляді індуктивного дроселя, доцільно його уявити як спіральний хвилевід радіусом *a*, кутом намотування ψ і кроком спіралі *s*, як показано на рисунку 2.

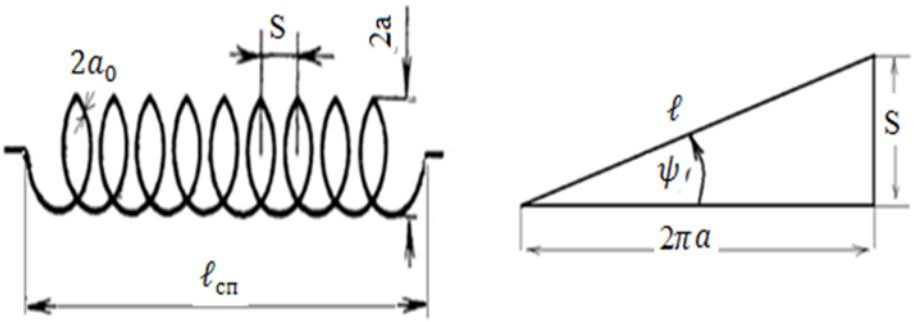


Рис. 2. Фазозсувний пристрій у вигляді індуктивного дроселя:
2a – діаметр спіралі; S – крок спіралі; ψ – кут намотування; $2a_0$ – діаметр дроту; $l_{сп}$ – довжина спіралі

Якщо припустити, що електромагнітна хвиля розповсюджується вздовж гвинтової лінії з фазовою швидкістю, то маємо вираз (1):

$$V_{ф} = C\,, \tag{1}$$

де $C = 3 \times 10^{8}\ {}^{м}/_{с}$ – швидкість світла вздовж одного витка.

Хвиля розповсюджується за час Δt, вираз (2):

$$\Delta t = \frac{2\pi a}{c}\,. \tag{2}$$

За цей час хвиля зміщується вздовж осі Z на відстань S – крок спіралі. Позначивши швидкість розповсюдження хвилі вздовж спіралі як $V_{\text{ф}}$, отримаємо вираз (3):

$$\Delta t = \frac{S}{V_{\text{ф}}}. \tag{3}$$

Отже, коефіцієнт сповільнення $\text{К}_{\text{с0}}$ буде дорівнювати (4):

$$\text{К}_{\text{с0}} = \frac{\text{С}}{V\text{ф}} = \frac{\sqrt{(2\pi\text{a})^2 - S^2}}{S} = \frac{2\pi a}{S} = \frac{1}{sin\psi}, \tag{4}$$

за умови, що $S<<2\pi a$.

Із вище вказаного доцільно рекомендувати алгоритм розрахунку параметрів індуктивного дроселя у наступній послідовності.

Вихідними даними виступають: f – робоча частота; вимоги до геометричних розмірів індуктивного дроселя (2a – діаметр спіралі; $l_{\text{сп}}$ – довжина котушки).

Спочатку визначаємось з Λ – довжиною хвиль у спіральному хвилеводі, вираз (5):

$$\Lambda = \frac{\lambda_0}{\text{К}_{\text{со}}}, \tag{5}$$

де λ_0 – довжина хвилі в вільному просторі; $\text{К}_{\text{со}} = {2\pi\text{a}}/{S}$ – коефіцієнт сповільнення.

Для забезпечення зсуву фази хвилі в 180° довжина спіралі $l_{\text{сп}}$ повинна дорівнювати (6):

$$l_{\text{сп}} = \frac{\Lambda}{2} = \frac{\lambda_0}{2\pi\text{a}} \cdot S. \tag{6}$$

Кут натягу ψ і довжина проводу вираховується співвідношенням, вираз (7):

$$\text{tg}\,\psi = \frac{S}{2\pi\text{a}};\ l_{\text{пр}} = 2\pi\text{a} \cdot N, \tag{7}$$

де N – кількість витків спіралі.

Представлена методика розрахунку параметрів ФЕ у вигляді індуктивного дроселя називається методикою нульового наближення, оскільки $\text{К}_{\text{с0}}$ – коефіцієнт сповільнення, незалежний від частоти і електромагнітних хвиль, який не володіє дисперсійними властивостями, що не відповідає дійсності.

Більш вимоглива теорія аналізу спіральних хвилеводів показує, що нульовим наближенням можна користуватись (8), коли:

$$ka\,\text{ctg}\,\psi \geq 3, \tag{8}$$

де $ka = {2\pi}/{\lambda_0}$ – хвильове число.

На сьогодні відомо декілька строгих методів аналізу електромагнітного поля в сповільнених системах, виконаних у вигляді спіральних хвилеводів.

Перший з них це представлення спіральної структури у вигляді нескінченого тонкого циліндра радіусом a, що володіє ідеальною провідністю, тільки в напряму витків спіралі.

У більш точному, але і більш складному методі, де враховується дискретність витків, розглядаються нескінчена тонка стрічкова спіраль з ідеальною провідністю.

Незалежно від використаного методу, кінцевий результат аналізу електромагнітного поля в сповільнених спіральних структурах з урахуванням дисперсії хвиль призводить до трансцендентного дисперсійного рівняння, яке має вид (9):

$$(ka\ \text{ctg}\,\psi)^2 = (\gamma a)^2\,\frac{I_0(\gamma a)K_0(\gamma a)}{I_1(\gamma a)K_1(\gamma a)}, \tag{9}$$

де $I_0(\gamma a)$, $I_1(\gamma a)$ – модифіковані функції Беселя;

$K_0(\gamma a), K_1(\gamma a)$ – функції Макдональда;

$\gamma^2 = \beta^2 - K^2$ – стала розповсюдження;

β – повздовжнє хвильове число.

При великих значеннях параметра γa для модифікованих функцій Беселя можна використовувати лише перші члени асимптотичних розкладань (10), (11):

$$I_m(x) = \frac{1}{\sqrt{2\pi x}} l^x, \tag{10}$$

$$K_m(x) = \sqrt{\frac{\pi}{2x}} l^{-x}. \tag{11}$$

Тоді, дисперсійне рівняння (9) має прийнятий вигляд (12):

$$(ka \operatorname{ctg} \psi)^2 = (\gamma \mathrm{a})^2. \tag{12}$$

Підставивши значення $(\gamma \mathrm{a})^2$ з формули (11) в формулу (13)

$$(\beta \mathrm{a})^2 = (\gamma \mathrm{a})^2 + (R\mathrm{a})^2, \tag{13}$$

отримаємо вираз (14) для K_{c0} – коефіцієнту сповільнення:

$$\mathrm{K}_{\mathrm{c0}} = \frac{\beta \mathrm{a}}{Ra} = \frac{C}{V_{\phi}} = \sqrt{1 + \cot \psi} = \frac{1}{\sin \psi}. \tag{14}$$

Це співвідношення справедливе при

$$ka \ \operatorname{ctg} \psi \geq 3 \tag{15}$$

та дає похибки обчислення K_{c0} приблизно 5÷10 %.

Ця методика щодо методики нульового наближення не враховує дисперсійних властивостей хвиль та передбачає, що хвиля розповсюджується виткам спіралі зі швидкістю світла.

Якщо в асимптотичних формулах розкладання недиференційних функцій Беселя обмежуються двома членами рядка, то дисперсійне рівняння приймає вигляд (16):

$$(R_a \operatorname{ctg} \psi)^2 = (\gamma \mathrm{a})^2 \left[1 + \frac{1}{2(\gamma \mathrm{a})^2}\right]. \tag{16}$$

Тоді K_{c1} – коефіцієнт сповільнення в першому наближенні буде визначатись наступним виразом (17):

$$\mathrm{K}_{c1} = \frac{\beta_a}{R_a} = \frac{1}{\sin \psi} \sqrt{1 + \frac{sin^2 \psi}{2(K_u)^2}}. \tag{17}$$

Цією формулою можна користуватись вже до значень (18):

$$\gamma_{\mathrm{a}} \geq 0{,}5 \text{ або } R_a \ \operatorname{ctg} \psi \geq 0{,}5. \tag{18}$$

У цьому випадку похибка розрахунку складає 5 %, що цілком допустимо для інженерної практики.

На рисунку 3 представлені графіки залежності коефіцієнта сповільнення K_{c} від конструктивних розмірів індуктивного дроселя, що виконує роль фазозсувного пристрою з колінеарною антеною послідовного типу. Результати розрахунку наглядно демонструють дисперсійну область роботи індуктивного дроселя, де недоцільно приймати формули нульового і першого приближення для розрахунку коефіцієнта сповільнення.

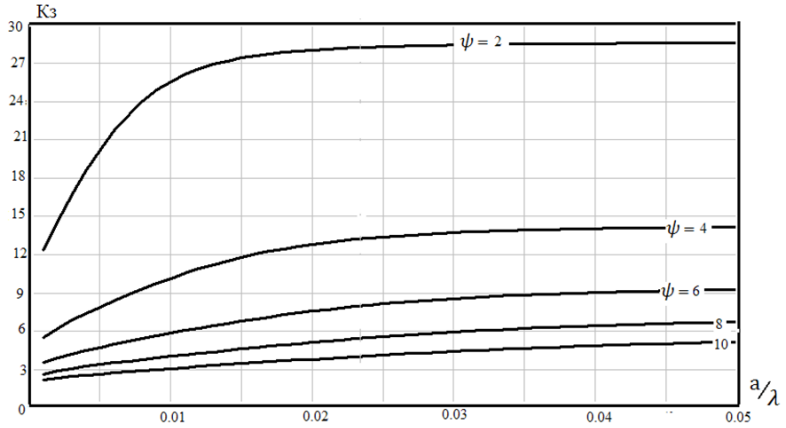


Рис. 3. Залежність коефіцієнта сповільнення K_{c}) від конструктивних розмірів індуктивного дроселя

В якості демонстрації викладених методик з розрахунку котушки індуктивності як основного елемента колінеарної антени проведемо розрахунок її основних електричних параметрів і зробимо висновок про межу використання.

За вихідні дані маємо: f = 915 МГц – робоча частота (λ = 32,78 – довжина хвилі); $2a_0$ = 1 мм – діаметр провідника.

Нехай діаметр котушки 2a = 8 мм; $^{a}/_{\lambda}$= 0,012, а кут обмотки $\psi = 4{,}6°$. У цьому випадку теорія нульового наближення за розрахунком $К_с$ дає наступні результати: $К_{с0} = 12{,}6$; $N_0 = 6{,}5$; $L_{про} = 164$мм.

Теорія першого наближення: $К_{с1} = 8{,}6$; $N_1 = 9{,}5$; $L_{прі} = 240$мм.

Строга теорія: $К_с = 9$; $N = 9{,}1$; $L_{пр} = 230$мм.

При збільшенні розмірів індуктивної котушки в 2,5 рази:

$2a = 18$мм; $^{a}/_{\lambda} = 0{,}03$; $\psi = 2°$; $К_a \cot\psi = 4{,}5$.

Отримуємо:

$$К_{с0} = 28;\ N_0 = 3;\ L_{пр} = 164;$$
$$К_{с1} = 28;\ N_1 = 3;\ L_{пр} = 166;$$
$$К_с = 28;\ N = 3;\ L_{пр} = 164.$$

Отримані результати дозволяють зробити важливий практичний висновок: за умови $ka\ \mathrm{ct}g\,\psi > 3$ (відсутність дисперсії в котушці індуктивності), довжина дроту $L_{прд}$ вибирається рівною $^{\lambda}/_{2}$, для конкретного кута нахилу спіралі ψ. На рисунку 4 показано межі використання методики нульового наближення з розрахунків коефіцієнта сповільнення в фазозсувному пристрої, який виконано в вигляді індуктивної котушки.

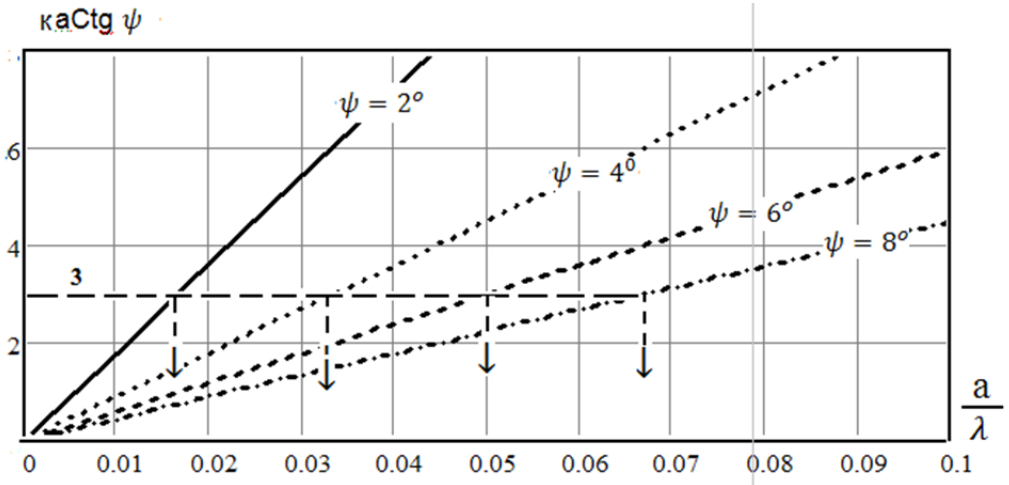


Рис. 4. Графік вибору методики до розрахунку $К_с$ – коефіцієнта сповільнення

Висновки. Таким чином, запропонований алгоритм розрахунку коефіцієнта сповільнення в індуктивній котушці, яка виконує функцію фазозсувного пристрою, дозволяє достатньо просто спроєктувати і розрахувати параметри колінеарної антени послідовного типу, виконаної в симетричних або несиметричних варіантах.

Потенційні області застосування цих досліджень містять розробку та оптимізацію базових і абонентських антенно-фідерних пристроїв у системах мобільного зв’язку, де більшість факторів є низьким рівнем завантаження сигналу та високою якістю зв’язку. Дослідження можуть знайти застосування в секторах транспорту, військовій техніці та інших галузях, де потрібна ефективна комунікація з рухомими об’єктами. Загальні результати цієї роботи вказують на важливість і перспективи використання колінеарних антен системного типу в системах радіозв’язку.

Отримані наукові результати мають практичне значення для інженерів та розробників, які використовують проєктування та оптимізацію бездротових комунікаційних систем.

Напрямком подальших досліджень є розрахунок більш складних конфігурацій колінеарних антен та дослідження їх взаємодії з іншими компонентами системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Борисов І. В., Гурський Т. Г., Ільїнов М. Д., Гриценок К. М. Підвищення ефективності функціонування систем радіозв’язку за рахунок використання адаптивних антенних решіток // Збірник наукових праць ВІТІ. 2015. № 1. С. 16–24.

2. Гриценюк К. М., Гурський Т. Г. Методика формування діаграми спрямованості кільцевої антенної решітки радіостанції мобільної радіомережі в умовах навмисних завад // Збірник наукових праць ВІТІ. 2018. № 3. С. 6–16.

3. Боголій С. М., Гурський Т. Г., Макарчук В. І., Хижий О. І. Підвищення завадозахищеності мобільних радіомереж з використанням технології адаптивного діаграмоутворення // Збірник наукових праць ВІТІ. 2022. № 2 (2). С. 5–14.

4. Кувшинов О. В. Адаптивне управління засобами завадозахисту військових систем радіозв’язку // Збірник наукових праць ВІКНУ. 2009. Вип. 17. С. 125–130.

5. Davies D.E.N., Rizk M.S.A.S. A broadband experimental null-steering antenna system for mobile communications. Proc/ IERE? 1978, Vol. 48, № 10.

6. Davies D.E.N., Rizk M.S.A.S. A small radius circular array antenna with 3600 null-steering capability/ - Int/ Conf/ Antennas and Propag., London, 1978, p. 60–64.

7. Rahim T., Guy J.R.F., Davies D.E.N. A wideband UHF circular array. Proceeding of IEE Antennas and Propagation Conference, York, 1981, 13–16 April.

8. Ломан В. И., Нестеренко И. К. Поляризационный компенсатор помех // Известия вузов. Радиоэлектроника. Том 28. № 3. 1985. С. 59–61.

9. Силин Р. А., Сазонов В. П. Замедляющие системы // Советское радио. 1968. С. 248–301.

10. Лебедев И. В. Техника и приборы СВЧ // Высшая школа. Том 1 «Техника сверхвысоких частот». 1970. С. 196–224.

DOI: 10.58254/viti.3.2023.10.81

УДК 355. 424

Радченко М. М. ORCID: 0000-0002-8272-0727 (ВІТІ ім. Героїв Крут)
Шаповал В. М. ORCID: 0000-0003-4637-9362 (ВІТІ ім. Героїв Крут)
Терещенко Т. П. ORCID: 0000-0002-9659-7897 (ВІТІ ім. Героїв Крут)
Дикий О. В ORCID: 0000-0001-7327-8589 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ РОЗРАХУНКУ КІЛЬКІСНИХ ПОКАЗНИКІВ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАХИСТУ КРИТИЧНОГО ОБ'ЄКТА ІНФРАСТРУКТУРИ ВІД УДАРІВ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

Зростання потенційних можливостей застосування безпілотних комплексів, які призначені виконувати бойові завдання в повітрі, на землі, на/під водою, ніж будь-коли раніше веде до збільшення загроз для оборонного ландшафту учасників сил оборони. Це стає причиною зростання швидкими темпами інтересу до технологій, які знешкоджують загрози подібного типу. Для сторони, яка захищає критичний об'єкт від повітряного нападу з боку безпілотного авіаційного комплексу (або групи) завжди актуальне питання гарантованої ефективності або економічної співмірності способів захисту від низько-вартісних атак, які можуть здійснюватися такими комплексами.

Процес функціонування критичного об'єкта інфраструктури, який містить у своєму складі розгорнуту систему захисту, пункт керування та підсистеми з критичним обладнанням, через які здійснюється загальне цільове призначення цього об'єкта, пропонується описувати за аналогією з моделлю процесу функціонування відновлюваної системи з обмеженою надійністю елементів. Для кількісної оцінки пропонується взяти комплексний показник надійності функціонування відновлюваної системи.

Отримані показники для кількісної оцінки ефективності захищеності критичного об'єкта інфраструктури від повітряних атак в подальшому будуть конвертуватися в конкретні пропозиції для осіб, які приймають рішення щодо підбору засобів необхідних видів протидії безпілотним авіаційним комплексам для нарощування системи захисту, і які вимагаються для обґрунтування фінансово-економічних затрат при здоланні такого типу загроз.

Напрямками подальших досліджень з метою забезпечення заданих показників захисту критичного об'єкта інфраструктури стане методика розрахунку резервування засобів захисту.

Ключові слова: *інтенсивність атак, кількісні показники ефективності, час відновлення, час нормального функціонування, критичний об'єкт інфраструктури, система захисту від БпАК.*

M. Radchenko, V. Shapoval, T. Tereshchenko, O. Dykyi Model for calculating quantitative indicators for assessing the efficiency of protecting a critical infrastructure object from impacts of unmanned aviation complexes.

The growing potential for the use of unmanned systems, which are designed to perform combat missions in the air, on the ground, on/under water than ever before, leads to an increase in threats to the defense landscape of defense forces. This is the reason for the rapid growth of interest in technologies that neutralize threats of this type. For the party that protects a critical object from an air attack by an unmanned aircraft complex (or group), the issue of guaranteed effectiveness or economic proportionality of methods of protection against low-cost attacks that can be carried out by such complexes is always relevant. The answer to this question begins with the availability of a device for calculating quantitative indicators for evaluating the effectiveness of protecting a critical infrastructure object from an air attack.

The process of functioning of a critical infrastructure object, which includes a deployed protection system, a control point and subsystems with critical equipment, through which the general purpose of this object is carried out, is proposed to be described by analogy with the model of the process of functioning of a renewable system with limited element reliability. In order to quantitatively assess the effectiveness of the protection of a critical infrastructure object from air attacks by unmanned aerial systems, it is proposed to take a comprehensive indicator of the reliability of the functioning of the renewable system, which consists of the following components: the readiness factor, the vulnerability factor and the protection from air attacks. Expressions of calculation formulas are given in accordance with the proposed process description model.

The obtained indicators for the quantitative assessment of the effectiveness of the protection of a critical infrastructure object from air attacks will be converted into specific proposals for persons who make decisions on the selection of the necessary types of countermeasures against unmanned aircraft systems for the expansion of the defense system, and which are required for the justification of financial and economic costs when overcoming this type of threat.

The directions of further research in order to ensure the specified indicators of the protection of a critical infrastructure object will be the method of calculating the reservation of protection means.

Keywords: *intensity of attacks, quantitative indicators of effectiveness, recovery time, time of normal operation, critical infrastructure object, anti-UAC protection system.*

Постановка завдання у загальному вигляді. Сучасна військово-політична обстановка у світі свідчить про виникнення нових загроз, пов’язаних із удосконаленням технологічної складової протиборчих сторін. Найбільш економічно розвинені держави активно розробляють та приймають на озброєння комплекси із безпілотними апаратами різного призначення разом із засобами протидії їм. Тому створення вітчизняних сучасних систем протидії загрозам, що виникають від застосування безпілотних комплексів, є актуальним завданням. Огляд загальних трендів розвитку перспективних видів озброєння [1] у збройних силах різних країн для розвідки та моніторингу, ретрансляції радіосигналів, цілевказівки та нанесення вогневого ураження ворожому учаснику воєнного конфлікту показує активне застосування технологій створення безпілотних роботизованих комплексів, які діють на землі, в повітрі на воді чи під водою.

У Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 р. № 392 [2], зазначається, що використання робототехніки та автономних безпілотних апаратів є одним із сучасних напрямів розроблення систем озброєнь. Розробка, виробництво безпілотних роботизованих систем, а також комплексів боротьби з ними, переживають бурхливе зростання в усьому світі. На ринок цього сегмента новітньої техніки виходять країни, які раніше не здійснювали наукових розробок і виробництва безпілотних літальних апаратів чи безпілотних наземних апаратів, а безперечними ж лідерами в цій галузі залишаються США, Ізраїль, Німеччина та Туреччина, що відображається у пріоритетах за обсягами фінансування їхніх програм зі створення та модернізації подібних систем. Експерти безпілотної техніки, для прикладу, прогнозують, що провідні країни світу матимуть до 2025 р. у складі бойової авіації до 80% безпілотної складової [3].

На сьогодні підрозділи сектору безпеки та оборони знаходяться під постійним впливом різноманітної номенклатури безпілотних авіаційних комплексів (далі – БпАК). Комплекси БпАК впливають на бойові порядки підрозділів, критичні об’єкти інфраструктури логістичного забезпечення та пунктів управління учасників сил оборони розвідкою і вогневим ураженням боєприпасами (в тому числі що баражують безпілотними літальними апаратами – камікадзе), як протягом підготовки, так і при веденні бойових дій. Не на останньому місці застосування противником засобів протидії безпілотним засобам наших підрозділів. З метою захисту військ та об’єктів інфраструктур учасників сил безпеки та оборони від подібного впливу виникає необхідність розробки систем, що забезпечать протидію БпАК.

Таким чином, робота щодо пошуку шляхів впровадження сучасних технологій захисту від БпАК, які практикуються світовими військово-промисловими групами, триває, тому дослідження підходів розрахунку кількісних показників оцінки ефективності захисту (коефіцієнти готовності, вразливості та захищеності) критичних об’єктів інфраструктури складових сектору безпеки та оборони автори цієї статті вважають актуальним.

Аналіз останніх досліджень і публікацій. Публікацій на тему розробки формалізованих моделей щодо повітряного захисту критичних об’єктів складових сил оборони і країни у цілому з огляду на важливість питання існує достатня кількість. Нижче наведемо деякі з них.

Автори методики [4] розрахунку ефективності прикриття дій наземних сил підрозділами протиповітряної оборони (далі – ППО), яка дає можливість оцінити ефективність ведення бойових дій зенітно-ракетних комплексів (далі – ЗРК) або зенітно-артилерійських комплексів (далі – ЗАК) при відбитті нападу з повітря, пропонували використовувати теорію ймовірностей для вибору параметрів елементів і структури підрозділів ППО. На підставі моделі марківських процесів розроблена модель оцінювання ефективності ППО з урахуванням інформаційних зв’язків між ЗРК (ЗАК), що забезпечує прогнозування ефективності стрільби вогневих засобів ППО у різних умовах очікуваних і поточних бойових дій. Таким чином, враховуються кількість засобів радіолокаційної інформації та структура інформаційних зв’язків між батареями ЗРК. Це впливає на середнє значення вірогідності виявлення повітряної цілі під час протиповітряного бою з урахуванням

знищення командних пунктів наземних сил, що очікувано допоможе військовому командирові підрозділів ППО різного рівня ієрархії оцінювати варіанти структури своїх підрозділів ППО, вибирати раціональні інформаційні зв'язки з кращою ефективністю прикриття та допоможе прийняти правильне рішення на відбиття ударів з повітря.

У наступному джерелі [5] здійснена оцінка ефективності бою (дій) підрозділів ППО в оборонному бою, яка враховує вибір показників ефективності бою (дій) та надає можливість створювати моделі оцінки бою (дій) для підрозділів ППО за допомогою математичного апарату, використовуючи теорію марківських процесів з безперервним часом і дискретними станами, тобто виникає можливість застосування методу аналітико-стохастичного моделювання. Наведений підхід дозволяє розраховувати ефективність бою (дій) підрозділів ППО по прикриттю загальновійськових підрозділів в оборонному бою. Методику можна адаптувати для розрахунку ефективності бою (дій) підрозділів ППО, які мають батареї зі змішаним складом зенітних засобів, що буде основою успішного виконання поставлених бойових завдань.

В [6] запропонована методика визначення достатнього рівня ефективності застосування підрозділу ППО Сухопутних військ (далі – СВ) при захисті загальновійськових підрозділів від ударів повітряного противника дає можливість визначити показники та критерії для оцінювання ефективності бойових дій підрозділів ППО СВ залежно від прогнозованого ступеня боєздатності загальновійськового підрозділу в ході загальновійськового бою (наскільки визначений склад сил та засобів ППО дозволяє зберегти визначену боєздатність загальновійськових підрозділів, що прикриваються від ударів з повітря).

Таким чином, для здійснення ефективного захисту критичного об'єкта інфраструктури (далі – КОІ) від впливу повітряних атак БпАК, необхідно визначити правила розподілу повітряних атак, націлених на КОІ, вибрати аналітичну модель оцінки його захищеності в умовах впливу такого типу атак для розрахунку коефіцієнтів готовності, вразливості та захищеності.

Мета статті: розробка моделі розрахунку кількісних показників оцінки ефективності захисту КОІ з системою захисту від БпАК в умовах впливу на нього потоку повітряних атак.

Виклад основного матеріалу. Розглянемо процес функціонування КОІ, який містить у своєму складі розгорнуту систему захисту (далі – СЗ), пункт керування (далі – ПК) та різні за функціональним призначенням підсистеми з критичним обладнанням (далі – ПКО) цього ж об'єкта (наприклад, у випадку гідроелектростанції це – гідросилове обладнання, водопідпірні та водоскидні споруди, енергетичні споруди, суднoплавні й лісосплавні споруди тощо) s, де $s = 1, 2, \ldots, S$, і S це – загальна кількість підсистем з критичним обладнанням об'єкта, що захищається (рис. 1). Кожна ПКО виконує свій функціонал, який направлений на загальне цільове призначення об'єкта та складається з деякої споруди, технічних засобів, які розміщені в ній, і особового складу, який забезпечує його роботу. Прогнозується, що по КОІ наноситься повітряний удар БпАК, а саме на систему захисту поступає потік БпАК, які атакують.

Введемо обмеження для запропонованої моделі функціонування КОІ в умовах повітряних атак:

на вхід КОІ надходить сумарний потік випадкових потоків повітряних атак, який в сумі наближається до простішого [7];

після СЗ виходить простий потік, який наближається до простішого;

під час повітряних атак інтервали функціонування КОІ розподілені за експоненціальним законом [8] (рис. 2, 3);

повітряні загрози, які надходять в потоці атак, співпадають з вразливостями КОІ з інтервалами часу, розподіленими за експоненціальним законом.

Спрощена структурна схема такого КОІ наведена на рисунку 1, де прийняті наступні позначення:

λ – інтенсивність загального потоку повітряних атак на КОІ, $\lambda = \lambda_з + \lambda_к$;

$\lambda_{кпк}$ – інтенсивність потоку повітряних атак на КОІ, які націлені на його ПК;

$\lambda_{кs}$ – інтенсивність потоку повітряних атак на КОІ, які націлені на деяку ПКО *s,* де $s = 1, \ldots, S$ після впливу на потік атак СЗ КОІ;

$\lambda_к$ – інтенсивність потоку атак після спрацювання СЗ на відбиття атаки (інтенсивність атак після успішної нейтралізації частини БпАК, що атакують), $\lambda_к = \lambda_{кпк} + \lambda_{кs}$;

$\lambda_з$ – інтенсивність потоку атак, який знешкодила СЗ КОІ;

A_s – деяка ПКО, де $s = 1, \ldots, S$.

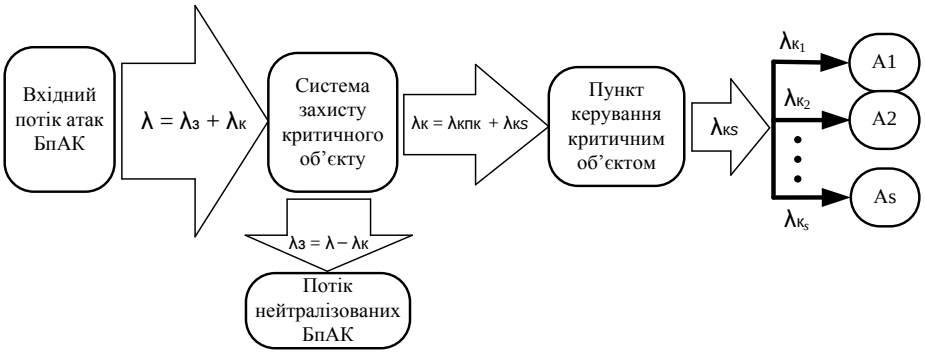


Рис. 1. Спрощена схема розподілу інтенсивностей атак, які впливають на складові КОІ

СЗ критичного об'єкта не є досконалою і тому відбувається тільки розрідження вхідного потоку атак БпАК на КОІ, частина, з яких з інтенсивністю $\lambda_{кпк}$ спрямована на ПК, а частина з інтенсивністю $\lambda_{кs}$ на інші складові КОІ (підсистеми критичного обладнання 1, 2, …, *S*). Будемо вважати, що вдала повітряна атака на ПК призведе до повного блокування функціонування КОІ у цілому. Вдала атака на обладнання *s*-ї критичної підсистеми не приведе до повної зупинки КОІ, а лише до втрати здатності виконувати ним свої функції у повному обсязі.

Розглянемо процес функціонування ПК після впливу на нього атаки БпАК. Будемо вважати, що в момент виявлення впливу атаки, а саме після її закінчення, обслуговуючий персонал КОІ одразу приступає до відновлення працездатності обладнання ПК та критичних підсистем *s*. Тривалість відновлення ПК – випадкова величина $t_{впкi}$, $i = 1, 2, \ldots$, з функцією розподілення $F_{впк}(t) = P\{t_{впк} < t\}$ та кінцевим математичним очікуванням середнього часу відновлення $T_{впк} < \infty$. В момент завершення відновлення ПК, КОІ відновлює нормальне функціонування до моменту впливу наступної повітряної атаки. Тривалість нормального функціонування ПК є випадковою величиною $t_{пкi}$, $i = 1, 2, \ldots$, з функцією розподілення $F_{нфпк}(t) = P\{t_{нфпк} < t\}$, $F_{пк}(t) = P\{t_{пк} < t\}$ та кінцевим математичним очікуванням $T_{нфпк} < \infty$.

Графічне зображення цього процесу зображено на рисунку 2, де прийняті наступні позначення:

t_i – моменти початку впливу повітряних атак на ПК, що не знешкоджені СЗ, де $i = 0, 1, 2, \ldots$;

$t_{впкi}$ – тривалість відновлення ПК після впливу повітряної атаки, де $i = 1, 2, \ldots$;

$t_{пкi}$ – тривалість нормального функціонування ПК, де $i = 1, 2, \ldots$.

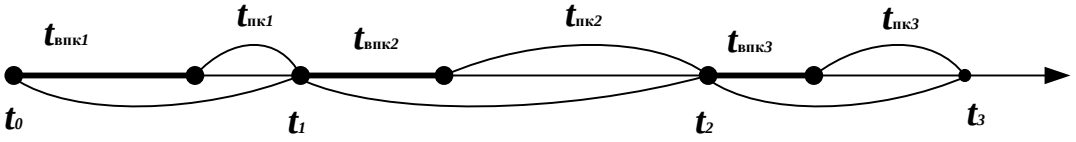


Рис. 2. Графічне зображення процесу функціонування ПК КОІ в умовах впливу повітряних атак з інтенсивністю $\lambda_{кпк}$

Аналогічно функціонує кожна ПКО *s* при впливі повітряних атак на них з сумарною інтенсивністю $\lambda_{кs}$, що не були нейтралізовані СЗ, де $s = 1, \ldots, S$. Процес функціонування ПКО в умовах впливу повітряних атак відображено на рисунку 3, де прийняті наступні позначення:

$t_{вsi}$ – реалізація випадкових величин часу відновлення працездатності ПКО s після впливу повітряної атаки, де $i = 1, 2, \ldots$;

t_{si} – тривалість нормального функціонування ПКО s після чергового відновлення працездатності КОІ, де $i = 1, 2, 3, \ldots$.

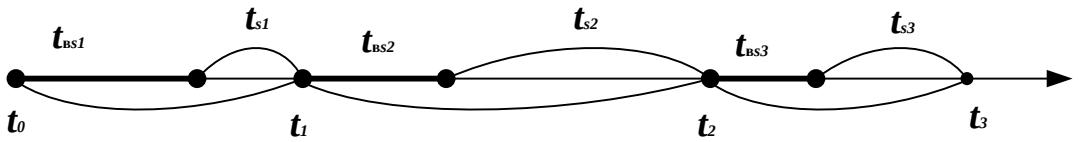


Рис. 3. Графічне зображення процесу функціонування ПКО s в умовах впливу повітряних атак з інтенсивністю $\lambda_{кs}$

Отже можна зауважити, що модель процесу функціонування КОІ в умовах впливу потоку повітряних атак перебуває у певній відповідності (аналогічна) до моделі процесу функціонування відновлюваної системи з обмеженою надійністю елементів. Тому для кількісної оцінки ефективності захисту КОІ від повітряних атак БпАК доцільно використати комплексний показник надійності функціонування відновлюваної системи $K_г$ – коефіцієнт готовності [8], коефіцієнти вразливості – $K_{вр}$ та захищеності – $K_з$ від повітряних атак [9].

Під коефіцієнтом готовності КОІ, який функціонує під впливом повітряних атак з інтенсивністю λ, будемо розуміти ймовірність того, що відновлювальний КОІ опиниться працездатним (буде нормально функціонувати) в довільний момент часу.

Визначимо через $p_0(t)$ ймовірність працездатності КОІ в момент часу t, а через $p_1(t)$ ймовірність непрацездатності КОІ в умовах потоку повітряних атак. Тоді зазначимо, що

$$p_0(t) + p_1(t) = 1. \tag{1}$$

Розглянемо формулу для ймовірності $p_0(t)$ під час впливу повітряних атак на КОІ при ураженні ПК, коли випадкові величини $t_{пкi}$ та $t_{впкi}$ (рис. 2) розподілені за експоненціальним законом [9] з параметрами $\lambda_{кпк} = 1/T_{нфпк}$, $\mu_{пк} = 1/T_{впк}$, де $\lambda_{кпк}$ – інтенсивність потоку повітряних атак на ПК; $\mu_{пк}$ – інтенсивність його відновлення; $T_{нфпк}$ – статистична оцінка середнього значення випадкової величини $t_{пкi}$; $T_{впк}$ – статистична оцінка середнього значення випадкової величини $t_{впкi}$.

Тоді для аналізу ймовірності $p_0(t)$ КОІ згідно з [8] можливо долучити наступну формулу (2):

$$p_0(t) = \frac{1}{1+K_в}\left(1 + K_в \cdot e^{-\lambda\left(\frac{1+K_в}{K_в}\right)t}\right), \tag{2}$$

де $K_в = T_{впк}/T_{нфпк}$ – показник норми відновлення КОІ (за рахунок відновлення працездатності ПК).

Використовуючи формулу (2), наведемо формулу (3) для коефіцієнту готовності ПК до початку атаки:

$$\lim p_0(t) = K_{гпк} = 1/(1+K_{впк}) = T_{нфпк}/(T_{нфпк}+T_{впк}). \tag{3}$$

Це означає, що існує стале значення ймовірності $p_0(t)$, яке не залежить від часу [9]. Таким чином ймовірність отримати КОІ працездатним у довільний момент часу в сталому режимі експлуатації, через деякий час після моменту $t = 0$ відповідає постійній величині, яку називають стаціонарним коефіцієнтом готовності. Зазначимо, що формула (3) вірна при довільних функціях розподілення випадкових величин $t_{пкi}$ та $T_{впкi}$. Ця формула найбільш вірогідно відображає фізичну суть коефіцієнта готовності як відносну частину часу, протягом якої КОІ знаходиться у працездатному стані.

Тоді статистична оцінка коефіцієнту готовності ПК (4):

$$K^*_{гпк} = 1/(1+K^*_{впк}) = T^*_{нфпк}/(T^*_{нфпк}+T^*_{впк}), \tag{4}$$

де $T^*_{\text{нфпк}}$ – статистична оцінка середнього значення випадкової величини $t_{\text{пк}i}$ (рис. 2) в сталому режимі (коли $t \to \infty$) знаходиться за виразом $T^*_{\text{нфпк}} = \frac{1}{n}\sum_{j=1}^{n} t_{\text{пк}j}$, а $T^*_{\text{впк}}$ – статистична оцінка середнього значення випадкової величини $t_{\text{впк}i}$ (рис. 2) знаходиться за виразом $T^*_{\text{впк}} = \frac{1}{n}\sum_{j=1}^{n} t_{\text{впк}j}$.

Розглянемо випадок, коли повітряна атака з інтенсивністю $\lambda_{\text{к}s}$ впливає на s-ту ПКО, де $s = 1, \ldots, S$ (рис. 3). Момент впливу повітряної атаки на ПКО s визначає втрату її працездатності та перемикання на режим відновлення. Оскільки всі підсистеми існують незалежно, тоді для s-ї ПКО можливо вивести формули (5), (6) коефіцієнтів готовності $K_{\text{г}s}$ та $K^*_{\text{г}s}$, де $s = 1, \ldots, S$ аналогічно наведеним вище виразам (3) та (4) для здійснення розрахунків коефіцієнтів для ПК:

$$K_{\text{г}s} = 1/(1+K_{\text{в}s}) = T_{\text{нф}s}/(T_{\text{нф}s}+T_{\text{в}s}); \quad (5)$$

$$K^*_{\text{г}s} = 1/(1+K^*_{\text{в}s}) = T^*_{\text{нф}s}/(T^*_{\text{нф}s}+T^*_{\text{в}s}), \quad (6)$$

де $T^*_{\text{нф}s} = \frac{1}{n}\sum_{j=1}^{n} t_{sj}$, $T^*_{\text{в}s} = \frac{1}{n}\sum_{j=1}^{n} t_{\text{в}sj}$.

Для того щоб застати ПКО s в довільний момент часу t в сталому режимі у працездатному стані, необхідно щоб в момент часу t були працездатними всі його підсистеми одночасно. З точки зору надійності таку систему можливо уявити як структурну схему, що складається з S ПКО, і коефіцієнт готовності $K_{\text{г}s}$ якої буде розраховуватися за формулою (7):

$$K_{\text{г}s} = \prod_{i=1}^{S} K_{\text{г}i} = \prod_{i=1}^{S} \frac{T_{\text{нф}i}}{(T_{\text{нф}i}+T_{\text{в}i})}, \quad (7)$$

Визначимо розрахунок коефіцієнта $K_{\text{г}}$ для КОІ, який функціонує в умовах впливу повітряних атак на ПК з інтенсивністю $\lambda_{\text{кпк}}$ та на всі підсистеми s з інтенсивністю $\lambda_{\text{к}s}$ (рис. 1). Використовуючи формулу повної ймовірності [10] для сталого режиму функціонування КОІ отримаємо вираз (8):

$$K_{\text{г}} = P_{\text{пк}} K_{\text{гпк}} + \prod_{i=1}^{S} P_s K_{\text{г}i}, \quad (8)$$

де $K_{\text{гпк}}$ та $K_{\text{г}s}$ розраховуються за формулами (4) та (7) відповідно, а $P_{\text{пк}}$ та P_s згідно з [10] виразом (9):

$$P_{\text{пк}}=\lambda_{\text{кпк}}/(\lambda_{\text{кпк}}+\lambda_{\text{к}s}),\ P_s=\lambda_{\text{к}s}/(\lambda_{\text{кпк}}+\lambda_{\text{к}s}), \quad (9)$$

де $P_{\text{пк}}+P_s = 1$.

Під коефіцієнтом вразливості КОІ – $K_{\text{вр}}$ вважатимемо співвідношення інтенсивності потоку атак, які пройшли скрізь захисний вплив СЗ на складові об'єкта – $\lambda_{\text{к}}$ до інтенсивності загального потоку λ атак на КОІ $K_{\text{вр}} = \lambda_{\text{к}}/\lambda$, і відповідно, $K_{\text{з}}$ – коефіцієнт захищеності КОІ згідно з [11] знаходимо за виразом $K_{\text{з}} = 1 - K_{\text{вр}} = 1 - \lambda_{\text{к}}/\lambda$.

Приклад розрахунку. Розглянемо випадок коли на ПК та ПКО у складі $S = 5$ підсистем впливає не знешкоджена повітряна атака з інтенсивністю відповідно $\lambda_{\text{кпк}} = 1/T_{\text{нфпк}} = 0{,}1$, $\lambda_{\text{к}s} = 1/T_{\text{нф}s} = 0{,}1428$, де $s = 1, \ldots, 5$. Приймемо, що середній час нормального функціонування ПК $T_{\text{нфпк}} = 10$ годин, а час нормального функціонування s-ї ПКО $T_{\text{нф}s} = 7$ годин, де $s = 1, \ldots, 5$. Середній час відновлення працездатності ПК $T_{\text{впк}}$ дорівнює 0,5 годин, а час відновлення працездатності кожної s-ї підсистеми $T_{\text{в}s} = 1$ година, де $s = 1, \ldots, 5$. Розрахуємо при цих вихідних даних значення стаціонарного коефіцієнта готовності КОІ – $K_{\text{г}}$, коефіцієнта вразливості КОІ – $K_{\text{вр}}$ та коефіцієнта захищеності КОІ – $K_{\text{з}}$.

Рішення. Використовуючи формули (3), (5), (7)–(9) проведемо розрахунки:

$$K_{\text{гпк}} = T_{\text{нфпк}}/(T_{\text{нфпк}}+T_{\text{впк}}) = 10/(10{,}0+1{,}0) = 0{,}9091;$$

$$K_{\text{г}i} = T_{\text{нф}i}/(T_{\text{нф}i}+T_{\text{в}i}) = 7{,}0/(7{,}0+1) = 0{,}875;$$

$$K_{\text{г}s} = \Pi_i\, K_{\text{г}i} = 0{,}875^5 = 0{,}5129.$$

Згідно з формулою (9) розраховуємо значення $P_{пк}$ та P_s:

$$P_{пк} = \lambda_{кпк}/(\lambda_{кпк}+\lambda_{кs}) = 0,1/(0,1 + 0,1428) = 0,4119,\ P_s = 1 – 0,4119 = 0,8581.$$

За допомогою виразу (8) розраховуємо значення коефіцієнта готовності $K_г$ КОІ у цілому:

$$K_г = 0,4119 \cdot 0,9091+0,8581 \cdot 0,5129 = 0,8146.$$

У випадку, коли інтенсивність загального потоку повітряної атаки $\lambda = 30,0$, а $\lambda_к = 0,2428$ коефіцієнт вразливості КОІ становитиме $K_{вр}= 0,2428/30,0 = 0,0081$, а коефіцієнт захищеності становитиме $K_з = 1 – K_{вр}= 1 – 0,0081 = 0,9919$, що дозволить оцінювати захист КОІ та в подальшому приймати рішення, щодо необхідності оптимізації засобів СЗ від БпАК.

Висновки. Таким чином, розглянутий підхід розрахунку кількісних показників оцінки ефективності захисту критичного об’єкта інфраструктури складових сектору безпеки та оборони в умовах повітряних атак БпАК передбачає використання моделі процесу функціонування відновлюваної системи з обмеженою надійністю елементів. Запропонована модель оцінки захисту критичного об’єкта від нападу БпАК дозволяє визначити основні показники ефективності захисту і може використовуватись для розробки оперативних рішень щодо залучення та визначення кількості таких засобів протидії, які б гарантовано забезпечували задані значення відповідних показників захисту.

Предметом подальших досліджень стане методика розрахунку резервування засобів захисту критичного об’єкта інфраструктури для забезпечення заданих показників його захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кваша Т. К. Світові наукові та технологічні тренди у сфері забезпечення національної безпеки / Т. К. Кваша. 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: 27.03.2023).

2. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/news/volodimir-zelenskij-zatverdiv-strategiyu-nacionalnoyi-bezpek-63577 (дата звернення: 27.03.2023).

3. Щодо розвитку виробництва безпілотних роботизованих систем на основі державно-приватного партнерства: аналітична записка // Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/schodo-rozvitku-virobnictva-bezpilotnikh-robotizovanikh-sistem-na (дата звернення: 27.03.2023).

4. Коваленко С. П. Методика розрахунку ефективності прикриття наземних сил підрозділами ППО при веденні локальних конфліктів / С. П. Коваленко, А. Ф. Волков, С. І. Корсунов // Збірник наукових праць Національної академії Національної гвардії України. 2021. Вип. 1. С. 12–23. URL: http://nbuv.gov.ua/UJRN/znpavs_2021_1_4 (дата звернення: 27.03.2023).

5. Лезік О. В. Розробка рекомендацій командиру підрозділу ППО з підвищення оперативності розрахунку вогневих можливостей підрозділу в умовах оборонного бою / О. В. Лезік, Г. А. Левагін, А. Ф. Волков, М. В. Мужук, В. Ю. Лукашов, М. В. Шевченко // Системи озброєння і військова техніка. 2021. № 3 (67). С. 7–18. URL: https://journal-hnups.com.ua/article/download (звернення: 27.03.2023).

6. Волков А. Ф. Методика визначення достатнього рівня ефективності бойових дій підрозділу протиповітряної оборони сухопутних військ для збереження боєздатності загальновійськових підрозділів, що прикриваються // А. Ф. Волков, О. В. Лезік, М. В. Мужук, І. В. Гуленов, Д. О. Васильченко / Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4 (70). С. 7–14. URL: https://journal-hnups.com.ua/index.php/zhups/article/view/751/649 (дата звернення: 27.03.2023).

7. Давыденко В. П., Доронин Є. М. Основы военной кибернетики. Ленинград: ЛВВИУС, 1980. 314 с.

8. Жердєв М. К., Лєнков С. В., Креденцер Б. П. Фізичні основи теорії надійності: підручник. Київ: Київський національний університет імені Тараса Шевченка, 2008. 215 с.

9. Куцаєв В. В., Радченко М. М., Терещенко Т. П. Модель оцінки готовності інформаційно-телекомунікаційного вузла зв’язку в умовах кібернетичних атак // Збірник наукових праць ВІТІ. Київ, 2019. Вип. 3. С. 43–50 URL: https://www.viti.edu.ua/files/zbk/2019/5_3_2019.pdf (звернення: 27.03. 2023).

10. Вентцель Е. С. Теория вероятностей: учебник для вузов. Москва: Высш. шк., 1999. 576 с.

11. Куцаєв В. В. Радченко М. М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла // Збірник наукових праць ВІТІ. Київ, 2018. Вип. 2. С. 67–76. URL: https://www.viti.edu.ua/index.php?view=coll_2018_2 (дата звернення: 27.03.2023).

DOI: 10.58254/viti.3.2023.11.88

UDC 621.396.4

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

A MODEL OF SITUATIONAL CONTROL OF THE TELECOMMUNICATION AERIAL PLATFORM FLIGHT TRAJECTORY TO COLLECT DATA FROM NODES OF A WIRELESS SENSOR NETWORK

Романюк В. А., Гримуд А. Г. Модель ситуаційного управління траєкторією польоту телекомунікаційної аероплатформи для збору даних з вузлів безпроводової сенсорної мережі.

Телекомунікаційна аероплатформа на базі безпілотного літального апарата розглядається як перспективна технологія для збору даних у безпроводових сенсорних мережах в умовах відсутності зв'язності між вузлами мереж та будь-якої комунікаційної інфраструктури. Фактично телекомунікаційна аероплатформа виступає в ролі мобільного шлюзу та має можливість збирати дані з декількох вузлів одночасно. Траєкторія його переміщення, локація точок та інтервали обміну даними суттєво впливають на ефективність процесу збору даних. У статті розглядається модель ситуаційного управління побудовою траєкторії польоту для збору даних телекомунікаційною аероплатформою для досягнення певних цільових функцій: оптимізації часу збору даних та часу функціонування мережі.

У роботі класифікована множина ситуацій на мережі та визначені відповідні продукційні правила з побудови траєкторії телекомунікаційної аероплатформи, які реалізують визначену ієрархію прийняття рішень: мережа, кластер, телекомунікаційна аероплатформа, вузол з врахуванням цільових функцій управління. На мережевому рівні застосовується правила визначення кількості та розмірів кластерів, будується базове рішення з визначення точок збору та траєкторії їхнього обльоту. На рівні кожного кластера телекомунікаційна аероплатформа в процесі польоту корегує базове рішення на основі врахування параметрів фактичного стану вузлів кластера. На рівні взаємодії телекомунікаційна аероплатформа – вузол оптимізуються енерговитрати вузла та швидкість передачі даних завдяки зменшенню відстані вузла до телекомунікаційної аероплатформи. Для скорочення перебору правил запропоновані метаправила. Такий підхід дозволяє досягати оптимізації цільових функцій процесу збору даних та забезпечити прийняття рішення в реальному часі. Результати імітаційного моделювання довели можливість зменшення часу збору даних на 10–15 % або підвищення часу функціонування мережі на 12–17 % порівняно з існуючими рішеннями.

Ключові слова: *безпроводова сенсорна мережа, телекомунікаційна аероплатформа, траєкторія польоту, збір даних, база правил, ситуаційне управління.*

V. Romaniuk, A. Hrymud A model of the situational control of the telecommunication aerial platform flight trajectory to collect data from nodes of a wireless sensor network.

A telecommunication aerial platform (TA) based on an unmanned aerial vehicle is considered a promising technology for data collection in wireless sensor networks in the absence of connectivity between network nodes and any communication infrastructure. In fact, TA acts as a mobile gateway and could collect data from several nodes at the same time. The trajectory of its movement, location of points and data exchange intervals significantly affect the efficiency of the data collection process. The article considers a model of situational control of flight trajectory construction for data collection to achieve certain target functions: optimization of data collection time and network operation time.

In the work, a set of situations on the network is classified and corresponding production rules for building a TA trajectory are defined, which implement a defined decision-making hierarchy: network, cluster, TA, node, considering the target management functions. At the network level, the rules for determining the number and size of clusters are applied, and a basic solution for determining the collection points and the trajectory of their flight is being built. At the level of each cluster, the TA adjusts the basic solution during the flight based on considering the parameters of the actual state of the cluster nodes. At the level of TA-node interaction, the energy consumption of the node and the speed of data transmission are optimized by reducing the distance of the node to the telecommunication aerial platform. To reduce the number of rules, meta-rules are proposed. This approach allows you to achieve optimization of the target functions of the data collection process and ensure decision-making in real time. The simulation results proved the possibility of reducing data collection time by 10–15 % or increasing network operation time by 12–17 % compared to existing solutions.

Keywords: *wireless sensor networks, telecommunication aerial platform, UAV trajectory, data collection, rule base, situation control.*

1. Statement of the problem. In recent years, there has been a rapid development of wireless sensor network technologies that are used to solve various problems: monitoring the parameters of objects (territories) for compliance with environmental standards; monitoring the condition of crop fields, forests, product pipelines, power lines, borders; search and rescue and military operations (monitoring the movement of their own and enemy troops), etc.

The peculiarity of wireless sensor networks (WSNs) 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. Certain areas of application of WSNs determine the peculiarities of the placement and functioning of sensor nodes (in remote or disaster-affected areas without any available public telecommunications infrastructure, a significant distance between nodes or terrain does not allow building a coherent network structure, etc.) In these conditions, it is proposed to use telecommunication aerial platforms (TA), which are built based on unmanned aerial vehicles (UAV), as a mobile air gateway to collect data from network nodes [1; 2]. This allows: first, to organize the collection of monitoring data from unconnected network nodes; second, to obtain line-of-sight radio channels to the TA node; and third, to reduce the energy consumption of nodes for data transmission (increase the network lifetime), unlike the classical architecture of building sensor networks.

This raises the scientific task of constructing a trajectory for the overflight of the TA nodes of the network, determining the points (intervals) of data collection to achieve certain target functions: minimizing the energy consumption of nodes (maximizing the network operation time) and/or minimizing the data collection time [3; 4]. Solving this problem will allow to control the parameters of the telecommunication aerial platform and nodes, which will increase the network lifetime and reduce the time of monitoring data collection (for example, this parameter is critical in military applications). Models and algorithms for solving this problem can be used in specialized network management system software.

2. Analysis of recent publications. The solution to the problem of overflight and direct data collection by a telecommunication air platform from each WSN node can be achieved in the following ways (according to these methods, the research is proposed).

1. Flying over the entire territory (area) occupied by the WSN with simultaneous collection of monitoring data from the network nodes. Researchers have analyzed the options for flying over the entire network area [5]: by squares, by spiral, by angle, etc. The purpose of the study is to reduce the length of the flight route and, accordingly, the time of the network flight. However, the time to fly over the entire area of the WSN remains very significant, which imposes additional requirements on the technical characteristics of the aircraft. This method 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 power level, etc.)

2. Flying over only certain clusters (zones) of the WSN network in conditions of heterogeneous node placement. To do this, before the TA flight, the ground network control center (GCC) conducts its virtual clustering, determines the points (intervals) of monitoring data collection by the telecommunication air platform in clusters (in the simplest case, the data collection point is the geometric center of the cluster), builds the shortest route to fly around the data collection points.

Under such conditions, in most publications [6-8], the calculation of the TA flight route is considered only as a solution to the classical traveling salesman problem - finding the shortest route between the start and end point of the TA flight with a flight over the data collection points. This problem belongs to the class of NP-hard problems. Obtaining an exact solution for a network of significant dimensionality is problematic. Therefore, in practice, heuristic algorithms are proposed to obtain an approximate solution that have a low computational complexity: nearest neighbor [6], spiral [7], FPPWR (Fast Path Planning with Rules) [8], convex hull CHIH (Convex Hull Insertion Heuristic) [9], etc. However, in such a problem statement, only the shortest flight route is calculated, the state of the nodes' parameters is not considered, and the energy consumption of the nodes is not optimized. Therefore, the application of the shortest path search algorithm can be used for the initial (basic) solution for its further improvement.

In the work [10] study of several strategies for constructing a flight path and collecting data from the TA in a clustered WSN are investigated: flying through the center of the cluster and collecting data during the flight at the closest node-to-AV distance; flying through critical nodes in clusters and collecting data during the flight; flying 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 research [11], simple heuristics for building a TA trajectory are considered, which try to reduce the data collection time by sequentially adding potentially possible hanging points.

In paper [12], it is proposed to determine the TA data collection points considering the ability of the MAC protocol to change the radio channel bandwidth depending on the radio range. However, these solutions do not consider the ability of the MAC protocol to change the transmission power (reduce the energy consumption of node batteries).

In research [13], a deep neural network is used to find the 3D flight path of the TA to optimize the data collection time and radio channel bandwidth, but the network lifetime is not optimized.

In the work [14], the authors proposed a method of direct data collection of TA from WSN nodes, which allows for multi-criteria optimization of data collection indicators. However, the process of deciding on the flight path for data collection is not disclosed in detail. Therefore, the proposed article develops a decision-making mechanism using a situational management model.

The dynamic formation of clusters and their sizes, the trajectory of TA movement, the location of points and intervals of TA data exchange with nodes significantly affect the efficiency of data collection. However, publications [1-13] do not consider several efficiency criteria, their dependence on a set of parameters of the state of network nodes and clusters, and the trajectory of the vehicle. Thus, the unresolved problem when considering the process of building a TA flight path is to determine the points (intervals) of the data collection trajectory while considering two criteria: minimizing the time of data viewing and maximizing the network operation time.

The aim of the article is to develop a model for situational control to build a flight path for a telecommunication air platform with defining points (intervals) for collecting data from nodes in the WSN to achieve certain object functions.

Summary of the main material.

Problem statement. We consider a wireless sensor network of considerable dimensions (tens, hundreds of sensor nodes) with stationary nodes that are randomly located in a remote area, are not interconnected, and operate in the absence of any public telecommunications infrastructure. Each sensor node has the following main elements: battery, touch sensors, processor, memory, transceiver, antenna, positioning system, and control system. In the process of operation, the node collects and stores environmental parameters (objects of observation) of the monitoring area assigned to it before the TA approaches.

The UAV-based TA has additional equipment to implement the data collection process: a processor, memory, a transmitter, an antenna, a positioning system, and a corresponding control system. The TA flies around the data collection points (intervals) along a certain trajectory, using a directional antenna to form a ground coverage area (radio communication) of the WSN nodes with a radius of R_k (the size of the temporary k-th cluster of the local network). When nodes enter the TA radio connectivity zone, it establishes radio communication with them, determines the exchange schedule, and receives monitoring data from the nodes (Fig. 1).

The planning of temporary network clusters, trajectory and speed of the TA flight, points (intervals) of data collection from nodes, etc. is carried out by the ground-based network control center. The TA control system allows for independent decision-making (on clustering, flight path, data collection points and intervals, etc.) in the absence of communication with the ground network control center.

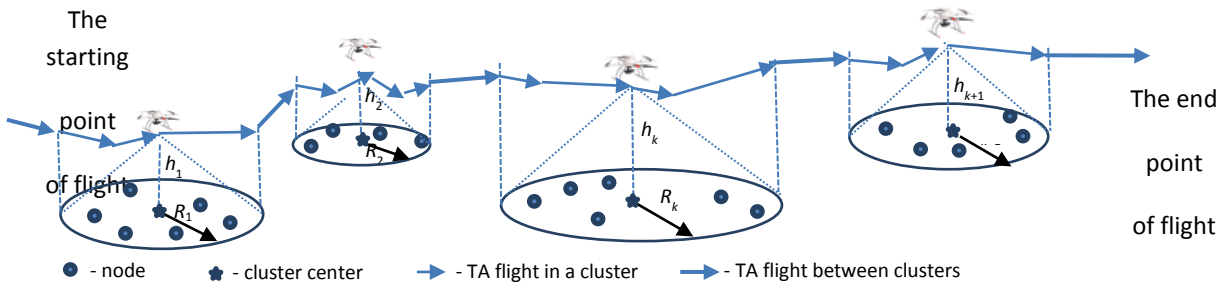


Fig. 1. An example of a TA fly over of cluster nodes through its center

Given:

– Monitoring area of WSN nodes; number of network nodes $i = 1 \ldots N$, coordinates of their location on the ground (x_i, y_i); the amount of monitoring data collected by the i-th node - V_{dmi}.

– 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 of data for the selected MAC protocol and type of equipment, etc.

– Flight characteristics of the TA - speed, altitude, flight time, the ability to hover and move in space at a constant or variable speed, etc.

– Communication characteristics of the TA - MAC protocol, antenna, transceiver parameters, etc.

Restrictions and requirements:

– The TA flight area has no prohibited zones; the flight trajectory is formed in the form of certain coordinates of points in space (modeling of the TA flight process is not considered).

– Information about the nodes' state parameters (location coordinates, battery energy level, amount of monitoring data) is collected during the initial overflight of the TA network, and then the information about the nodes' state is updated during each round of overflight.

– TAs and sensor nodes have radio equipment with the same MAC protocol, which allows to change the data transmission rate depending on the signal-to-noise ratio ("radio channel range") [2] and to adjust the transmission power (energy consumption for transmission) [14], for example, IEEE 802.11.

– Memory capacity of sensor nodes and telecommunication aerial platform is sufficient to store monitoring data.

– The value of the battery (fuel) energy of the TA is sufficient for a round of network circling.

– The control algorithms implemented by the TA should have a low computational complexity to ensure the real-time data collection process.

It is necessary to: determine the trajectory and flight speed of the TA, the points (trajectory intervals) of TA data collection, the procedure (schedule) of TA data exchange with cluster nodes. At the same time, it is necessary to implement one of the defined objective functions (OF) of data collection management [14]:

– Minimize data collection time T_{col}

$$T_{col} \to min \tag{1}$$

ensuring a given network operation time $T_{ot} \geq T_{otgiv}$.

– maximum operating time

$$T_{ot} \to max \tag{2}$$

ensuring a given data collection time$T_{col} \leq T_{col\,giv}$.

– Optimization of both criteria, considering their priority

$$\begin{cases} T_{col} \to min \\ T_{ot} \to max \end{cases} \tag{3}$$

– Obtaining an acceptable solution

$$T_{col} \le T_{colgiv} \text{ and/or } T_{ot} \ge T_{otgiv}, \quad (4)$$

with restrictions Ω on:

– Type of TA (rotorcraft); speed, altitude, time and range of TA flight – $v = [v_{min}, v_{max}]$; $h = [h_{min}, h_{max}]$; $t_{fly} \le t_{flymax}$; $L_{fly} \le L_{flymax}$.

– Number of clusters in the network – $1 \le k \le N$.

– Initial energy of the node batteries $e_{min} \le e_i \le e_{max}$ and TA $e_{TA} \le e_{TAmax}$.

– An amount of monitoring data of each i-th node – $V_{dmi} \le V_{dmmax}$.

– Node-TA radio communication range – $d_{i-TA} \le d_{max}$.

– The radius of the TAs coverage area (cluster) – $R_{min} \le R \le R_{max}$.

The solution. To solve the problem in accordance with the objective functions, it is proposed to divide the decision-making process into stages [14]:

– To perform virtual two-step (homogeneous and heterogeneous) clustering of the network and determine the number of clusters $k = 1 \dots K$ of the network, their sizes.

– Determine the hang points Q_k for the collection of TA data from the cluster nodes with coordinates in space $(x, y, h)_k$.

– Calculate the basic (initial) flight route of the TA in the network from the initial position A to the final position B through the data collection points Q_k from the cluster nodes.

– Build the flight path of the TA in clusters with the definition of data collection points (intervals), the schedule of data exchange with nodes by adjusting the base route.

Let's consider in detail the sequence of the hierarchy of the main stages of optimization (Fig. 2).

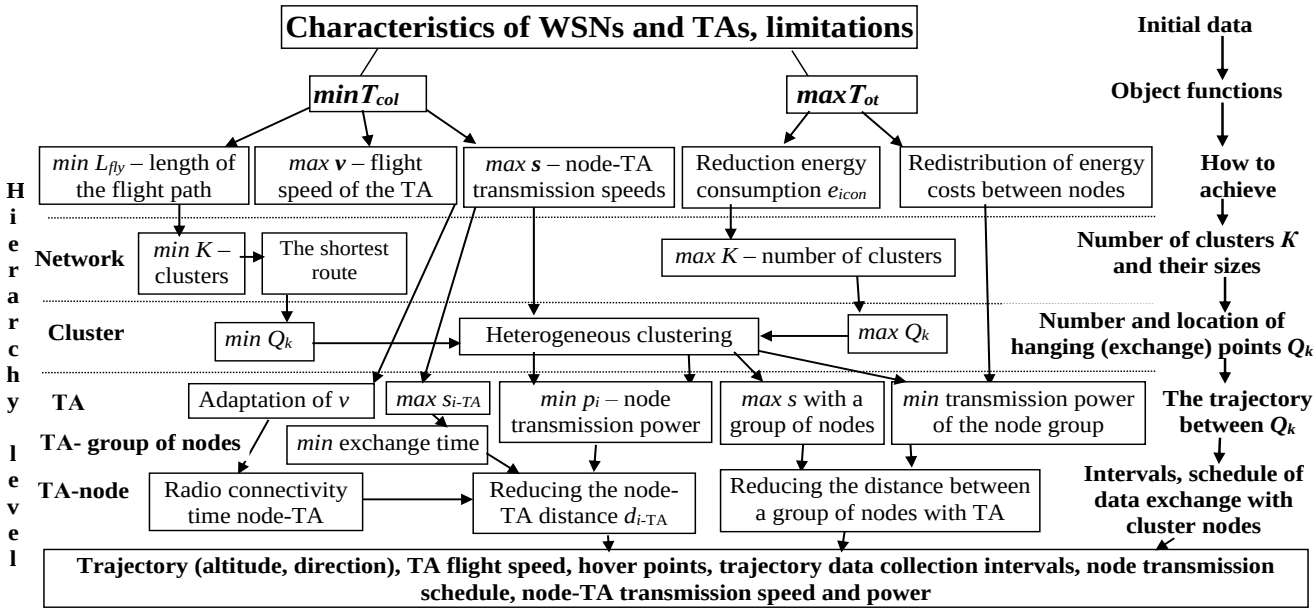


Fig. 2. The hierarchy of the decision-making process for achieving the objective functions

The time of data collection T_{col} by the telecommunication aerial platform from the network nodes depends on the following parameters (5) [14]:

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

– Number of nodes $i = 1 \dots N$ and coordinates of their location on the territory (x_i, y_i).

– Number of $k = 1 \dots K$ clusters, their area, number of nodes n_k, relative positioning.

– Trajectory *TR* of the TA flight in the network defined by the strategy St_k overflight and data collection from the nodes of each *k*-cluster (in-flight and/or hover data collection, one or more hover points in the cluster, etc.).

– Flight velocity of the TA v.

– The amount of monitoring data V_{dmi} in the network nodes.

– Number of data collection points Q_k with coordinates in space $(x, y, h)_k$ in each *k*-th cluster when the TA hangs.

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

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

– flight altitudes h_k, restrictions Ω resources of nodes and TAs.

Reducing the number of clusters *k* in the network reduces the length of the TA flight route (respectively, the flight time), but leads to an increase in the energy consumption of sensor nodes (due to the increase in the node-TA distance) and an increase in the node-TA exchange time (decreases the transmission rate of the MAC protocol). And vice versa. An increase in the number of clusters leads to an increase in the length of the TA flight route, but reduces the node-TA distance and, accordingly, reduces the node-TA exchange time and node energy consumption. That is, there is a certain optimum of the number of clusters *k*, their sizes, the location of points Q_k in them, and the intervals INT_i of TA data collection, which determines a compromise solution with respect to the objective functions.

That is, reducing (minimizing) data collection time T_{col} can be achieved by (Fig. 2):

– Reducing the length of the flight path (reducing the number of clusters and building the shortest route to fly around them).

– Increasing the speed of movement of TAs (determining the maximum v_{max} flight speed of TAs between clusters and, if there is no connectivity between nodes in the cluster, adapting v in clusters to the time required to exchange data with nodes).

– Increasing the transmission rate in the radio channels TA-node s_{i-TA} by reducing the distance TA-node d_{i-TA} (this is provided by the MAC protocol), i.e., by bringing the TA trajectory points closer to node i.

The increase in the network operation time T_{ot} can be achieved by:

– Reducing the energy consumption of nodes (reducing the transmission power of a node) by reducing the TA-node distance

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

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

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

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

– The relative position of the nodes relative to the trajectory (it is advisable to exchange data in the nearest intervals of the TA's flight path 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.

The achievement of the objective functions occurs sequentially at the following hierarchy levels: network, cluster, TA, group of nodes, and individual node. At the network level, performance indicators are optimized by determining the number of clusters and their sizes (by determining the flight height or hover of the TA), and by building the shortest flight route.

At the cluster level, the number and coordinates of hover points (intervals), the strategy for flying over them and collecting TA data are determined. Possible strategies are shown in Fig. 3 [10; 14].

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

– Energy consumption of each cluster node for data collection (transmission and reception) $e_{\text{con}i}$, total energy consumption of cluster nodes $E^k_{\text{con}} = \sum_{i \in k} e_{coni}$ [14].

– Time of data collection in the cluster t^k_{col}, which is determined by the flight time and hover time of the TA.

At the levels of TA-group of nodes, TA-node, the distance is determined (actually, the trajectory points are adjusted), which allows optimizing the time of exchange between them and energy consumption.

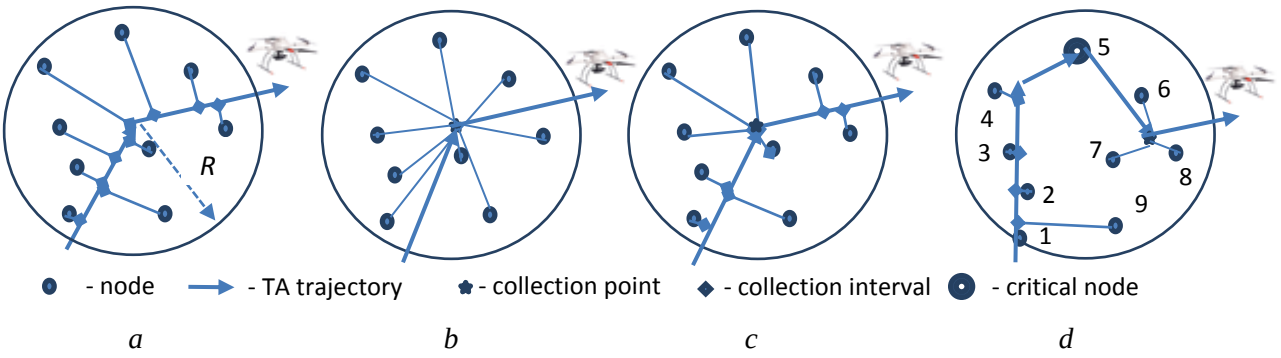


Fig. 3. Main options for flight strategies and data collection from cluster nodes:
a – data collection during the flight of the TA through the center (center of mass) of the cluster;
b – data collection only when the TA hovers in the center (center of mass) of the cluster;
c – data collection during the flight and with hovering at one point (center) – a hybrid strategy;
d – data collection in flight and several hovering points (proposed strategy)

To reduce the options for searching and reduce the time for finding a solution along the trajectory of flying over the nodes and collecting data, it is proposed to use the situational control method. The essence of situational management is reduced to the transformation of state information (current situation) $S^{current}$ into a controlling influence U_z, that brings the control object to a new state S^{new} ($S^{current} \rightarrow U_z \rightarrow S^{new}$), where $z = 1 \ldots Z$ – a set of controlling influences. For this purpose, a limited number of situations S (a set of parameters of network states, clusters, TAs, nodes) is formed and classified, a certain set of controlling influences U_z and an appropriate base of product-type decision-making rules is developed: **IF <condition>, THEN <action>** [14] (Fig. 4).

According to the objective functions, the rules are divided into:

– On the network – minimum or limitation of data collection time T_{col}, maximum or achievement of a certain network operation time T_{ot} (1)–(4).

– in the k-th cluster – minimum data collection time t^k_{col}, minimum energy consumption of nodes E^k_{con};

– in the i-th node – minimum time of collection (exchange) with TA $t_{coli-TA}$, minimum energy consumption $e_{coni-TA}$.

By network, cluster, TA, node status parameters that determine the situation on the network:

– Parameters of the WSN, TA, nodes, number of clusters, their area, number of nodes in a cluster, their relative location, data collection parameters (collection time, operation time), etc.

– A set of parameters of the cluster nodes (energy, data volume, relative location).

– Location of the nodes relative to the flight path of the TA in the cluster.

– Node status parameters (coordinates, battery power, amount of monitoring data).

– Parameters of node exchange with TA (time, energy consumption of the node), etc.

– Node status parameters: battery power level, amount of monitoring data, location.

In terms of controlling influence, it is possible to determine (change): the number of clusters (by changing the altitude of the TA, the antenna pattern), the location of hovering and data collection points, the strategy of flying around the cluster nodes, the flight path, the TA-node

exchange intervals on the path, the transmission power of the nodes, the TA flight speed on certain parts of the path, etc.

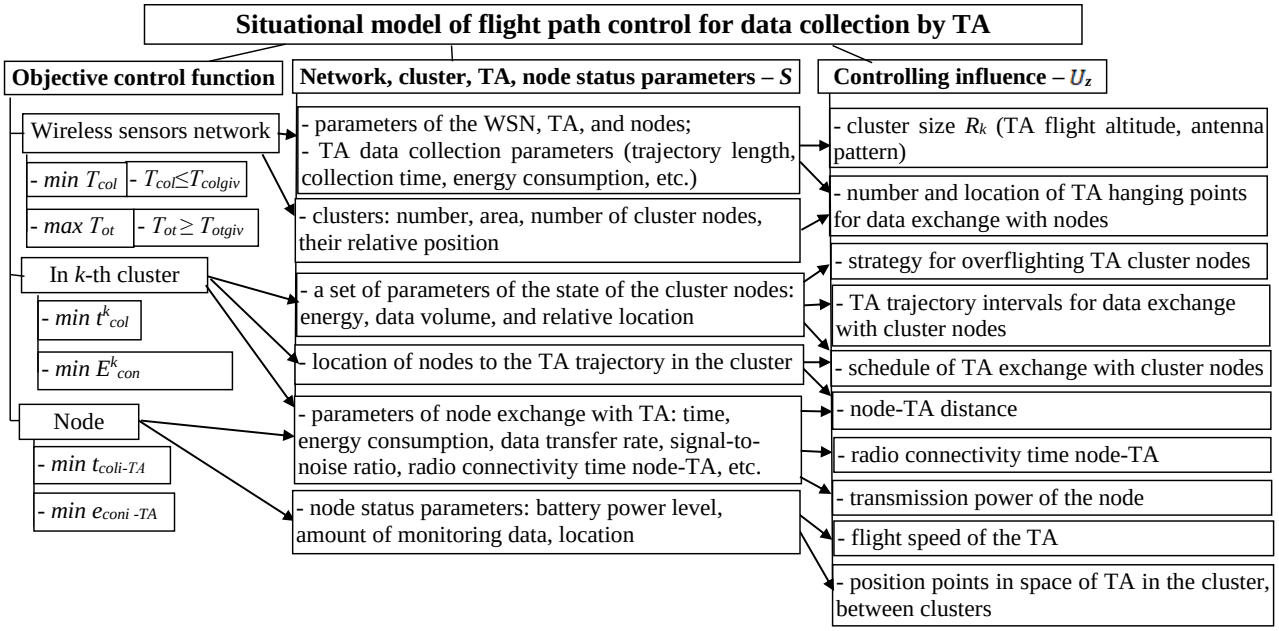


Fig. 4. Scheme of the situation management model

Let's consider several general rules for determining the flight path and data exchange, which are conditionally divided into groups (for determining the number and size of clusters, data collection points (intervals), trajectory correction, redistribution of energy consumption of nodes, etc.) that implement the corresponding control objectives (1)–(4) [14].

The rule for determining the number of clusters: IF the object function T_{col}→min (T_{ot}→max), THEN increase (decrease) the size and number of clusters.

The rule for determining hang points for data collection: IF there are clusters of nodes in the cluster (loaded or with low battery energy), THEN determine the TA hang point for collecting data from these cluster nodes, which minimizes the exchange time or energy consumption of these nodes.

The rule for correcting the flight path TA: IF it is necessary to reduce the transmission time in the node-TA radio channel and/or reduce the energy consumption of the node, THEN it is necessary to place (move) the TA trajectory points closer to the node.

The rule to reduce and equalize transmission costs: IF multiple nodes are competing for exchange intervals with the TA, THEN determine the closest INT exchange interval on the TA's flight path to the node with the lower battery energy.

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

IF the object function T_{col}→min, the number of nodes in the cluster is small (medium) and the amount of data is insignificant, THEN determine the basic strategy (TA flight through the center of the cluster with the definition of exchange intervals on the flight path) (Fig. 5*a*).

IF the object functionT_{ot}→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. 5*b*).

Rule for shortening the trajectory length in a cluster (Fig. 5*c*): IF the objective function T_{col}→min, the i-th node is at a considerable distance from the TA flight path, has a significant battery level and a small amount of data, THEN plan the TA exchange with node i in motion.

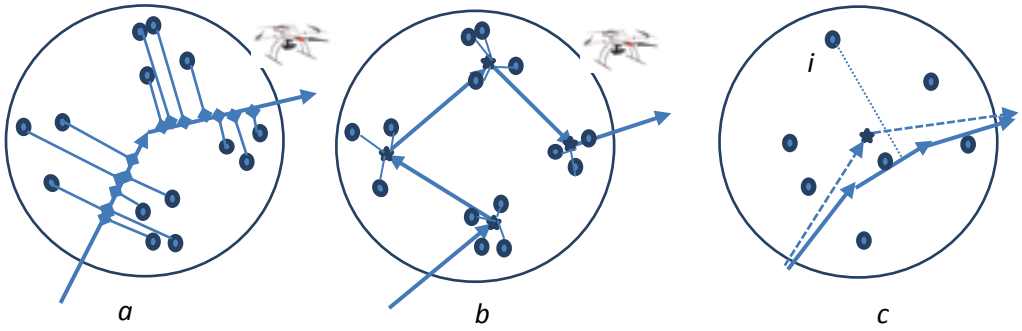


Fig. 5. Variants for implementing the rules for building a flight path and collecting TA data

The rule for maintaining "critical" nodes: IF a node has a critical battery level (significant amount of data) and is a significant distance from the TA flight path, THEN change the TA flight path to reduce the distance from that node.

To reduce the list of possible variants of the TA flight trajectory and determine the points (exchange intervals), a set of meta-rules is proposed that determine the priority sequence of rules for achieving the target function according to its priority. Let's consider a few [14].

Metarule 1: IF the objective function is T_{col}→min, THEN (the problem is reduced to a single-criterion optimization) finding:

– The maximum number of network clusters;

– Set the basic trajectory of the TA through the center of the clusters, find the shortest path (use the shortest path search algorithm) to fly around the centers.

– Determine possible additional TA collection points (hang-ups) according to the position and amount of data in the cluster nodes (grouping of nodes with a significant amount of data), recalculate the shortest path.

– Determine the strategy of flying around the cluster nodes.

– Set the maximum speed of TA movement in the cluster (which meets the requirements for TA data exchange with cluster nodes).

– Calculate the intervals and schedule of node transmissions during the flight of the TA, considering the state of the nodes using rules that are focused on increasing the transmission rate in the radio channel.

Metarule 2: IF T_{col}→min and T_{ot}→max, the first OF takes precedence over the second, THEN (lexicographic optimization method):

– Find a certain significant number of network clusters.

– Determine the collection points (hang-ups) of TA according to the priority of the OF.

– Determine the strategy for flying around the cluster nodes.

– Calculate the TA trajectory through the collection points.

– Calculate the intervals and schedule of node transmissions during the flight at a minimum distance, considering the available energy of the nodes.

The proposed situational model is realized by the interaction of algorithms in the GCC, control systems of the TA, and nodes. The network management cycle consists of the following stages: collecting data on the state of network nodes (performed by the TA in the next round of overflight), analyzing and identifying the state of the network, searching and making decisions, implementing the decision during the overflight.

In accordance with the OF, the GCC solves the following main tasks:

– Network clustering, optimization of the number and size of clusters.

– Calculation of the number and coordinates of data collection points (hovering) of the TA.

– Determination of the strategy for overflight and data collection of TAs in clusters.

– Calculation of the TA flight trajectory with the determination of its intervals and exchange schedule.

In the absence of radio communication between the TA and the GCC, the control tasks are performed by the TA in an autonomous mode. The diagram of the generalized algorithm for implementing the model, which is part of the method of direct data collection by the TA [14], is shown in Fig. 6. Let us consider the main steps of the method.

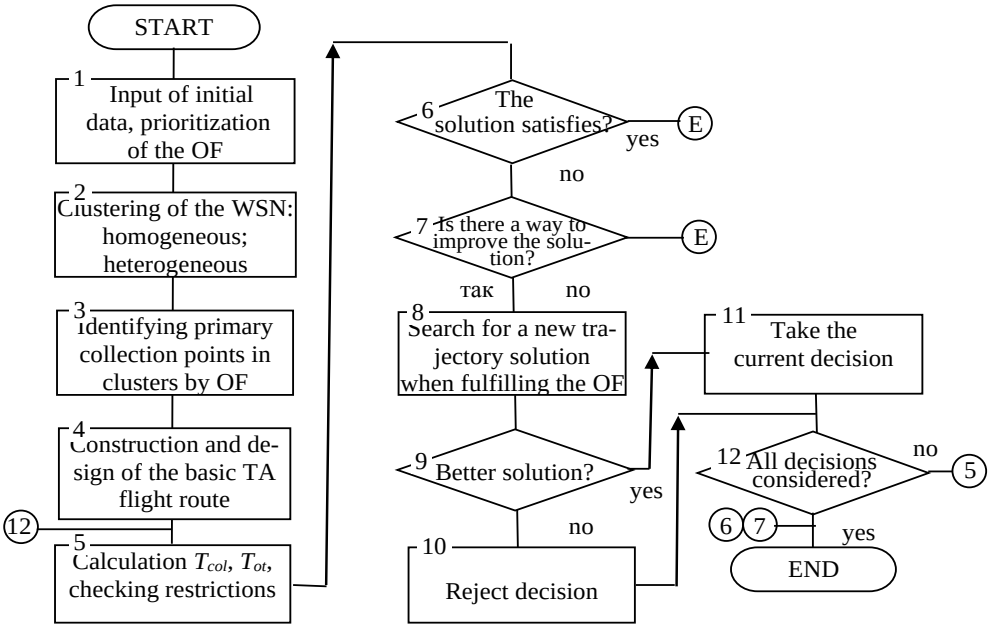


Fig. 6. Schematic algorithm for finding a solution along the flight path and data collection

Step 1. Collection and entering data (according to the task).

Step 2. A 2-stage clustering of the network is implemented to achieve the specified OFs:

– homogeneous clustering of the network – finding a certain number of clusters using the FOREL (FORmal ELement) cluster analysis algorithm by applying a rule base to adapt the coverage radius *R.*

– heterogeneous clustering – clustering (splitting) of clusters according to the rule base, the priority of the OF and the relative position of clusters and the state of nodes in clusters.

Step 3. Determination of primary (base) TA data collection points in each cluster according to the analytical models proposed in [14].

Step 4. Building the basic route of the TA flight along the identified data collection points by searching for the shortest path (for example, Convex Hull Insertion Heuristic [8; 14]).

Step 5. Calculation T_{col} and T_{ot} [14], checking the restrictions Ω.

Step 6. If the data collection parameters of the resulting solution meet the requirements, then it's over, otherwise, proceed to the next step.

Step 7. Identification the network state, check if the rule base can be used (to improve the solution). If yes, then proceed to step 8, otherwise – the end.

Step 8. Search for a new solution for the flight path and data collection using a rule base to achieve the defined objective functions.

Step 9. Evaluation of data collection performance, checking the Ω constraints. Checking the quality of the solution in comparison with the basic (previous) one.

If the solution is better, then accept the decision (block 11), otherwise reject it (block 10).

Step 10. Check verification: all solution options have been considered (block 12). If so, then it's over, otherwise – go to step 5.

Fig. 7 shows an example of the application of the situational model of controlling the TA trajectory for data collection in a cluster compared to the basic TA trajectory with data collection in flight through the center of the cluster. The initial cluster C, obtained as a result of homogeneous clustering of the network for the implementation of a certain OF, is divided into seven heterogeneous clusters based on the analysis (identification) of the state of the nodes $\{c_1, \dots, c_7\}$.

Each of these clusters has its own strategy for flying over and collecting data (for example, with in-flight collection and hovering – for clusters c_1, c_3, c_5, c_6; for c_5 – flying over each critical node; for c_2 – during the flight not through the center, etc.).

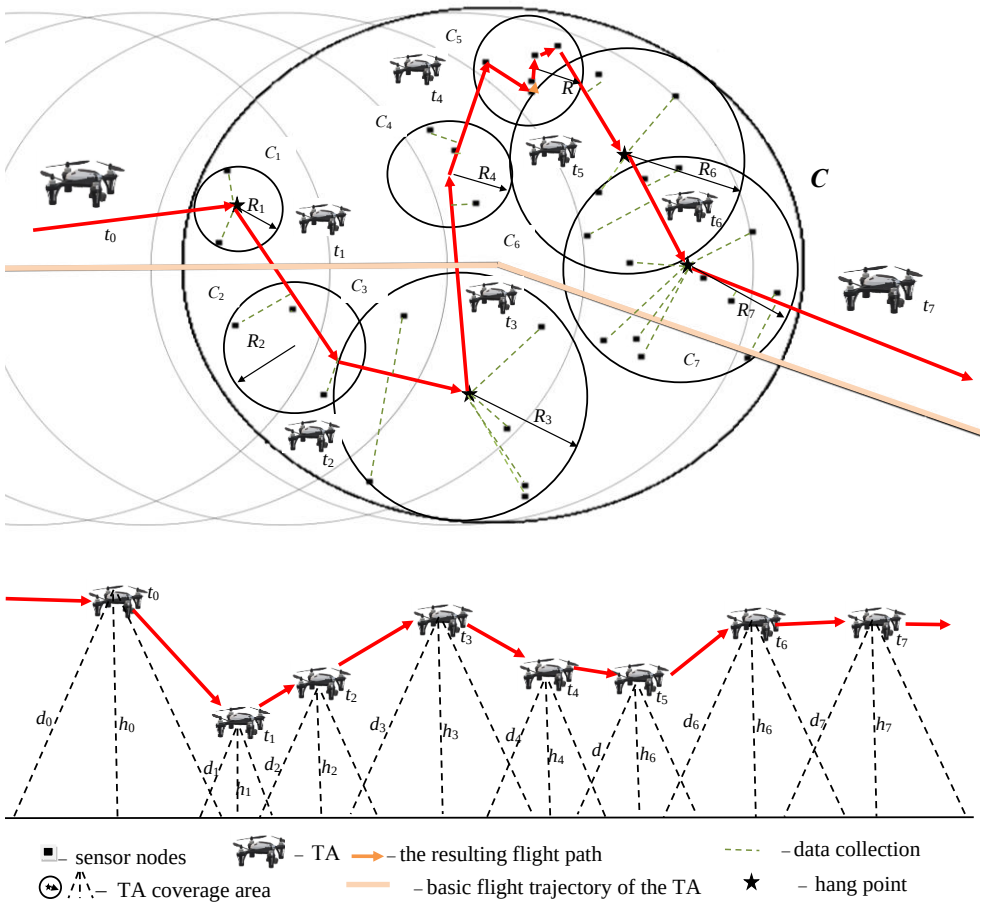


Fig. 7. Decision on the trajectory and points (intervals) of data collection by a telecommunications aerial platform using the situational management model

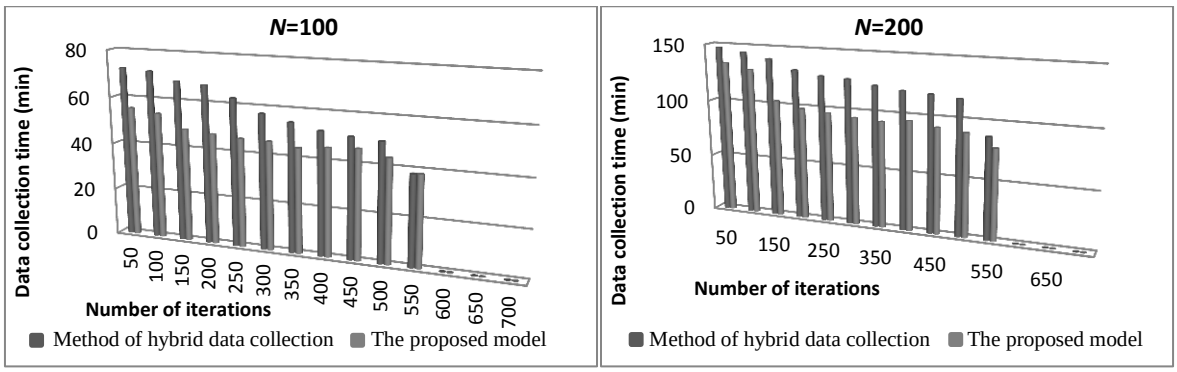
To evaluate the effectiveness of the proposed model, we developed a simulation program in C#. The input data for the simulation are the parameters of the network, nodes, TAs, algorithms and rules that implement the TA data collection process. Programmatically implemented:

– A network clustering algorithm and a model for determining collection points.
– An algorithm for finding the shortest route to fly around the CHIH network clusters.
– The decision-making process (according to the situational model and a certain rule base) on the flight path in clusters for data collection, etc.

The effectiveness of the proposed model was studied in comparison with the hybrid strategy of in-flight data collection through the cluster center [10] with different initial data: network dimension, number of clusters, number of nodes in a cluster, amount of monitoring data in nodes, etc. In the process of modeling, the energy consumption of nodes is calculated according to the cost model given in [14], and the data collection time is calculated.

Initial data for modeling: nodes are randomly placed on a plane of 6000×6000 m; number of nodes $N = 100, 200, 500$; $e_0 = 0.1\,J$, $d_{max} = 250$ m, $h = 50 \ldots 250$ m, $v = 0 \ldots 10$ m/s, MAC-protocol – IEEE 802.11g, V_{dmi}= 0.1…1 Mb, energy consumption for transmission bit, etc.

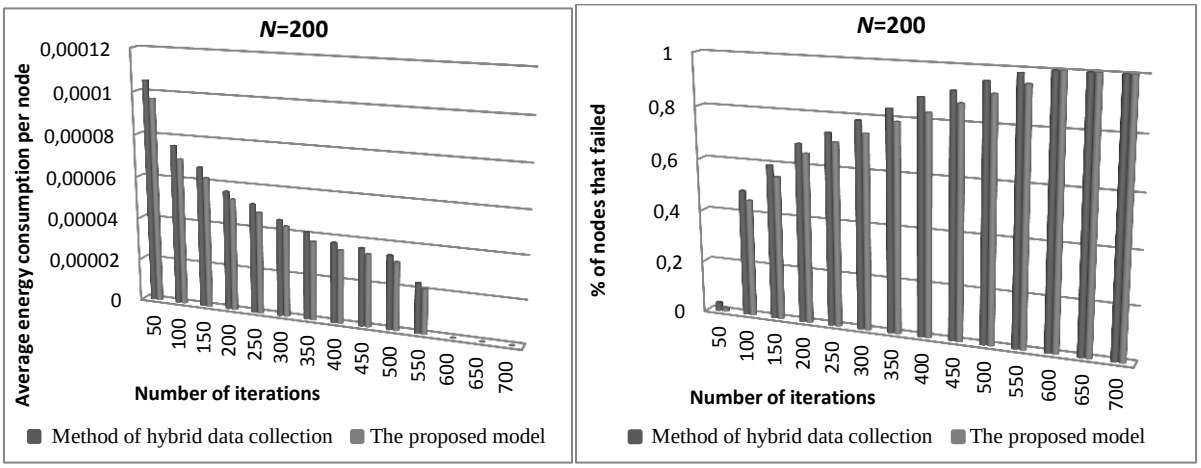
Fig. 8 shows the dependence of the data collection time T_{col} of the model in comparison with the hybrid method [10] at different numbers of nodes in the cluster $N = 100, 200$. The data collection time of the proposed model is 10–15 % less compared to the hybrid collection method [10].



a *b*

Fig. 8. T_{col} dependence at different number of network nodes:
$a - N = 100$; $b - N = 200$

Fig. 9 shows the dependence of the average node energy consumption and the percentage of failed nodes on the number of rounds of circling for a network with $N = 200$ nodes. The average energy consumption of nodes (Fig. 9*a*) in the proposed model is 10 % lower compared to [10], so the percentage of failed nodes (Fig. 9*b*) in the proposed model is lower, which correspondingly increases the network lifetime by 12–17 %.



a *b*

Fig. 9. Dependence of the energy costs and of the percentage of failed nodes on the number of flight rounds

The results of modeling the model of situational control of the flight path and data collection of the TA [13] in comparison with the hybrid method [10] showed that the time of data collection from the TA nodes is reduced by 10–15 % or the network operation time is increased by 12–17 % when certain restrictions are met. It is important to note that the proposed model can be used in special software of the data collection management system. The low computational complexity of the model allows its application in real time.

Conclusions. The developed model of situational control of the flight trajectory and data collection from nodes by a telecommunication aerial platform is implemented in the method of direct data collection by TA [14]. The novelty of the situational control model is the hierarchy of decision making: network, cluster, TA, node, considering the target control functions. At the network level, rules for determining the number and size of clusters are applied; a basic solution is built to determine the collection points and their flight paths. At the level of each cluster, during the flight, the TA adjusts the basic solution considering the parameters of the actual state of the cluster nodes. At the level of TA-node interaction, the node's energy consumption and data transmission rate are optimized by determining the node-TA distance. For each set of situations on the network, in the cluster, and on the node, a corresponding set of rules has been developed. Meta-rules are proposed to reduce the number of solution options. This approach allows us to achieve optimization

of the objective functions of the data collection process and ensure real-time decision-making. The results of simulation modeling of the situational management model have proven the possibility of reducing the data collection time by 10–15 % or increasing the network operation time by 12–17 % compared to existing solutions.

The direction of further research is the use of deep learning neural networks to develop appropriate control actions along the flight path to collect TA data from the WSNs.

REFERENCES

1. Dan Popescu, Florin Stoican, Grigore Stamatescu, Oana Chenaru, Loretta Ichim. (2019). A Survey of Collaborative UAV–WSN Systems for Efficient Monitoring Sensors. 19 (21), 4690; DOI: 10.3390/s19214690.

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.

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.

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.

5. Sarmad Rashedand Mujdat Soyturk. (2017). Analyzing the Effects of UAV Mobility Patterns on Data Collection in Wireless Sensor Networks Sensors. 17, 413. DOI: 10.3390/s17020413.

6. 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.

7. 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.

8. 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.

9. Kumar Nitesh and Prasanta K. Jana. (2018). Convex hull based trajectory design for mobile sink in wireless sensor networks. Published Online: December 19, pp. 26–36. DOI: 10.1504/IJAHUC.2019.097092.

10. 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.

11. Josiane da Costa Vieira Rezende, Ronellídio da Silva and Marcone Jamilson Freitas Souza. (2020). Gathering Big Data in Wireless Sensor Networks by Drone. Sensors, 20, 6954. DOI: 10.3390/s20236954.

12. Shams ur Rahman and You-Ze Cho. (2018). UAV positioning for throughput maximization. Journal on Wireless Communications and Networking. DOI: 10.1186/s13638-018-1038-0.

13. Nguyen, K. K., Duong, T. Q., Do-Duy, T., Claussen, H., & Hanzo, L. (2022). 3D UAV Trajectory and Data Collection Optimisation via Deep Reinforcement Learning. IEEE Transactions on Communications. DOI: 10.1109/TCOMM.2022.3148364

14. Hrymud A., Romaniuk V. (2022). Modifying a method for direct data collection by a telecommunication aerial platform from nodes of wireless sensor networks. Eastern-European Journal of Enterprise Technologies, 4 (9 (118)), pp. 15–29. DOI: 10.15587/1729-4061.2022.263559.

15. Vipin Pal, Girdhari Singh, Rajender Prasad Yadav (2012). SCHS: Smart Cluster Head Selection Scheme for Clustering Algorithms in Wireless Sensor Networks. Wireless Sensor Network, 4, 273–280. http://dx.doi.org/10.4236/wsn.2012.411039.

DOI: 10.58254/viti.3.2023.12.101

УДК 621.396.6

канд. техн. наук Сакович Л. М. ORCID: 0000-0002-8257-7086 (ІСЗЗІ НТУУ «КПІ»)
канд. техн. наук Єлісов Ю. М. ORCID: 0009-0007-4441-0721 (НДІ ВР)
Мороз М. В. ORCID: 0009-0007-9455-3886 (НДІ ВР)

РОЗРОБКА ДІАГНОСТИЧНИХ ПРОГРАМ ДЛЯ ПОТОЧНОГО РЕМОНТУ ТЕХНІЧНИХ ЗАСОБІВ РОЗВІДКИ

Технічні засоби розвідки широко використовуються в усіх сферах розвідувальної діяльності. Їхня елементна база і схемні рішення безперервно удосконалюються в напрямку автоматизації виконання технологічних операцій. Це призводить до збільшення кількості елементів у виробі, що зі свого боку не сприяє підвищенню показників надійності. Тому питання відновлення працездатності при відмовах технічних засобів розвідки досить актуальні, оскільки час технічного діагностування займає до 80 відсотків часу ремонту. Автори багато років працюють в галузі технічної діагностики складних об'єктів і систем, які відрізняються за призначенням, схемною і конструктивною побудовою та вимогами до часу відновлення. При цьому важливо розробити якісне діагностичне забезпечення ремонту із врахуванням особливостей конкретного об'єкта діагностування, а також умов відновлення працездатності.

В окремих джерелах розглянуто використання деяких особливостей об'єкта діагностування під час розробки їхнього діагностичного забезпечення, але загальний підхід до цього відсутній. Тому в статті запропоновано використання всіх особливостей об'єкта діагностування для підвищення якості їхнього діагностичного забезпечення. Це дозволяє з мінімальними витратами забезпечити необхідну якість відновлення працездатності об'єкта діагностування. Запропоновані пропозиції доцільно використовувати під час удосконалення існуючого діагностичного забезпечення і його розробки для перспективних технічних засобів розвідки.

У подальшому автори планують виконати дослідження в напрямку підвищення ефективності діагностування дискретних об'єктів, а також з аварійними та бойовими пошкодженнями при наявності кратних дефектів.

Ключові слова: *технічні засоби розвідки, технічне діагностування, діагностичне забезпечення, метрологічне забезпечення.*

L. Sakovich, Y. Yelisov, M. Moroz Development of diagnostic programs for current repair of intelligence equipment.

Technical means of intelligence (hereinafter – TMI) are widely used in all spheres of intelligence activity. Their element base and schematic solutions are continuously improved in the direction of automating the execution of technological operations. This leads to an increase in the number of elements in the product, which in turn does not contribute increasing reliability indicators. Therefore, the issue of restoring performance in the event of failures of TMI is quite relevant, since the time of technical diagnosis takes up to 80 percent of the repair time.

The authors have been working for many years in the field of technical diagnostics of complex objects and systems, which differ in purpose, schematic and constructive construction, and requirements for recovery time. At the same time, it is important to develop high-quality diagnostic support for repairs, taking into account the specifics of the specific object of diagnosis, as well as the conditions for restoring performance.Some sources consider the use of some features of the object of diagnosis during the development of their diagnostic support, but there is no general approach to this. Therefore, the article proposes the use of all features of the object of diagnosis to improve the quality of their diagnostic support.

This makes it possible to ensure the necessary quality of restoration of the functionality of the object of diagnosis with minimal costs. It is advisable to use the proposed proposals during the improvement of the existing diagnostic support and its development for promising technical means of intelligence.In the future, the authors plan to conduct research in the direction of increasing the efficiency of diagnosing discrete objects, as well as with accident and combat damage in the presence of multiple defects.

Keywords: *technical means of intelligence, technical diagnostics, diagnostic support, metrological support.*

Постановка завдання. Сучасні технічні засоби розвідки (далі – ТЗР) широко використовуються в усіх сферах розвідувальної діяльності. Елементна база ТЗР і схемні рішення безперервно удосконалюються в напрямку автоматизації виконання технологічних операцій. Це призводить до збільшення кількості елементів у виробі, що зі свого боку не сприяє підвищенню показників надійності. Тому питання відновлення працездатності при відмовах ТЗР є досить актуальним, так як час технічного діагностування займає до 80 відсотків часу ремонту.

Автори вважають що необхідно вирішити наступну наукову задачу, а саме здійснити аналіз сучасних досягнень в галузі технічної діагностики і метрології, встановити їхні можливості щодо підвищення якості діагностичного забезпечення (далі – ДЗ) перспективних та існуючих ТЗР. У світі накопичено великий досвід в галузі технічної діагностики складних об’єктів і систем, які відрізняються за призначенням, схемною і конструктивною побудовою та вимогами до часу відновлення [1–5]. При цьому важливо розробити якісне ДЗ ремонту із врахуванням особливостей конкретного об’єкта діагностування (далі – ОД), а також умов відновлення працездатності. В окремих джерелах розглянуто використання деяких особливостей ОД під час розробки їхнього ДЗ, але загальний науковий підхід до цього відсутній. У статті запропоновано аналіз та наукове обґрунтовування щодо використання всіх особливостей ОД та підвищення якості їхнього ДЗ. Це дозволить забезпечити необхідну якість відновлення працездатності ОД з мінімальними витратами. Запропоновані пропозиції доцільно використовувати під час удосконалення існуючого ДЗ та при його розробці для перспективних ТЗР.

Аналіз останніх досліджень і публікацій. Сучасні дослідження в галузі технічної діагностики ТЗР направлені на підвищення достовірності оцінки їхнього технічного стану, скорочення середнього часу відновлення, мінімального відхилення діагнозу від істинного при помилці фахівця в оцінці результату виконання перевірки. Це досягається без додаткових витрат на створення ДЗ і тільки завдяки використанню особливостей побудови ТЗР та впровадженню в практику розробки ДЗ сучасних досягнень технічної діагностики.

У зарубіжних роботах [1; 2] для підвищення комплексного показника надійності, а саме «коефіцієнта готовності», основну увагу приділяють не скороченню часу відновлення, а збільшенню значення показника напрацювання на відмову. Цей підхід доцільно використовувати для ТЗР загального призначення, але неможливо для техніки силових структур, яка може під час їхньої експлуатації отримувати аварійні або бойові пошкодження.

Залежно від типу ТЗР (аналогові або дискретні) під час відновлення працездатності використовують функціональне або тестове діагностування з використанням відповідних моделей ОД [3; 4]. При цьому сучасні ТЗР відносяться до програмно керованих об’єктів, що також впливає на процес діагностування: він може бути непрацездатним як при відмові апаратурної частини, так і при наявності помилок програмного забезпечення [5; 6].

Окремо розглянуто особливості розробки ДЗ ТЗР із аварійними або бойовими пошкодженнями при наявності кратних дефектів [7], а також багато вихідних ОД, до яких відносяться підсистеми електроживлення ТЗР [8; 9].

Відновлення ТЗР великої розмірності з рознесеними в просторі елементами виконують бригади фахівців. При цьому використовують груповий пошук дефектів, що суттєво скорочує середній час відновлення працездатності [10; 11].

Останнім часом при розробці ДЗ сучасних ТЗР особливу увагу приділяють якості метрологічного забезпечення [12; 13] і врахуванню можливості помилки фахівця в оцінці результату виконання перевірки при роботі у важких польових умовах та стресовій ситуації [4; 14]. При цьому важливо, щоб при реалізації ремонту ТЗР агрегатним методом навіть при помилці фахівця в оцінці результату виконання перевірки несправний елемент знаходився в середині конструктивної частини виробу, яка підлягає заміні.

При усуненні кратних дефектів внаслідок аварійних або бойових пошкоджень ТЗР виникає задача раціонального розподілу зусиль між етапами дефектації з метою визначення ступеня пошкодження і діагностування, яка отримала рішення в [15; 16].

Проведений аналіз показав, що у відомих публікаціях автори досліджували окремі питання розробки ДЗ сучасних ТЗР, причому не завжди враховуючи отримані раніше результати. Таким чином виникає наукове завдання дослідження можливості підвищення ефективності ДЗ існуючих і перспективних ТЗР різноманітного призначення шляхом об’єднання і комплексного використання відомих результатів.

Метою статті є розробка загального алгоритму створення ДЗ сучасних ТЗР з врахуванням відомих, отриманих раніше часткових результатів, удосконалення цього

процесу для досягнення максимального ефекту скорочення середнього часу відновлення при будь-якому ступені пошкодження об'єкта і залежно від його розмірності при роботі одного або бригади фахівців.

Виклад основного матеріалу. Сформульована авторами наукова задача щодо розробки діагностичних програм для підвищення ефективності поточного ремонту ТЗР вирішується поетапно відповідно до наступних кроків.

1. Отримання й аналіз вихідних даних:

$T_{\text{ВП}}$ – максимально припустимий час відновлення ТЗР;

S – ступінь пошкодження (визначається під час дефектації);

μ – кількість фахівців;

t – середній час виконання перевірки;

t_Y – середній час усунення несправностей;

відомості про метрологічне забезпечення:

n – кількість засобів вимірювальної техніки (ЗВТ), які використовуються при ремонті ТЗР;

p_i – ймовірність правильної оцінки результату виконання перевірки ЗВТ виду $i = \overline{1,n}$;

$P_i(\tau)$ – ймовірність відсутності метрологічних відмов ЗВТ виду $i = \overline{1,n}$ за період між плановими перевірками τ.

2. Формування цільової функції і показника якості системи ремонту.

До цільової функції висуваються такі вимоги: однозначність (наявність екстремуму), відповідність реальному процесу, запис через параметри керування, розробка до головного показника системи і відсутність розривів. При цьому частина аргументів виноситься у вигляді обмежень (ймовірність рішення задачі за встановлений час, вартість, показники надійності не гірше необхідних й інші).

Для системи ремонту ТЗР цільова функція полягає в мінімізації розрахункового часу відновлення:

$$T_{\text{ВР}} \le T_{\text{ВП}};\ T_{\text{ВР}}(X) = \min T_{\text{ВР}}\,(X*);\ X* \in \Delta,$$

де X – параметри системи ремонту;

X* – значення при вирішенні завдання;

Δ – область припустимих значень зміни параметрів.

Параметри системи ділять на керовані (наприклад, алгоритми діагностування) і некеровані, які неможливо змінити (наприклад, кількість фахівців ремонту і їхня кваліфікація). Якщо основних параметрів декілька (наприклад, час і вартість) й цільова функція є системою рівнянь або нерівностей, то у цьому випадку доцільно знаходити не оптимальне за кожним критерієм, а компромісне раціональне рішення в сенсі Парето. У простому випадку це двомірна модель, але можливо і більше оцінюючих показників (наприклад, час, вартість, надійність).

Математична формалізація завдання у вигляді цільової функції дозволяє кількісно оцінити ефект від її рішення у вигляді показника ефективності. Як правило, він відображається не в абсолютних, а у відносних одиницях (відсотках). У такому разі для системи ремонту ТЗР показник ефективності характеризує відносне зменшення середнього часу відновлення в модернізованій системі ремонту відносно до існуючої або до припустимого:

$$0 \le \frac{T_{\text{ВП}} - T_{\text{ВР}}}{T_{\text{ВП}}} \le 1; \qquad \eta = \frac{T_{\text{ВП}} - T_{\text{ВР}}}{T_{\text{ВП}}} 100\%.$$

Далі обґрунтовується адекватний математичний апарат і розробляється структура рішення завдання отримання цільової функції у явному вигляді, враховуючи особливості ОД, початкових даних, обмежень і припущень функціонування ремонтного органу (рис. 1).

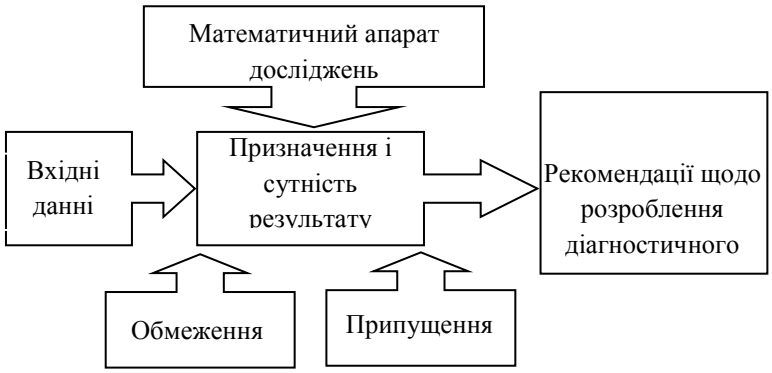


Рис. 1. Структура процесу розроблення ДЗ сучасних ТЗР

3. Аналіз ОД й обґрунтування вибору його моделі.

Залежно від схемної та конструктивної побудови ТЗР, вони мають окремі види надлишковості чи їх сукупності, що дозволяє підвищити достовірність визначення технічного стану (рис. 2).

Рис. 2. Використання видів надлишковості ТЗР
для підвищення достовірності результатів їхнього діагностування

Порівняльний аналіз варіантів підвищення достовірності діагностування ТЗР за рахунок використання їхньої надлишковості наведено в таблиці 1.

Таблиця 1

Порівняльний аналіз варіантів підвищення
достовірності діагностування ТЗР з використанням їхньої надлишковості

Варіант	Переваги	Недоліки
Конструктивний	– реалізація ремонту агрегатним методом; – використання процедур пробних заміщень; – зменшення часу діагностування	– застосування тільки для об’єктів модульної конструкції; – збільшення обсягу і вартості ЗІП
Часовий	– простота реалізації; – відсутність матеріальних витрат;	– збільшення часу діагностування;
Структурний	– зменшення кількості внутрішніх перевірок; – розрізнення незалежних кратних дефектів; – застосування неоднорідних алгоритмів пошуку	– застосування тільки для об’єктів з дивергуючими структурами; – можливість помилкових діагнозів при наявності кратних дефектів
Функціональний	– використання методу переключень; – скорочення простору пошуку; – граф-схемне зображення алгоритмів пошуку	– застосування тільки для багаторежимних і багатофункціональних об’єктів
Інформаційний	– можливість виявлення і усунення несправностей частини датчиків; – локалізація кратних дефектів; – зменшення часу діагностування, застосування неоднорідних алгоритмів і групового пошуку дефектів	– ускладнення апаратурної реалізації засобів діагностування; – необхідність додаткової підготовки фахівців і використання дорогих ЗВТ

Під ОД розуміють виріб або його складові частини, технічний стан яких підлягає визначенню. За характером перетворення енергії і інформації ОД поділяють на безперервні (аналогові) і дискретні (цифрові). Формальний опис ОД, який враховує можливість зміни його стану в часі, називається діагностичною моделлю, яка має властивості виявлення і розрізнення дефектів. ТЗР як ОД і моделювання мають функціональну різноманітність, ієрархічну конструкцію і відрізняються складністю завдань, які виконуються, високою автономністю і вартістю наслідків відмов, що дозволяє віднести їх до категорії складних технічних систем, які представляються основними групами діагностичних моделей:

1. Безперервні моделі, які представляють об’єкт і процеси, що в ньому протікають в безперервно змінюваному часі.
2. Дискретні моделі, які визначають стан ОД для послідовності дискретних значень часу.
3. Гібридні моделі, які описують реальні моделі, що складаються з пристроїв безперервної дії і дискретних пристроїв.
4. Спеціальні моделі, які враховують особливості ДЗ і функціонування об’єкта.

За видами представлення взаємозв’язків між станами ОД, його елементами і параметрами вихідних сигналів методи синтезу моделей поділяються на аналітичні, графоаналітичні, функціонально-логічні й інформаційні.

Узагальнена класифікація моделей ОД приведена на рисунку 3.

Словесні або описові моделі є найпростішими, але досить широко використовуються не тільки в технічній, але й в медичній діагностиці. До них відносяться симптоми стану ОД і таблиці типових несправностей. Подібні моделі використовуються при підготовці ремонтного персоналу в процесі ремонту складної побутової радіоелектронної апаратури спеціалістами низької кваліфікації.

Графічні моделі володіють наочністю, відображають логіку взаємодії елементів об’єкта, проходження енергії й інформації. Використовуються для розробки алгоритмів діагностування, які розрізняють дефекти типу обрив і перевантаження. Подібні моделі мають обмеження: елементи можуть мати будь-яке число входів, але тільки один вихід.

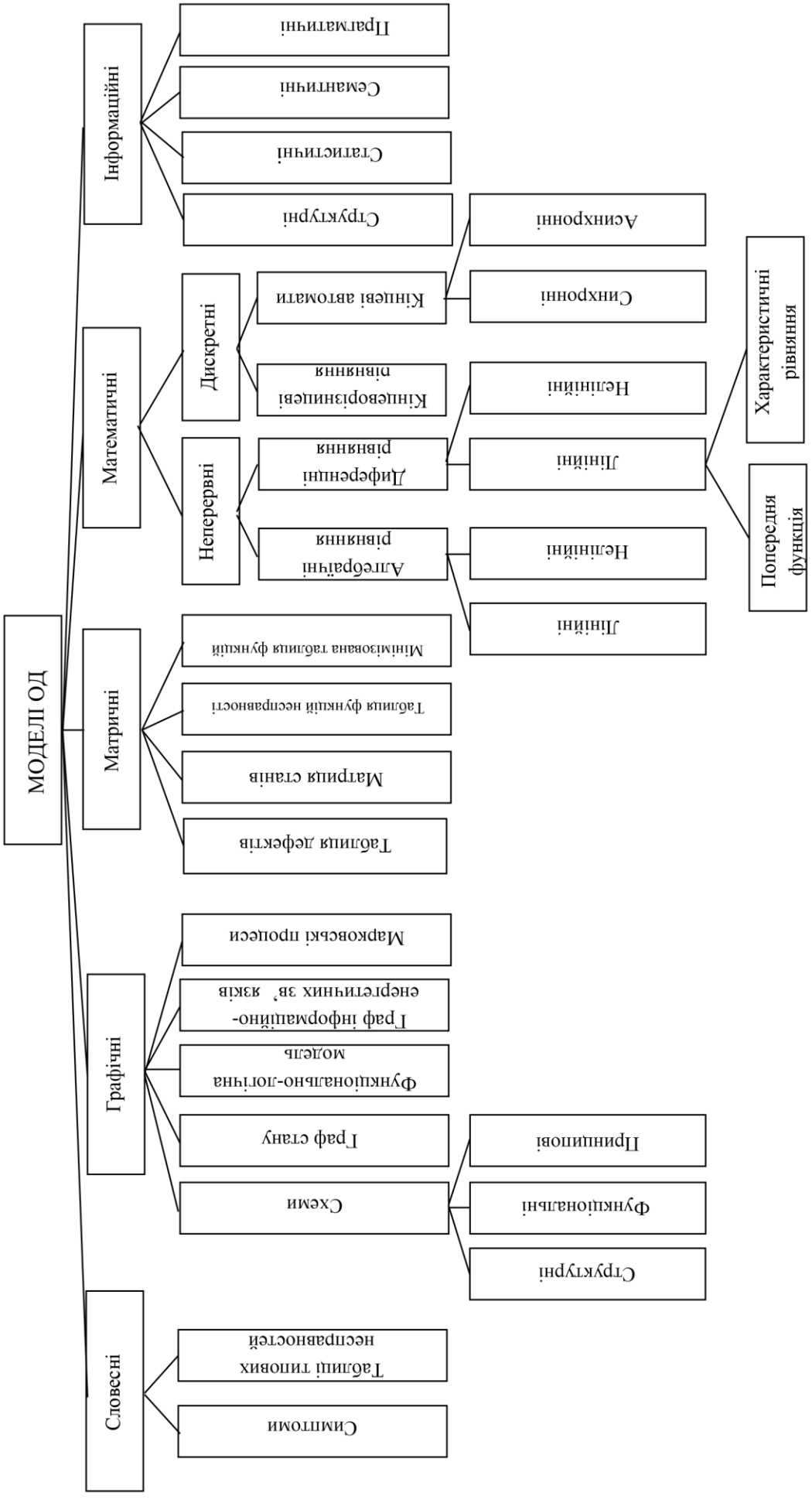


Рис. 3. Узагальнена класифікація моделей ОД

Матричні моделі зручні для обробки за допомогою ЕОМ і не вимагають від користувача високої кваліфікації при підготовці вихідних даних. На їхній базі можливий синтез як умовних, так і безумовних алгоритмів діагностування. Ці моделі мають обмеження на ступінь пошкодження об’єкта: при наявності кратних дефектів можливе встановлення неправильного діагнозу. Вони можуть подаватись у формі таблиці дефектів, матриці станів, таблиці функцій несправностей (далі – ТФН) або мінімізованої ТФН і широко використовуються при розробці засобів технічного діагностування (далі – ЗТД).

Математичні та інформаційні моделі використовуються переважно при проєктуванні засобів і систем технічного проєктування (далі – СТД) складних об’єктів на базі ЕОМ. Так, наприклад, застосування моделей у вигляді диз’юнктивно-нормальної форми (далі – ДНФ) або мінімальної ДНФ на мові алгебри логіки при синтезі ЗТД знімає обмеження на кратність дефектів в об’єкті і на число виходів його елементів.

Аналіз моделей ОД показує їх взаємозв’язок і можливість перетворення з одного виду в інший залежно від завдань, що виконуються (розробка алгоритмів або засобів діагностування), та кваліфікації користувача.

Залежно від використання процедур діагностування, які встановлюють послідовність та зміст дій оператора, розрізняють тестове і функціональне діагностування. Процедури зовнішнього огляду, проміжних вимірювань і пробних заміщень є універсальними. При тестовому діагностуванні використовується аналіз деформації сигналу, послідовна або комбінаторна процедури. При функціональному діагностуванні об’єктів з кратними дефектами застосовуються специфічні скорочені процедури пошуку.

Узагальнення сучасних досягнень в галузі технічної діагностики і метрології дозволяє обґрунтувати алгоритм розробки ДЗ ТЗР (рис. 4).

Під час аналізу вихідних даних з керівних документів визначають значення $T_{\text{ВП}}$. Також отримують опис схемної і конструктивної побудови. Із аналізу можливих умов ремонту визначають кількість μ і кваліфікацію фахівців, що впливає на значення t і t_y. Також важливо отримати відомості щодо метрологічного забезпечення: тип і кількість ЗВТ, їхні показники, що впливають на час ремонту ($p\ P(\tau)$).

За цільову функцію приймається досягнення мінімального часу відновлення в заданих умовах роботи ремонтного органу, а показник ефективності кількісно оцінює відносне зменшення розрахункового часу відновлення, порівняно з максимально допустимим згідно із завданням.

Важливо якісно виконати аналіз ОД. Насамперед, схемну і конструктивну побудову: визначити ділянки, які охоплюють вбудовані засоби діагностування, щоб пізніше використовувати їх при розробці ДЗ поточного ремонту. Аналіз конструкції дозволяє визначити глибину пошуку дефектів L і вид ремонту (агрегатний чи детальний). Властивості багаторежимності і багатофункціональності, а також наявність окремих видів надлишковості, також підвищують ефективність ДЗ. Важливо враховувати можливий ступінь пошкодження ОД для визначення виду ремонту: поточний (наявність одного дефекту) або усунення аварійних і бойових пошкоджень (наявність кратних дефектів). При цьому доцільно оптимально розподілити час дефектації і діагностування для мінімізації значення $T_{\text{ВР}}$.

Враховуючи вимоги до ДЗ, визначають критерії оптимізації алгоритму діагностування: мінімум часу відновлення або вартості ремонту при заданих обмеженнях. Далі обирають вид та форму алгоритму пошуку дефектів. Перевагу мають умовні алгоритми мінімальної форми. При наявності тільки функціональної схеми виробу використовують граф інформаційно-енергетичних зв’язків як діагностичну модель і побудову алгоритму діагностування виконують методом половинного ділення за допомогою індексів передування. За наявності додаткових даних щодо часу і вартості виконання окремих перевірок, показників надійності елементів на обраній глибині пошуку доцільно використовувати ймовірність переважного вибору перевірок, що також скорочує значення

Для отриманого алгоритму пошуку дефектів кількісно оцінюють його показники якості: середню кількість перевірок для локалізації несправного елемента, ймовірність правильної постановки діагнозу, метрологічну надійність ЗВТ, відхилення діагнозу від

істинного значення при помилці фахівця в оцінці результату виконання перевірки, розрахункове значення середнього часу відновлення й ефект від впровадження ДЗ в практику ремонту ТЗР.

Якщо $T_{ВР} > T_{ВП}$, то необхідно замінити алгоритм діагностування на більш ефективний або замінити вихідні дані щодо кваліфікації фахівців, умов ремонту, якості метрологічного забезпечення. А при $T_{ВР} \leq T_{ВП}$ отриманий алгоритм використовують для розробки діагностичної програми.

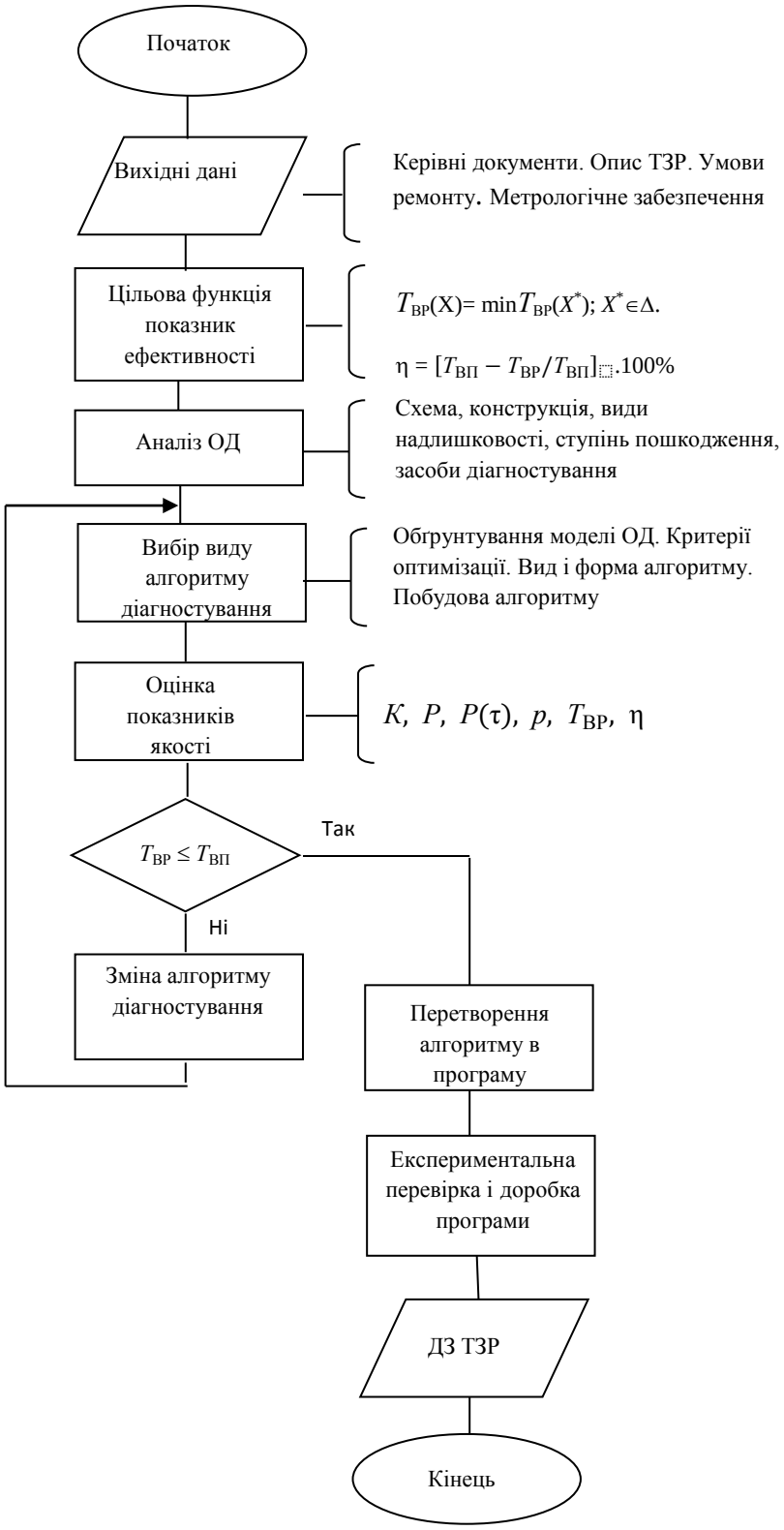


Рис. 4. Загальний алгоритм розроблення ДЗ ТЗР

Якщо при експериментальній перевірці програми виникають суперечності, які потребують пояснення, тоді здійснюють її доопрацювання. Таким чином отримують ДЗ ТЗР, яке відповідає вимогам.

Під час розроблення ДЗ використовують відомі рекомендації, приведені в [3; 6–11; 14], щодо оптимізації форми алгоритму діагностування із врахуванням особливостей ОД і кількісної оцінки його показників якості.

Висновки. Проведено аналіз сучасних досягнень в галузі технічної діагностики і метрології, встановлено їхню можливість для підвищення якості ДЗ перспективних та існуючих ТЗР.

Запропоновано загальний алгоритм розроблення ДЗ радіоелектронних засобів з врахуванням особливостей їхньої побудови, умов ремонту, метрологічного забезпечення для мінімізації середнього часу відновлення.

Подальші дослідження доцільно виконати в напрямку підвищення ефективності діагностування дискретних об’єктів, а також з аварійними та бойовими пошкодженнями при наявності кратних дефектів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kharchenko V. A. (2015), Problems of reliability of electronic components‖, Modern Electronic Materials, Volume 1, Issne 3, pp. 88–92. DOI: http://dx.doi.org/10.1016/j.moem.2016.03.002.

2. Yi Wan, Hailong Huang, Diganta Das, Michael Pecht (2016). Thermal reliability prediction and analysis for high-density electronic systems based on the Markov process‖, Microelectronics Reliability, Volume 56, pp. 182–188. DOI: http://doi.org/10.1016/j.microrel.2015.10.006.

3. Ксенз С. П. Диагностика і ремонтопригодность радиоэлектронных средств. М.: Радио и связь, 1989. 248 с.

4. Ксенз С. П., Полтаржицький М. И., Алексеев С. П., Минеев В. В. Борьба с диагностическими ошибками при техническом обслуживании и ремонте систем управления связи и навигации. СПб.: ВАС, 2010. 240 с.

5. Бобало Ю. Я. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем / Ю. Я. Бобало, Б. Ю. Волочій, О. Ю. Лозинський, Б. А. Манздій, Л. Д. Озірківський, Д. В. Федасюк, С. В. Щербаковських, В. С. Яковина. Львів: Львівська політехніка, 2013. 300 с.

6. Гнатюк С. Є. Кількісна оцінка надійності програмно керованих засобів зв’язку / С. Є. Гнатюк, Л. М. Сакович, Є. В. Рижов // Information Technology Security. 2016. Том. 4. № 1. С. 84–90.

7. Сакович Л. Н., Рижаков В. А. Оптимизация формы алгоритмов диагностирования средств связи с кратными дефектами // Зв’язок. 2002. № 5. С. 33–34.

8. Сакович Л. М. Діагностичне забезпечення підсистем електроживлення засобів спеціального зв’язку / Л. М. Сакович, Я. Ю. Богдан // Спеціальні телекомунікаційні системи та захист інформації. 2018. № 2 (4). С. 69–73.

9. Сакович Л. М. Дослідження умовних алгоритмів діагностування багатовивідних об’єктів / Л. М. Сакович, О. В. Ходич, Ю. В. Мирошніченко // Спеціальні телекомунікаційні системи та захист інформації. 2021. Вип. 1 (8). С. 13–21.

10. Романенко В. П. Сакович Л. М. Методика розробки діагностичного забезпечення групового пошуку дефектів при ремонті техніки зв’язку в польових умовах // Зв’язок. 2015. № 2. С. 53–56.

11. Рижов Є. В. Сакович Л. М. Дослідження показників якості групового пошуку дефектів під час поточного ремонту військової техніки зв’язку // Збірник наукових праць військової академії. 2017. № 2 (28). С. 82–88.

12. Основи експлуатації засобів вимірювальної техніки військового призначення в умовах проведення АТО / В. Б. Кононов, О. В. Водолажко, О. В. Коваль та ін. Х.: ХНУПС, 2017. 288 с.

13. Dependence of parameters of repair of military communication means on the quality of metrological support / V. Kononov, Ye. Ryzhov, L. Sakovych // Advanced Information Systems. Vol. 2, № 1. Pp. 91–95. DOI: https://doi.org/10.20998/2522-9052.2018.1.17.

14. Ryzhov Ye. Minimization measurement requirements for maintenance and repair special communication means / Ye. Ryzhov, L. Sakovych // Institute of Special communication and Information Protection National Technical University of Ukraine – Igor Sikorsku Kyiv Politechnic Institute – Scientific Works – Information Technology and Security. 2017. Vol. 5, Iss. 1 (8). Pp.106–114.

15. Павлов В. П., Сакович Л. М. Синтез алгоритму дефекації техніки зв’язку з аварійними пошкодженнями // Зв’язок. 2007. № 6. С. 54–55.

16. L. Sakovych. Metod of time distribution for repair of radio electronic means with multiple defects / L. Sakovych, Ye. Ryzhov, A. Sobolev // Військово-технічний збірник НАСВ. 2019. № 21. С. 72–77. DOI: https://doi.org/10.33577/2312-4458.21.2019/72-77.

DOI: 10.58254/viti.3.2023.13.110

УДК 621.396.6

канд. техн. наук Сакович Л. М. ORCID: 0000-0002-8257-7086 (ІСЗЗІ НТУУ «КПІ»)
канд. військ. наук Слюсарчук О. О. ORCID: 0000-0002-9954-9129 (НДІ ВР)
Слюсар П. П. ORCID: 0009-0007-3738-2523 (НДІ ВР)

АЛГОРИТМ РЕАЛІЗАЦІЇ МЕТОДУ ОБҐРУНТУВАННЯ МІНІМАЛЬНО НЕОБХІДНОЇ КІЛЬКОСТІ ПАРАМЕТРІВ ТЕХНІЧНИХ ЗАСОБІВ РОЗВІДКИ ДЛЯ МОНІТОРИНГУ ЇХНЬОГО ТЕХНІЧНОГО СТАНУ

У статті вперше запропоновано рішення однієї із задач технічної діагностики – мінімізації кількості параметрів для постійного контроля їхніх значень під час експлуатації технічних засобів розвідки. До таких об'єктів відносяться системи спеціального радіозв'язку, радіоелектронної розвідки та багато інших. Їхнє функціонування об'єктивно оцінюється сукупністю параметрів, постійно контролювати значення яких недоцільно внаслідок значної вартості та надлишковості, а також наявності взаємозалежних параметрів в системі. Тому виникає завдання визначення їх мінімально припустимої кількості за обґрунтованим критерієм, що об'єктивно оцінює готовність системи до виконання необхідних функцій. Рішення задачі залежить від важливості параметрів для користувача системи, об'єму частини комплексу, що перевіряється, вартості вбудованих засобів контролю та інших показників якості, які об'єднуються комплексним показником. Його значення нормується ймовірністю переважного вибору параметра для моніторингу технічного стану виробу. Ранжування параметрів за цим показником дозволяє обґрунтовувати їх мінімально необхідну кількість для моніторингу при забезпеченні заздалегідь заданого значення показника якості контролю.

У статті запропонована схема, математичний апарат і алгоритм реалізації методу обґрунтування мінімально необхідної кількості параметрів для моніторингу стану технічних засобів розвідки. Отримані результати із використанням інформаційних технологій дають можливість прогнозування технічного стану об'єкта контроля для підтримання необхідних значень показників надійності. Подальші дослідження доцільно направити на використання отриманих результатів для прогнозування технічного стану засобів на основі сучасних інформаційних технологій, що дозволить оптимізувати періоди ТО і планових ремонтів за критерієм мінімуму вартості при збереженні необхідних значень показників надійності.

Ключові слова: *технічні засоби розвідки, моніторинг параметрів, технічний стан, ймовірність переважного вибору.*

L. Sakovich, O. Slyusarchuk, P. Slyusar Algorithm for implementation of the method of justification of the minimum necessary number of parameters of technical means of intelligence for monitoring their technical condition.

In the article the solution to one of the problems of technical diagnostics is offered for the first time — minimizing the number of parameters for constant monitoring of their values during the operation of technical means of intelligence. They include systems of special radio communication, signal intelligence and many others. Their functioning is objectively evaluated by a set of parameters, the values of which are impractical to constantly monitor due to significant cost and redundancy as well as the presence of interdependent parameters in the system. Therefore, there is a task of determining their minimum acceptable number according to a well-founded criterion that objectively assesses the readiness of the system to perform the necessary functions. The solution to the problem depends on the importance of the parameters for the system user, the volume of the inspected part of the complex, the cost of built-in controls and other quality indicators, which are combined by a complex indicator. Its value is normalized by the probability of the preferred choice of the parameter for monitoring the technical condition of the product. The ranking of parameters according to this indicator allows you to justify their minimum necessary number for monitoring while ensuring the predetermined value of the control quality indicator.

The article proposes a scheme, a mathematical apparatus and an algorithm for the implementation of the method of substantiating the minimum necessary number of parameters for condition monitoring. The obtained results with the use of information technologies make it possible to predict the technical condition of the control object in order to maintain the required values of reliability indicators.

Keywords: *technical means of intelligence, parameter monitoring, technical condition, probability of the preferred choice.*

Постановка проблеми. Кількісна оцінка функціонування технічних засобів розвідки (далі – ТЗР) можлива тільки завдяки моніторингу оптимальної сукупності технічних параметрів. Як правило, це завдання вирішує особовий склад чергових змін. Але внаслідок впливу суб'єктивного фактора можлива неадекватна оцінка технічного стану (далі – ТС)

об'єктів, як військових, так і цивільних (наприклад, аварії на об'єктах критичної інфраструктури [1; 2].

Відомо, що наразі безперервно розвиваються теорія експлуатації складних технічних систем, технічна діагностика їхнього обладнання, метрологічне забезпечення та оцінка надійності всіх компонент [3; 4]. Питання моніторингу параметрів ТЗР внаслідок їх старіння і багаторічної експлуатації залишається важливим та досить актуальним. Тому наразі є актуальним вирішення наукового завдання обґрунтування мінімально необхідної кількості параметрів ТЗР, достатніх для якісного моніторингу їхнього ТС.

Аналіз останніх досліджень та публікацій. Найбільш досліджені питання контролю параметрів ТЗР під час їх технічного обслуговування (далі –ТО) і поточного ремонту [3; 5; 6], тобто не постійно, а періодично. Це дозволяє оцінити ТС тільки під час ТО або діагностування ТЗР, але не в період між ними. Останнім часом у зв'язку зі скрутним економічним становищем виникає необхідність ТО за станом, коли перевіряють мінімально необхідну кількість параметрів ТЗР, а перелік робіт залежить від результатів їхнього контролю [5–7].

Тобто, відомі результати неможливо використовувати для рішення завдання постійного моніторингу параметрів ТЗР критичної інфраструктури. Тому виникає наукова задача щодо обґрунтування мінімально необхідної кількості параметрів ТЗР для якісного моніторингу їхнього ТС, яка і вирішується у цій статті.

Мета статті – розробка алгоритму обґрунтування мінімально необхідної кількості параметрів для постійного контролю їхніх значень з метою визначення ТС ТЗР із заданою високою ймовірністю отримання достовірної оцінки ТС ТЗР.

Виклад основного матеріалу. На рис. 1 наведена схема реалізації методу обґрунтування мінімально необхідної кількості параметрів ТЗР для моніторингу і оцінки їхнього ТС із заданою ймовірністю [4]. Послідовність ранжування всієї сукупності параметрів необхідних для оцінки ТС ТЗР визначається тим, що обов'язково необхідно контролювати значення найбільш важливих параметрів, необхідних для функціонування ТЗР із врахуванням надійності елементів, що впливають на їхні значення, а також надійності і вартості вбудованої системи контролю (бінарних перетворювачів – нормалізаторів значень параметрів).

Залежно від призначення та умов використання внаслідок експертного опитування провідних фахівців в цій галузі визначають вагові коефіцієнти важливості кожного параметра для користувача k_i, надійності сукупності елементів, що впливають на значення параметра n_i, вартості v_i та надійності w_i вбудованої системи контролю параметрів, причому'

$$k_i + n_i + v_i + w_i = 1;\ i = \overline{1N},$$

де i – змінний параметр ТЗР;

N – загальна кількість параметрів ТЗР.

Надійність сукупності елементів і системи контролю оцінюють середнім значенням наробітку на відмову T_i, яку отримують за результатами випробувань або розрахунком параметра потоку відмов Z_i, за відомими методиками [7]. Вартість засобів контролю стану кожного параметра оцінюють реальними витратами на їх створення.

$$u_i = \frac{k_i T_{РЕК} T_{ВЗК} F_{ВЗК}}{n_i T_{ei} w_i T_{зі} v_i F_i};\quad i = \overline{1N},$$

де $T_{РЕК}$ – наробіток на відмову ТЗР;

$T_{ВЗК}$ – наробіток на відмову вбудованих засобів контролю;

$F_{ВЗК}$ – загальна вартість вбудованих засобів контролю;

T_{ei} – наробіток на відмову сукупності елементів, які впливають на параметр i;

$T_{зі}$ – наробіток на відмову вбудованих засобів контролю параметра *i*;
F_i – загальна вартість вбудованих засобів контролю параметра *i*.

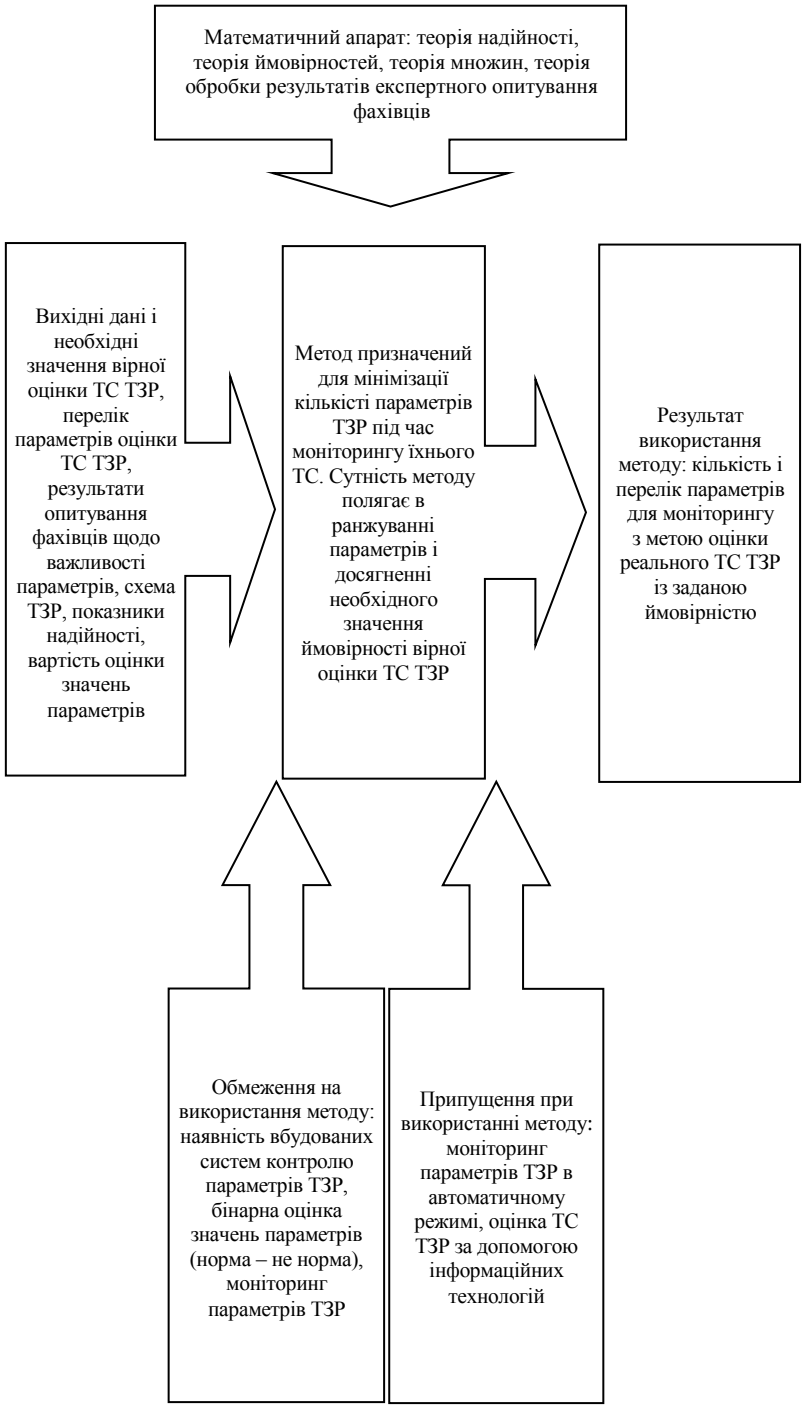


Рис. 1. Схема реалізації методу обґрунтування мінімально необхідної кількості параметрів ТЗР для моніторингу і оцінки їхнього ТС із заданою ймовірністю необхідною для отримання достовірної оцінки ТС ТЗР

У цьому випадку для ранжування параметрів ТЗР пропонується кожний з них оцінити комплексним показником u_i:

$$U_i = \frac{u_i}{\sum_{i=1}^{N} u_i}; \quad \sum_{i=1}^{N} U_i = 1.$$

Значення u_i безрозмірне та суттєво відрізняється для окремих параметрів, тому для їх ранжування доцільно використовувати ймовірність переважного вибору.

Після ранжування параметрів в порядку зменшення значення u_i визначають мінімальну необхідну кількість параметрів для моніторингу ТЗР за критерієм досягнення заданого значення ймовірності вірної оцінки ТС, як частини ТЗР, що перевіряють:

$$P_m = \frac{\sum_{i=1}^{m} L_i}{L} \geq P; \quad 1 \leq m \leq N,$$

де L_i – кількість елементів, які впливають на параметр i;

$L = \sum_{i-1}^{m} L_i$ – загальна кількість елементів ТЗР;

m – мінімально необхідна кількість параметрів ТЗР, які перевіряються під час моніторингу ТС.

Блок-схема алгоритму реалізації методу представлена на рисунку 2. Розглянемо його використання на прикладі ТЗР, теоретико-множинна модель якого представлена на рисунку 3, вихідні дані в таблиці 1.

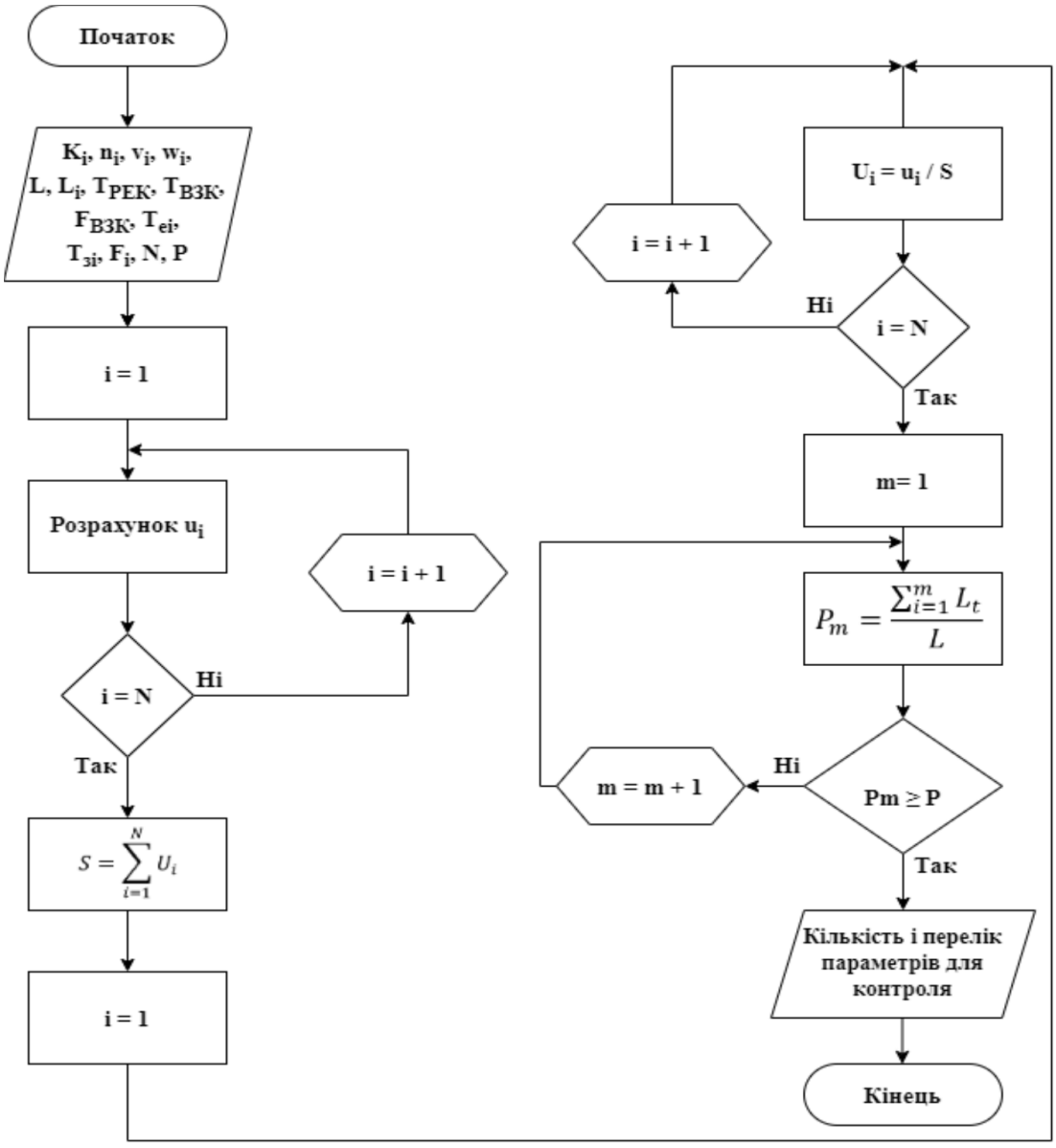


Рис. 2. Блок-схема алгоритму реалізації методу мінімізації кількості параметрів ТЗР

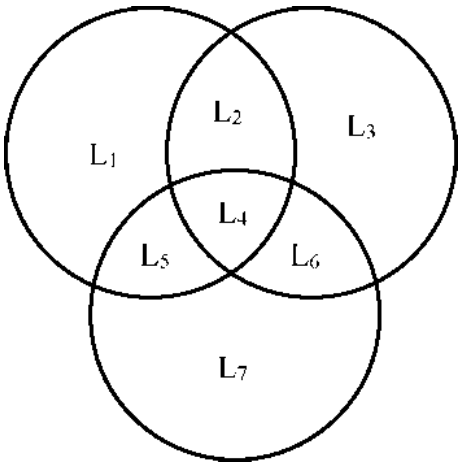


Рис. 3. Теоретико-множинна модель ТЗР від кількості перевірених параметрів після їх ранжування

Таблиця 1

Приклад реалізації методу мінімізації кількості параметрів ТЗР для оцінки їхнього ТС (вихідні дані)

i	**Вихідні дані**							
	k_i	n_i	v_i	w_i	T_{ei}	$T_{зi}$	F_i	L_i
1	0,70	0,2	0,05	0,05	800	11000	50	120
2	0,60	0,2	0,1	0,1	1200	9000	70	80
3	0,80	0,1	0,05	0,05	2000	12000	180	80
4	0,75	0,2	0,03	0,02	9000	8000	60	210
5	0,65	0,25	0,05	0,05	1400	10000	150	70
6	0,80	0,05	0,10	0,05	1100	13000	80	125
7	0,55	0,25	0,1	0,1	2500	14000	70	70

На рисунку 3 підмножини елементів L_i впливають на формування параметра i. В цьому випадку $N = 7$, а сукупність підмножин елементів ТЗР

$$L = \bigcup_{i=1}^{7} L_i \ .$$

Відповідно, для прикладу, який розглядається в статті, $T_{РЕК} = 175$ год; $T_{ВЗК} = 1520$ год; $F_{ВЗК} = 470$.

Результати розрахунків згідно з блок-схемою алгоритму (див. рис. 2) представлено в таблиці 2.

Таблиця 2

Ранжування параметрів радіоелектронного комплексу

i	u_i	U_i	$P_{анг}$	P_m
1	397,8	0,1435	2	0,4370
2	49,6	0,0179	6	0,9073
3	92,6	0,0335	4	0,7086
4	1808,7	0,6526	1	0,2781
5	61,9	0,0223	5	0,8013
6	349,7	0,1262	3	0,6026
7	11,2	0,0040	7	1,0000

Необхідно визначення ТС з ймовірністю не нижче $P \geq 0,9$. У такому разі $S = 2771,5$ і $L = 755$. Розрахунки показують, що для досягнення необхідної ймовірності оцінки ТС РЕК достатньо контролювати m = 6 параметрів, при цьому $P = 0,9073$.

Ефект від використання методу кількісно оцінюється відносним скороченням числа контрольованих параметрів:

$$\eta = \frac{N - mN}{N} 100\% = \frac{7-6}{7} 100\% = 14{,}3\% .$$

Тобто, в прикладі, що розглядається, сьомий параметр контролювати не обов'язково (рис. 4).

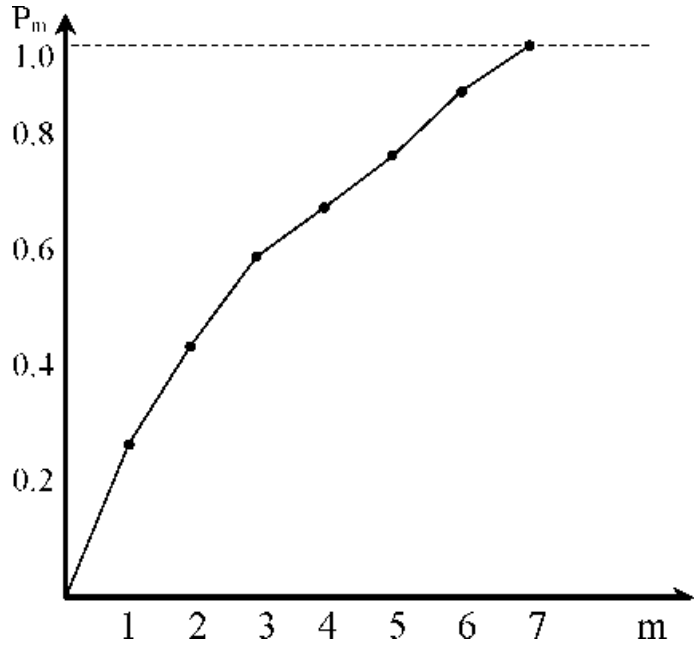


Рис. 4. Залежність ймовірності правильної оцінки ТС ТЗР

Аналіз результатів показує, що значення правильної оцінки ТС комплексу (рис. 3) суттєво збільшується зі збільшенням кількості перевірених параметрів *m.*

Причому $\Delta_i = P - P_{i-1}$, тобто приріст ймовірностей правильної оцінки ТС збільшується з кожним кроком:

$$\Delta_{i-1} \leq \Delta_i; \quad i = \overline{1, m.}$$

Це свідчить про те, що ранжування порядку перевірки параметрів ТЗР виконано правильно.

Висновки. Вперше запропоновано алгоритм обґрунтування мінімально необхідної кількості параметрів ТЗР для моніторингу їхнього ТС.

Розроблено схему і алгоритм реалізації методу з використанням комплексного показника кожного параметра виробу, який враховує його важливість для користувача, надійність елементів і вартість засобів контролю.

Як критерій при визначенні кількості параметрів для моніторингу ТС ТЗР пропонується відношення кількості елементів перевіреної частини комплексу до загального числа його елементів після ранжування параметрів за обраним комплексним показником, що відповідає достовірній оцінці його ТС.

Приведено приклад використання методу з оцінкою його ефективності за відносним скороченням кількості параметрів для моніторингу до їх загального числа.

Подальші дослідження доцільно направити на використання отриманих результатів для прогнозування ТС ТЗР на основі сучасних інформаційних технологій, що дозволить оптимізувати періоди ТО і планових ремонтів за критерієм мінімуму вартості при збереженні необхідних значень показників надійності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грохольський Я. М. Військовий зв’язок в початковий період ліквідації аварії на Чорнобильській АЕС / Я. М. Грохольський, Л. М. Сакович, Г. Я. Криховецький // Системи управління, навігації та зв’язку. 2021. № 2 (64). С. 125–131.

2. Abraham, S., Dhaliwal, H., Efford, R. J., Keen, L. J., McLellan, A., & Wood, P. (2004). Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations. Retrieved from https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

3. Volodymyr Kononov, Yevhen Ryzhov, Lev Sakovych. Dependence of parametrs of repaire of military communication means on the quality of metrological support. Advanced Information Systems. 2017, Vol. 2, № 1, P. 91–95. DOI: http//doi.org/10.20998/2522-9052.2018.1.17.

4. Бобало Ю. Я. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем: монографія / Ю. Я. Бобало, Б. Ю. Волочій, О. Ю. Лозинський та ін. Львів: Львівська політехніка, 2013. 300 с.

5. Рижов Є. В., Сакович Л. М. Метод визначення послідовності перевірки параметрів під час технічного обслуговування військової техніки зв’язку за станом // Озброєння та військова техніка. 2017. № 4 (16). С. 70–72. DOI: https//doi.org/10.34169/2414- 0651.2017.4(16).70-72.

6. Гнатюк С. Є., Сакович Л. М., Мирошниченко Ю. В. Моделювання порядку перевірки параметрів при технічному обслуговуванні за станом радіоелектронних засобів // Електронне моделювання. 2020. Т. 42, № 5. С. 120–128.

7. Сакович Л. М., Криховецький Г. Я., Міхін О. В., Мирошниченко Ю. В. Оцінка впливу метрологічного та діагностичного забезпечення на технічне обслуговування за станом засобів зв’язку // Сучасні інформаційні системи. 2021. Т. 5, № 2. С. 120–125.

DOI: 10.58254/viti.3.2023.14.117

УДК 004.94:[355.582:621.396.9]

канд. техн. наук Телюков С. М. ORCID: 0000-0002-0067-8028 (ХНУПС ім. Івана Кожедуба)
Дроль О. Ю. ORCID: 0000-0002-5472-208X (ХНУПС ім. Івана Кожедуба)
канд. техн. наук Куценко В. В. ORCID: 0000-0002-4174-2145 (ДНДІ ВС ОВТ)
доктор філософії Горбачов К. М. ORCID: 0000-0001-7931-1028 (НУОУ ім. Івана Черняховського)

ПРОСТОРОВО-ЧАСОВА МОДЕЛЬ ВИЗНАЧЕННЯ МОЖЛИВОСТІ СВОЄЧАСНОЇ ПРОТИДІЇ ПРОТИВНИКУ СИЛАМИ І ЗАСОБАМИ СПОСТЕРЕЖНОГО ПОСТА ПІДРОЗДІЛУ ОХОРОНИ

Досвід виконання бойових (службово-бойових) завдань різними складовими сектору безпеки та оборони у початковому періоді російсько-української війни вказує на необхідність надійної охорони та оборони військових частин (об'єктів), основою якої є планування та здійснення силами оперативного реагування заходів, що спрямовані на повну нейтралізацію або зменшення негативного впливу від дій диверсійних сил противника.

Для забезпечення якісного планування охорони та оборони об'єкта (об'єктів) військової частини командирам (начальникам) необхідно мати відповідний інструмент підтримки прийняття обґрунтованих рішень, а саме математичний (розрахунковий, аналітичний) апарат, що дасть можливість у визначених умовах спрогнозувати події, які можуть статись у разі нападу противника, та визначити дієві заходи щодо максимального збереження цілісності (боєздатності) об'єктів, що охороняються.

У статті представлено просторово-часову модель визначення можливості своєчасної протидії противнику силами і засобами спостережного поста підрозділу охорони, що ґрунтується на вирішенні просторово-часової задачі та на відміну від існуючих враховує: вогневі можливості своїх сил та противника; маневрені можливості основних (чергових) сил підрозділу охорони; взаємне розміщення противника відносно спостережного поста і об'єктів охорони, а також основних (чергових) сил підрозділу охорони.

У подальшому запропонована в статті модель може бути використана як складова частина методики визначення раціонального складу сил та засобів охорони та оборони військових частин (об'єктів). Також даний інструмент може бути впроваджений у навчальний процес.

Ключові слова: *російсько-українська війна, охорона та оборона об'єктів, оперативне реагування, оцінювання результативності дій, елементи безпосередньої сили охорони, просторово-часова модель.*

S. Telyukov, O. Drol, V. Kutsenko, K. Horbachov A spatio-temporal model for determining the possibility of timely counteraction to the enemy by the forces and means of the observation post of a security unit.

The experience of carrying out combat (service-combat) tasks by various components of the security and defense sector in the initial period of the russian-Ukrainian war points to the need for reliable protection and defense of military units (objects), the basis of which is the planning and implementation by operative response forces of measures aimed at for complete neutralization or reduction of the negative impact from the actions of the enemy's subversive forces.

In order to ensure high-quality planning of the protection and defense of the object (objects) of the military unit, commanders (chiefs) need to have an appropriate tool to support informed decision-making, namely a mathematical (calculation, analytical) apparatus that will make it possible to predict events under certain conditions. which may occur in the event of an enemy attack and determine effective measures for maximum preservation of the integrity (combat capability) of the protected objects.

The article presents a spatio-temporal model for determining the possibility of timely countering the enemy with the forces and means of the observation post of the security unit, which is based on the solution of the spatio-temporal problem, and, unlike the existing ones, takes into account: the fire capabilities of the observation post and on-duty forces; maneuverability of the main (regular) forces of the security unit; mutual placement of the enemy in relation to the observation post and security facilities, as well as the main (on-duty) forces of the security unit.

In the future, the model proposed in the article can be used as an integral part of the methodology for determining the rational composition of forces and means of protection and defense of military units (objects). Also, this tool can be implemented in the educational process.

Keywords: *Russian-Ukrainian war, protection and defense of objects, operational response, evaluation of the effectiveness of actions, elements of direct protection force, spatio-temporal model.*

Постановка задачі в загальному вигляді. Виграш в просторі і часі надає перевагу та успіх при виконанні бойового завдання. Безумовно, своєчасне виявлення противника в обґрунтовано визначеному районі пошуку та його стримування забезпечить оперативне реагування на дії противника основними (черговими) силами підрозділу охорони військової

частини, з метою захисту об’єкта (об’єктів) охорони. Одним із основних елементів в системі охорони об’єкта (об’єктів) військової частини, що забезпечує своєчасне виявлення противника, є спостережний пост (спостережні пости) підрозділу охорони цієї частини [1].

Відповідальність за організацію охорони військових об’єктів несуть начальники штабів військових частин (органів управління), командири підрозділів [1–5], яким необхідно знати, розуміти та володіти методиками оцінювання можливості своєчасної протидії противнику та в подальшому визначення оптимального складу сил та засобів охорони об’єкта (об’єктів) військової частини.

Відповідно до мети охорони об’єкта (об’єктів) військової частини необхідним чинником, що впливає на ефективність організації охорони, є своєчасність виконання запобіжних та оборонних (стримуючих) заходів, що передбачає обов’язкову наявність у складі сил та засобів охорони осіб і обладнання, які будуть забезпечувати реалізацію процесу своєчасного виявлення ознак імовірної протидії або диверсії з боку противника, а також вести оборонні (стримуючі) дії до прибуття чергових сил підрозділу охорони.

Тому, з метою підготовки надійної охорони та оборони об’єкта (об’єктів) військової частини командирам (начальникам) необхідно мати відповідний інструмент підтримки прийняття обґрунтованих рішень, а саме математичний (розрахунковий, аналітичний) апарат, що дасть можливість у визначених умовах спрогнозувати події, які можуть статись у разі нападу противника, та визначити заходи щодо нейтралізації або максимального нівелювання їхнього негативного впливу на об’єкт, що охороняється.

Таким чином, з урахуванням того, що спостережні пости є одними з основних елементів безпосередньої охорони військової частини, оцінювання їхніх можливостей щодо протидії противнику до прибуття чергових сил підрозділу охорони дозволить особам, які приймають рішення, якісно планувати та здійснювати охорону та оборону об’єкта (об’єктів) військової частини.

Аналіз останніх досліджень і публікацій. У Збройних силах України та безпосередньо в частинах і підрозділах Повітряних сил Збройних сил України (ПС ЗС України) охорона об’єктів організована й здійснюється на підставі вимог низки організаційно-керівних та методичних документів [1–9], але на сьогодні в них не врахований досвід виконання аналогічних завдань іншими військовими формуваннями у початковому періоді російсько-української війни, а також відсутні конкретні алгоритми вибору більш ефективних способів виконання завдань.

Так, наприклад, у організаційно-керівних вказівках щодо заходів охорони об’єктів військової частини (підрозділу) визначено лише загальну послідовність їх виконання [1–5].

Аналіз результатів наукових робіт, що присвячені дослідженням процесів підготовки і ведення охорони, пріоритетності (важливості) об’єктів, які підлягають охороні, а також визначенню необхідного кількісного складу сил і засобів для забезпечення охорони державних об’єктів [10–16], показав, що наявний науково-методичний апарат не може бути застосований для оцінювання можливостей (результативності) елементів безпосередньої охорони військових частин (об’єктів), так як в основному призначений для формувань більш високого рівня [15; 16], а також не враховує низки факторів, вплив яких, за досвідом російсько-української війни, може суттєво змінити хід виконання завдань [10–14].

Тобто, на тактичному рівні вирішення завдання забезпечення посадових осіб, які приймають рішення, відповідними математичними (розрахунковими, аналітичними) інструментом підтримки, є досить важливим та актуальним.

Таким чином, розробка просторово-часової моделі визначення можливості своєчасної протидії противнику силами і засобами спостережного поста підрозділу охорони є одним з важливих кроків до впровадження наукового підходу у процес підготовки і практичної реалізації заходів охорони об’єкта (об’єктів) військової частини, який може в подальшому забезпечити можливість оперативного реагування на дії противника в різних умовах обстановки.

Метою статті є оприлюднення результатів розробки просторово-часової моделі визначення можливості своєчасної протидії противнику силами і засобами спостережного поста підрозділу охорони.

Виклад основного матеріалу. Своєчасність виявлення загроз полягає у створенні таких умов пошуку та ідентифікації противника, які забезпечать оперативне реагування на них силами підрозділу охорони об’єкта (об’єктів), як чергових, так і основних.

Оперативне реагування основних (чергових) сил підрозділу охорони полягає у своєчасному виконанні дій щодо блокування, придушення або примушення відмовитись від подальших дій противника до того, як він буде мати можливість знищити або зруйнувати об’єкт охорони. При цьому, основними факторами, які впливатимуть на можливості їх виконання силами і засобами спостережного поста, основних або чергових сил підрозділу охорони будуть:

– характеристики району виконання завдань: умови спостереження (пора року, час доби, погода та інші чинники, що можуть впливати на виявлення противника), умови переміщення (стан та прохідність доріг, прохідність місцевості та інші чинники, що можуть впливати на швидкість руху);

– імовірне вихідне положення противника (місце його виявлення), характер та напрямки руху, а також його вогневі можливості (наприклад, максимальна дальність ведення вогню);

– призначене вихідне положення основних (чергових) сил підрозділу охорони, можлива середня швидкість руху їхніх транспортних засобів, дальність дії зброї;

– розташування, роль і місце спостережного поста в системі охорони об’єкта;

– розташування об’єкта охорони.

Один з найпростіших варіантів вихідної обстановки для проведення розрахунків наведений на рисунку 1.

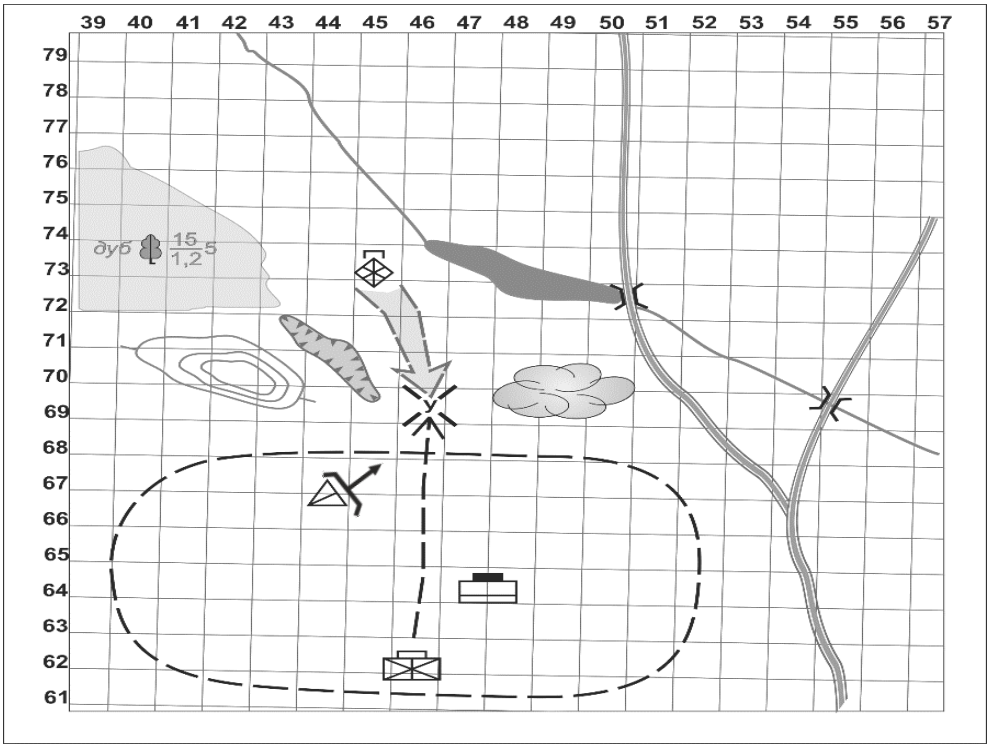


Рис. 1. Варіант схеми вихідної обстановки
Джерело: розроблено авторами за даними [1; 17]

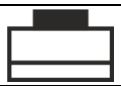
Визначення можливостей щодо протидії противнику може проводитись як відносно вихідного положення основних (чергових) сил підрозділу охорони, так і відносно спостережного поста, а в якості вихідних можуть розглядатись характеристики можливих

об'єктів охорони (пункти управління, технічні засоби, об'єкти критичної інфраструктури тощо), противника (диверсійно розвідувальна група або інші спеціально створені формування), своїх основних (чергових) сил (відділення, взвод, мобільна вогнева група тощо).

Умовні позначення, а також їхній можливий зміст, для графічного опису вихідних умов та процесу розрахунку можливостей протидії противнику основними (черговими) силами та силами спостережного поста підрозділу охорони наведені в таблиці 1.

Таблиця 1

Умовні позначення та їх зміст

Умовне позначення	**Зміст умовного позначення**
	Об'єкт охорони (об'єкт матеріально- технічного забезпечення)
	Спостережний пост
	Противник (диверсійно-розвідувальна група)
	Свої чергові сили (мобільна група)
	Рубіж атаки (відкриття вогню)

Джерело: розроблено авторами за даними [17]

Дані умови можуть бути представлені у вигляді прямокутної системи координат, яка відображена на рисунку 2, де:

$D_{\text{ВПр0}}$ – дальність виявлення противника відносно спостережного поста;

$\omega_{\text{ВПр0}}$ – азимут виявлення противника;

$X_{\text{Пр0}}$, $Y_{\text{Пр0}}$ – прямокутні координати виявлення противника;

$V_{\text{Пр}}$ – імовірна швидкість руху противника;

$\beta_{\text{Пр}}$ – кут імовірного напрямку руху противника;

$R_j^{\text{ЗрПр}}$ –інформація про імовірну дальність дії зброї j-го виду противника;

$D_{\text{Св0}}$ – дальність до місця знаходження основних (чергових) сил відносно спостережного поста;

$V_{\text{Св}}$ – швидкість руху основних (чергових) сил підрозділу охорони до рубежу атаки противника;

$\varphi_{\text{Св0}}$ – азимут місця знаходження основних (чергових) сил;

$\alpha_{\text{Св}}$ – необхідний напрямок руху основних (чергових) сил підрозділу охорони на рубіж атаки противника;

$X_{\text{Св0}}$, $Y_{\text{Св0}}$ – прямокутні координати місця знаходження основних (чергових) сил;

$R_i^{\text{ЗрСв}}$ – дальність дії зброї i -го типу основних (чергових) сил;

$R_i^{\text{ЗрСП}}$ – дальність дії зброї i-го типу спостережного поста зі складу підрозділу охорони;

$D_{\text{Ох}}$ – дальність до об'єкта охорони відносно спостережного поста;

$\lambda_{\text{Ох}}$ – азимут об'єкта охорони;

$X_{\text{Ох}}$, $Y_{\text{Ох}}$ – координати об'єкта охорони.

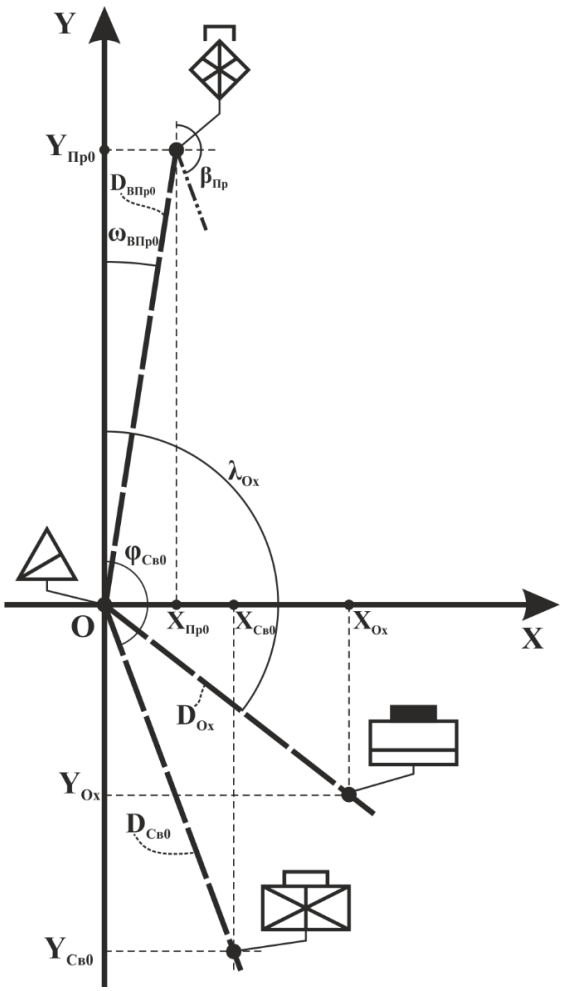


Рис. 2. Вихідні умови обстановки
Джерело: розроблено авторами

Необхідно визначити:

$t_{\text{РАСв}}$ – час для виходу на рубіж атаки противника основними (черговими) силами підрозділу охорони;

$L_{\text{РАСв}}$ – відстань від місця знаходження основних (чергових) сил підрозділу охорони до рубежу атаки противника;

$D_{\text{РАСв}}$ – дальність до рубежу атаки противника основними (черговими) силами відносно спостережного поста підрозділу охорони;

$X_{\text{РАСв}}$, $Y_{\text{РАСв}}$ – прямокутні координати рубежу атаки противника основними (черговими) силами підрозділу охорони;

$D_{\text{Р2}}$ – дальність до імовірного місця зупинення противника відносно спостережного поста;

$X_{\text{Р2}}$, $Y_{\text{Р2}}$ – координати місця можливої зупинки противника (рубіж № 2) основними (черговими) силами відносно спостережного поста підрозділу охорони;

$D_{\text{Р1}}$ – дальність до місця можливого зупинення противника (рубіж № 1) силами спостережного поста підрозділу охорони;

$X_{\text{Р1}}$, $Y_{\text{Р1}}$ – координати місця можливої зупинки противника силами спостережного поста підрозділу охорони.

Для розуміння процесу проведення розрахунків на рисунку 3 представлена їхня схема в прямокутній системі координат, де:

O – місце знаходження спостережного поста підрозділу охорони;

E – імовірне вихідне положення противника;

G – вихідне положення основних (чергових) сил підрозділу охорони;

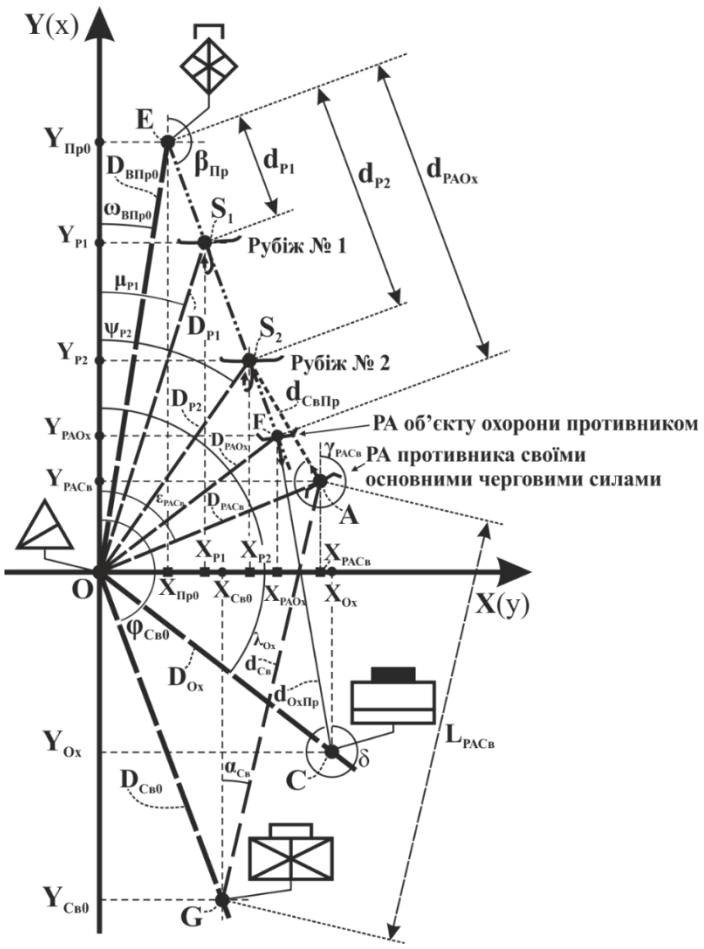


Рис. 3. Схема процесу розрахунку можливості протидії противнику основними (черговими) силами та силами спостережного поста підрозділу охорони.
Джерело: розроблено авторами

C – місце знаходження об’єкта охорони;

A – рубіж атаки противника основними (черговими) силами підрозділу охорони;

S_2 – місце можливого зупинення противника (рубіж № 2) основними (черговими) силами відносно спостережного поста підрозділу охорони;

$\psi_{\text{Р2}}$ – кут положення місця зупинення противника (рубіж № 2) основними (черговими) силами відносно спостережного поста підрозділу охорони;

$\varepsilon_{\text{РАСв}}$ – кут положення позиції для атаки противника основними (черговими) силами відносно спостережного поста підрозділу охорони;

S_1 – місце можливого зупинення противника (рубіж № 1) силами спостережного поста підрозділу охорони;

$\psi_{\text{Р1}}$ – кут положення місця зупинення противника (рубіж № 1) силами спостережного поста підрозділу охорони;

$\gamma_{\text{РАСв}}$ – кут атаки противника основними (черговими) силами підрозділу охорони;

$d_{\text{ОхПр}}$ – відстань, що може буте пройдена противником від місця його виявлення до можливого місця атаки об’єкта охорони противником;

$d_{\text{Р2}}$ – відстань, що може буте пройдена противником від місця виявлення до місця його можливого зупинення (рубіж № 2) своїми (черговими) силами підрозділу охорони;

$d_{\text{Р1}}$ – відстань, що може буте пройдена противником від місця виявлення до місця його можливого зупинення (рубіж № 1) силами спостережного поста підрозділу охорони;

$d_{\text{Св}}$ – відстань, що буде пройдена основними (черговими) силами підрозділу охорони відносно їхнього вихідного положення;

$d_{\text{Пр}}$ – відстань, що буде пройдена противником відносно його вихідного положення;

$d_{\text{СвПр}}$ – відстань між основними (черговими) силами підрозділу охорони та противником;

$d_{\text{ОхПр}}$ – відстань між об'єктом охорони у та місцем імовірної атаки противника цього об'єкта.

Обов'язковими умовами атаки противника основними (черговими) силами та силами спостережного поста підрозділу охорони є:

– умова 1 – відстань між противником та основними (черговими) силами підрозділу охорони повинна бути менше або дорівнюватись дальності дії зброї i-го типу своїх сил:

$$d_{\text{СвПр}} \le R_i^{\text{ЗрСв}}, i-1, I; \tag{1}$$

– умова 2 – умова захисту об'єкта охорони – відстані між об'єктом захисту та противником повинна бути більше дальності дії зброї j-го типу противника:

$$d_{\text{ОхПр}} > R_j^{\text{ЗрПр}}, j = 1, J; \tag{2}$$

– умова 3 – відстань між противником та спостережним постом підрозділу охорони повинна бути менше або дорівнюватись дальності дії зброї i-го типу спостережного поста:

$$D_{\text{Р1}} \le R_i^{\text{ЗрСП}}, i = 1, I. \tag{3}$$

Відстань між противником та основними (черговими) силами підрозділу охорони визначається таким чином:

$$d_{\text{СвПр}} = \sqrt{\left(X_{\text{Св}} - X_{\text{Пр}}\right)^2 + \left(Y_{\text{Св}} - Y_{\text{Пр}}\right)^2}, \tag{4}$$

де $X_{\text{Св}}$, $Y_{\text{Св}}$ – прямокутні координати поточного місцезнаходження основних (чергових) сил підрозділу охорони;

$X_{\text{Пр}}$, $Y_{\text{Пр}}$ – прямокутні координати поточного місцезнаходження противника.

Координати $X_{\text{Св}}$, $Y_{\text{Св}}$, $X_{\text{Пр}}$, $Y_{\text{Пр}}$ визначаються за наступними формулами:

$$X_{\text{Св}} = D_{\text{Св0}} \cdot sin(\varphi_{\text{Св0}}) + d_{\text{Св}} \cdot sin(\alpha_{\text{Св}}); \tag{5}$$

$$Y_{\text{Св}} = D_{\text{Св0}} \cdot cos(\varphi_{\text{Св0}}) + d_{\text{Св}} \cdot cos(\alpha_{\text{Св}}); \tag{6}$$

$$X_{\text{Пр}} = D_{\text{ВПр0}} \cdot sin\left(\omega_{\text{ВПр0}}\right) + d_{\text{Пр}} \cdot sin\left(\beta_{\text{Пр}}\right); \tag{7}$$

$$Y_{\text{Пр}} = D_{\text{ВПр0}} \cdot cos\left(\omega_{\text{ВПр0}}\right) + d_{\text{Пр}} \cdot cos\left(\beta_{\text{Пр}}\right). \tag{8}$$

Прямокутні координати та дальність до місця атаки противником об'єкта охорони відносно спостережного поста визначається як:

$$\left.\begin{matrix} X_{\text{РАОх}} = X_{\text{Пр}} \\ Y_{\text{РАОх}} = Y_{\text{Пр}} \end{matrix}\right| \text{якщо } d_{\text{ОхПр}} \le R_j^{\text{ЗрПр}}; \tag{9}$$

$$D_{\text{РАОх}} = \sqrt{{X_{\text{РАОх}}}^2 + {Y_{\text{РАОх}}}^2}. \tag{10}$$

Відстань між об'єктом захисту та імовірним рубежем атаки противником цього об'єкта визначається як:

$$d_{\text{ОхПр}} = \sqrt{(X_{\text{РАОх}} - X_{\text{Ох}})^2 + (Y_{\text{РАОх}} - Y_{\text{Ох}})^2}. \tag{11}$$

Відстань, що буде пройдена основними (черговими) силами підрозділу охорони та противником відносно їхніх вихідних положень, визначається наступним чином:

$$d_{\text{Св}} = V_{\text{Св}} \cdot \left(t - t_{\text{затр}}\right); \tag{12}$$

$$d_{\text{Пр}} = V_{\text{Пр}} \cdot t, \tag{13}$$

де t – поточний час;

$t_{\text{затр}}$ – час затримки, обумовлений моментом висування основних (чергових) сил підрозділу охорони з вихідного положення та часом їх розгортання на рубежі атаки.

Прямокутні координати та дальність до рубежу атаки противника основними (черговими) силами відносно спостережного поста підрозділу охорони визначаються як:

$$\left.\begin{matrix} X_{\text{РАСв}} = X_{\text{Св}} \\ Y_{\text{РАСв}} = Y_{\text{Св}} \end{matrix}\right| \text{якщо } d_{\text{СвПр}} \le R_i^{\text{ЗрСв}}; \tag{14}$$

$$D_{\text{РАСв}} = \sqrt{{X_{\text{РАСв}}}^2 + {Y_{\text{РАСв}}}^2}. \tag{15}$$

Відстань до місця розгортання для проведення атаки та час, що необхідний для висування своїх основними чергових сил підрозділу охорони від їхнього вихідного положення, визначаються наступним чином:

$$L_{\text{РАСв}} = \sqrt{(X_{\text{Св0}} - X_{\text{РАСв}})^2 + (Y_{\text{Св0}} - Y_{\text{РАСв}})^2}; \tag{16}$$

$$t_{\text{РАСв}} = \frac{L_{\text{РАСв}}}{V_{\text{Св}}}. \tag{17}$$

Необхідний напрямок руху основних (чергових) сил, а саме діапазон значень кута $\Delta\alpha_{\text{АСв}}$ та мінімально необхідна швидкість їх руху $V_{\text{АСв}}^{min}$ для проведення атаки противника, можуть бути визначені за допомогою наступної системи нерівностей (18):

$$\begin{matrix} \Delta\alpha_{\text{АСв}} = \{\alpha_{\text{АСв}}\} \leftarrow \alpha_{\text{Св}} \\ V_{\text{АСв}}^{min\, min\{V_{\text{Св}}\}} \end{matrix} \left\{\begin{matrix} \sqrt{\left(X_{\text{Св}} - X_{\text{Пр}}\right)^2 + \left(Y_{Св} - Y_{Пр}\right)^2} \le R_i^{\text{ЗрСв}} \\ \sqrt{\left(X_{\text{Пр}} - X_{\text{Ох}}\right)^2 + \left(Y_{\text{Пр}} - Y_{\text{Ох}}\right)^2} > R_i^{\text{ЗрПр}} \end{matrix}\right|. \tag{18}$$

Таким чином, згідно з (15)–(17) можливо визначити просторово-часові характеристики рубежу атаки $D_{\text{РАСв}}$, $L_{\text{РАСв}}$ та $t_{\text{РАСв}}$ противника основними (черговими) силами в заданих умовах (1) та (2), а за допомогою (18) визначити, при яких саме напрямках та мінімальній швидкості висування основних (чергових) сил, що дозволить визначити можливість проведення атаки противника основними (черговими) силами з метою забезпечення захисту об'єктів та стримування дій противника.

Також можливо визначити найбільш доцільне місцезнаходження основних (чергових) сил охорони для своєчасного здійснення атаки противника з метою захисту об'єкта, коли відомо декілька імовірних напрямків дій противника ES_1, ES_2 (див. рис. 3).

Для виконання умови (2), а саме умови захисту об'єкта охорони, необхідно зупинити противника на відстані від об'єкта охорони, що не дозволить йому знищити (зруйнувати) цей об'єкт. Тобто не допустити вихід противника на рубіж атаки об'єкта охорони. Тому необхідно визначити імовірне місце зупинення противника (рубіж № 1) силами спостережного поста та імовірне місце зупинення противника (рубіж № 2) основними (черговими) силами підрозділу охорони.

Прямокутні координати та дальність до імовірного місця зупинення противника (рубіж № 1) силами спостережного поста підрозділу охорони визначається як:

$$\begin{matrix} X_{\text{Р1}} = X_{\text{Пр}} \\ Y_{\text{Р1}} = Y_{\text{Пр}} \end{matrix} \Big| \text{якщо} \begin{matrix} d_{\text{ОхПр}} \le R_j^{\text{ЗрПр}} \\ D_{\text{Р1}} \le R_i^{\text{ЗрСП}} \end{matrix}; \tag{19}$$

$$D_{\text{Р1}} = \sqrt{{X_{\text{Р1}}}^2 + {Y_{\text{Р1}}}^2}. \tag{20}$$

Відстань від місця виявлення противника до місця імовірного зупинення противника (рубежу № 1) силами спостережного поста підрозділу охорони та час, за який противник буде знаходитись на імовірному місці зупинення, визначаються наступним чином:

$$d_{\text{Р1}} = \sqrt{\left(X_{\text{Пр0}} - X_{\text{Р1}}\right)^2 + \left(Y_{\text{Пр0}} - Y_{\text{Р1}}\right)^2}; \tag{21}$$

$$t_{\text{Р1}} = \frac{d_{\text{Р1}}}{V_{\text{Пр}}}. \tag{22}$$

Прямокутні координати та дальність до місця імовірного зупинення противника (рубіж № 2) основними (черговими) силами відносно спостережного поста підрозділу охорони визначається як:

$$\begin{matrix} X_{\text{Р2}} = X_{\text{Пр}} \\ Y_{\text{Р2}} = Y_{\text{Пр}} \end{matrix} \Big| \text{якщо} \begin{matrix} d_{\text{ОхПр}} > R_j^{\text{ЗрПр}} \\ D_{\text{Р2}} \le R_i^{\text{ЗрСв}} \end{matrix}; \tag{23}$$

$$D_{\text{Р2}} = K\sqrt{{X_{\text{Р2}}}^2 + {Y_{\text{Р2}}}^2}, \tag{24}$$

де K – коефіцієнт, що враховує збільшення відстані залежно від умов руху.

Відстань від місця виявлення противника до імовірного місця імовірного зупинення противника (рубежу № 2) основними (черговими) силами та час, за який противник буде знаходитись на імовірному місці зупинення, визначаються наступним чином:

$$d_{\text{Р2}} = K\sqrt{\left(X_{\text{Пр0}} - X_{\text{Р2}}\right)^2 + \left(Y_{\text{Пр0}} - Y_{\text{Р2}}\right)^2}; \tag{25}$$

$$t_{\text{Р2}} = \frac{d_{\text{Р2}}}{V_{\text{Пр}}}. \tag{26}$$

Затримка противника силами та засобами спостережного поста повинна забезпечувати зменшення швидкості просування противника (або тимчасове зупинення) і, як наслідок, зменшення часу виходу противника на імовірний рубіж атаки об'єкта охорони, який визначається таким чином:

$$t_{\text{РАОх}} = \frac{d_{\text{РАОх}}}{V_{\text{Пр}}}, \tag{27}$$

де $d_{\text{РАОх}}$ – відстань від місця виявлення противника до місця імовірного рубежу атаки об'єкта охорони противником:

$$d_{\text{РАОх}} = \sqrt{\left(X_{\text{Пр0}} - X_{\text{РАОх}}\right)^2 + \left(Y_{\text{Пр0}} - Y_{\text{РАОх}}\right)^2}. \tag{28}$$

Тобто умова затримки противника силами та засобами спостережного поста має наступний вид:

$$t_{\text{РАОх}} > t_{i_{\text{реак}}}^{\text{Св}}, \tag{29}$$

де $t_{i_{\text{реак}}}^{\text{Св}}$ – час реакції основних (чергових) сил підрозділу охорони з озброєнням i-го типу на дії противника.

Час реакції основних (чергових) сил залежить від: часу їх висування на рубіж атаки противника $t_{\text{РАСв}}$, часу розгортання вогневого засобу i-го типу $t_{i_{\text{розг}}}^{\text{Св}}$ та його циклу бойової роботи $t_{i_{\text{ЦБР}}}^{\text{Св}}$ вогневого засобу:

$$t_{i_{\text{реак}}}^{\text{Св}} = t_{\text{РАСв}} + t_{i_{\text{розг}}}^{\text{Св}} + t_{i_{\text{ЦБР}}}^{\text{Св}}. \quad (30)$$

Висновки. Отримана модель ґрунтується на вирішенні просторово-часової задачі у вигляді алгоритму розрахункового процесу, а також, на відміну від існуючих, враховує сукупність факторів, які за досвідом російсько-української війни можуть суттєво впливати на виконання завдань охорони та оборони об'єктів, а саме: вогневі можливості спостережного посту та чергових сил; маневрені можливості основних (чергових) сил підрозділу охорони; взаємне розміщення противника відносно спостережного поста і об'єктів охорони, а також основних (чергових) сил підрозділу охорони.

Адекватність даної просторово-часової моделі забезпечується використанням в ході її розробки декількох методів досліджень (аналіз, експертних оцінок, таксономії), сукупності сталих математичних виразів, а також обмежень та припущень, які дозволяють отримувати результати розрахунків з достатньою для прийняття рішень точністю, а саме:

– дальність виявлення противника силами і засобами охорони, що приймається для розрахунків, повинна відповідати умовам спостереження у визначеній обстановці;

– швидкість руху противника, що приймається для розрахунків, визначається як середнє арифметичне від швидкостей руху на різних ділянках імовірного маршруту виходу до об'єкта охорони;

– швидкість руху чергових сил підрозділу охорони, що приймається для розрахунків, визначається як максимально можлива для маршруту зближення з противником;

– дальність дії зброї, що приймається для розрахунків, визначається за найбільшою прицільною дальністю;

– розташування, роль і місце спостережного поста.

Запропонована просторово-часова модель може бути використана для вирішення наступних основних задач в ході оцінювання обстановки під час планування охорони та оборони військових частин (об'єктів):

– визначати основні просторово-часові характеристики дій противника та елементів безпосередньої охорони;

– визначати можливість проведення атаки противника черговими силами;

– прогнозувати своєчасність дій елементів безпосередньої охорони.

Тобто, розроблена просторово-часова модель дає змогу для визначення можливості своєчасної протидії противнику силами і засобами спостережного поста підрозділу охорони.

Отже, мету даної слід вважати досягнутою.

У подальшому представлена просторово-часова модель визначення можливості своєчасної протидії противнику силами і засобами спостережного поста підрозділу охорони може бути удосконалена за рахунок інтеграції даних, що отримуються від геоінформаційних систем, та використана як можлива складова частина методики з визначення оптимального складу сил та засобів охорони та оборони у військових частинах та органах військового управління в ході завчасного планування. Тобто, на підставі використання більш точних оціночних даних місцевості, тактико-технічних характеристик сил та засобів спостережного поста та підрозділу охорони, характеристик розміщення об'єкта охорони, а також імовірних тактико-технічних характеристик сил та засобів противника, можливо буде визначати райони посиленої уваги, в межах яких визначати цілі особливої важливості. У межах цих районів,

при заданих вихідних даних та умовах, можуть визначатись рубежі, на яких противник імовірно буде зупинений (атакований, заблокований, придушений і т. ін.).

Також даний інструмент може бути впроваджений в навчальний процес з метою розвитку у тих, хто навчається, аналітично-прогностичних здібностей для прийняття обґрунтованих та своєчасних рішень з використанням засобів імітаційного моделювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. СТП 11.033.01.01.4.05-2014 (01). Охорона та оборона важливого об’єкта. Центр оперативних стандартів і методики підготовки Збройних Сил України. 2014. 98с.

2. Про затвердження Порядку організації охорони об’єктів державної авіації: наказ Міністерства оборони України від 21.03.2016 № 152.

3. Про затвердження Інструкції з організації охорони державних повітряних суден та аеродромів Повітряних Сил Збройних Сил України: наказ Командувача Повітряних Сил Збройних Сил України від 22.11.2019 № 176.

4. Про затвердження Інструкції з організації і несення патрульної служби в окремо розташованих підрозділах Повітряних Сил Збройних Сил України: наказ Командувача Повітряних Сил Збройних Сил України від 15.06.2006 № 185.

5. ВП 3-01(02-08, 22-34) 01. Організація і здійснення охорони та оборони, повсякденної діяльності військових частин (підрозділів) Збройних Сил України, які розташовані у базових таборах. Центр оперативних стандартів і методики підготовки Збройних Сил України. 2018. 98 с.

6. ВП 3-01(02-08, 22-34) 03.01. Методичні рекомендації з організації і здійснення охорони та оборони, повсякденної діяльності військових частин (підрозділів) Збройних Сил України, які розташовані у базових таборах (за досвідом проведення ООС (раніше АТО)). Центр оперативних стандартів і методики підготовки Збройних Сил України. 2018. 98 с.

7. Про затвердження Положення про сторожову охорону та Інструкції з організації та несення служби сторожовою охороною: наказ Міністерства оборони України від 25.10.2016 № 561.

8. Методичний посібник щодо організації та здійснення охорони та оборони, повсякденної діяльності військових частин (підрозділів) Збройних Сил України, які розташовані у базових таборах. Затверджено ТВО НГШ – Головнокомандувачем ЗС України, липень 2018 р. 61 с.

9. Охорона та оборона баз. Тактика, методи (прийоми) та процедури. Центр узагальнення досвіду Сухопутнихвійськ США. Форт Левенворт КС 66027-1350. Управління військового співробітництва та миротворчих операцій Командування Сухопутних військ збройних Сил України. № 07–09, березень 2007 р. 69 с.

10. Таран І. А., Пугач В. В., Коцюба В. П. Імітаційна статистична модель процесу охорони периметра об’єкта // Системи озброєння і військова техніка. 2010. № 2 (22). С. 204–207.

11. Орлов М. М., Марущенко А. А. Методика обчислення сил охорони особливо важливих державних об’єктів // Системи озброєння і військова техніка. 28.09.2005. С. 58–65.

12. Городнов В. П., Репіло Ю. Є. Модель визначення чисельності особового складу, необхідного для вирішення завдань військовою частиною Національної гвардії України з охорони важливого державного об’єкта в особливий період // Честь і закон. 2019. № 2 (69). С. 4–9.

13. Городнов В. П., Репіло Ю. Є., Лазебник С. В. Методика розрахунку необхідної чисельності особового складу для виконання завдань з охорони важливого державного об’єкта в особливий період // Честь і закон. 2019. № 4 (71). С. 23–28.

14. Трембовецький О. Г., Гулеватий Д. Ю. Методика роботи штабу прикордонного загону щодо пошуку і ліквідації диверсійно-розвідувальних груп противника // Наука і техніка Повітряних Сил Збройних Сил України. 2018. № 4 (33). С. 119–127.

15. Телелим В. М., Шевчук В. В., Баргилевич А. В. Методичний підхід до визначення пріоритетності важливих об’єктів в зоні територіальної оборони, охорона та оборона яких покладається на формування територіальної оборони держави // Наука і техніка Повітряних Сил Збройних Сил України. 2020. № 4 (41). С. 37–43.

16. Застосування системи імітаційного моделювання «Follow Me»: навч.-метод. посіб. / Д. В. Антонов, А. М. Коваленко та ін. Х.: ХНУПС, 2021. 148 с.

17. Про затвердження Тимчасового порядку оформлення оперативних (бойових) документів: наказ Головнокомандувача Збройних Сил України від 11.09.2020 № 140.

DOI: 10.58254/viti.3.2023.15.128

УДК 621.391; 004.942

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 Бєляков Р. О. ORCID: 0000-0001-9882-3088 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ТОЧНОСНИХ ХАРАКТЕРИСТИК НАВІГАЦІЙНИХ СИСТЕМ МІКРОКЛАСУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У статті проведено аналіз впливу шумів основних видів, які виникають у процесі обміну навігаційною інформацією між GPS-приймачем мікрокласу безпілотного літального апарата та глобальною системою супутникової навігації за допомогою вдосконаленої розширеної імітаційної моделі в програмному середовищі Matlab – Simulink, що дозволяє побудувати репрезентативну статистичну модель у процесі проєктування алгоритмів навігаційної системи безпілотних літальних апаратів.

За допомогою моделювання процесу вибору коефіцієнта підсилення антени приймача безпілотного літального апарата та дослідження впливу якості прийому та обробки навігаційних сигналів під час збільшення відстані відносно супутникового сигналу глобальної навігаційної супутникової системи було встановлено, що зі збільшенням коефіцієнта підсилення антени рівень шуму зменшується. Однак підвищення коефіцієнта підсилення призводить до збільшення габаритних параметрів антени, а також, відповідно, підвищення енергоспоживання, що не задовольняє вимогам щодо масо-габаритних показників мікрокласу безпілотних літальних апаратів.

Також, у статті було досліджено процес роботи мікроелектромеханічних систем безплатформних інерційних навігаційних систем, а саме в момент зникнення глобальних супутникових систем на часовому інтервалі до 300 секунд, для визначення похибки обчислення параметра вертикальної компоненти (висоти) та вертикальної швидкості безпілотного літального апарата. За результатом моделювання було встановлено: орієнтація і навігація безпілотних літальних апаратів в автономному польоті істотно залежать від випадкових похибок мікроелектромеханічних систем безплатформних інерційних навігаційних систем, до них відносяться випадкове блукання кута (шумовий дрейф нуля);вплив лінійного прискорення датчика акселерометра, шляхом дослідження шумової моделі похибок мікроелектромеханічних систем на визначення параметра height velocity в автономному режимі польоту, який має суттєвий характер.

Ключові слова: *БпЛА, глобальна навігаційна супутникова система, GPS, безплатформна інерціальна навігаційна система, мікроелектромеханічна система*.

O. Fesenko, V. Ostapchuk, R. Bieliakov Analysis of navigation system accuracy characteristics for micro UAVs.

The article analyzes the noise influence of the main types that arise in the process of exchanging navigational information between the GPS receiver of an micro-class unmanned aerial vehicle and the global satellite navigation system using an improved advanced simulation model in the Matlab – Simulink software environment, which allows building a representative statistical model in the process designing algorithms of the navigation system of unmanned aerial vehicles.

With the help of modeling the process of choosing the receiver gain factor of an unmanned aerial vehicle and the study of the influence of the quality of reception and processing navigation signals during the increase of the distance relative to the satellite signal of the global navigation satellite system, it was established that with an increase in the gain factor of the antenna, the noise level decreases. However, an increase in the amplification factor leads to an increase in the dimensions of the antenna, as well as, accordingly, an increase in energy consumption, which does not meet the requirements for the mass-dimensional indicators of the microclass of unmanned aerial vehicles.

Also, the article investigated the operation process of microelectromechanical systems of platformless inertial navigation systems, namely, at the moment of the disappearance of global satellite systems at a time interval of up to 300 seconds, to determine the error of calculating the parameter of the vertical component (height) and vertical speed of an unmanned aerial vehicle. According to the simulation results, it was found that the orientation and navigation of unmanned aerial vehicles in autonomous flight depend significantly on random errors of microelectromechanical systems of platformless inertial navigation systems, these include random angle wandering (zero noise drift); the influence of linear acceleration of the accelerometer sensor, by studying the noise model of errors microelectromechanical systems to determine the eight velocity parameter in autonomous flight mode, which is of a significant nature.

Keywords: *UAV, global satellite navigation systems, GPS, platformless inertial navigation system, microelectromechanical system.*

Загальна постановка задачі. Під час російської військової агресії проти України зростає потреба у застосовуванні безпілотних літальних апаратів (далі – БпЛА) в таких задачах, як військова розвідка та ударні дрони, у зв'язку зі зменшенням масо-габаритних параметрів навігаційного та оптико-електронного обладнання. На сьогодні значна кількість завдань вирішується БпЛА злітною масою до 5 кг (клас «мікро») відповідно до міжнародної класифікації UVS International [1; 2]. Переваги цього класу БпЛА полягають в наступних основних характеристиках: дальність польоту до 10 км та максимальна злітна маса до 5 кг. Тенденція масштабування та інтеграції мікрокласу БпЛА у військові та цивільні галузі полягає в зниженні цінової політики на міжнародному ринку та заявленим технологічним показникам, таких як: висока мобільність та здатність до обробки та передачі фото- та відеоінформації в реальному часі.

Однак, якщо говорити в контексті застосування БпЛА у військових цілях, з'являється необхідність розглянути точносні характеристики навігаційних систем мікрокласу в різних умовах функціонування, так як виробники БпЛА, як правило, зазначають показники роботи навігаційних систем наближено до ідеальних умов, що значно впливає на їхнє використання в реальних умовах та підтверджується статистикою втрати БпЛА [3] внаслідок глушіння сигналів GPS.

Тому виникає необхідність дослідити точносні характеристики навігаційних систем з урахуванням впливу невизначеності динамічного середовища, особливо в контексті проєктування та розробки мікрокласу БпЛА.

Аналіз останніх досліджень та публікацій. Основною технологією обчислення параметрів навігаційних систем мікро-БпЛА, є Real Time Kinematic (RTK) [4], що включає сукупність способів отримання планових координат і висот точок місцевості сантиметрової точності за допомогою супутникової системи навігації Differential Global Positioning System (DGPS)/ГЛОНАСС. Однак точність DGPS [5] зменшується при віддаленні приймача від опорного пункту, коли для визначення параметрів позиціювання в процесі роботи навігаційної системи БпЛА не вистачає загального «сузір'я» супутників. Відомо, що RTK має значні функціональні обмеження нормального режиму роботи, а саме при умові, коли видимості одних і тих же GPS-супутників одночасно на базовій станції необхідно не менше 5, що є поширеною ситуацією для функціонування поза зоною прямої видимості БпЛА [5]. У роботі [6] показано вплив іоносферних збурень, які суттєво впливають на точність визначення географічних параметрів систем DGPS.

Так, на сьогодні розробка БпЛА типу квадрокоптер різних передових європейських відомих компаній дозволяють здійснювати точність позиціонування до 10–20 см [7] завдяки використанню двочастотних приймачів у складі бортового обладнання. Однак, вартість таких БпЛА набагато вища, мінімум в 4 рази, ніж вартість інших представлених БпЛА мікрокласу. При цьому приймачі навігаційної системи БпЛА також схильні до втрати і спотворення навігаційного сигналу та не захищені від навмисних завад. Методи підвищення точності позиціонування в разі спотворення/придушення роботи модуля навігаційної системи виробниками не передбачені.

Як правило, у навігаційних системах БпЛА інтегровані датчики мікроелектромеханічних систем (далі – МЕМС) інерціальної навігації, що не залежать від впливу радіоперешкод і можуть називатись повністю автономними. Однак, на сьогодні, реалізовані рішення МЕМС інерціальної навігації не використовуються як основний навігаційний апарат, а застосовуються для корекції сигналу глобальної навігаційної супутникової системи (далі – ГНСС) [8; 9]. Також необхідно зазначити, що як правило всіма виробниками замовчуються точносні характеристики БпЛА при спотворенні/придушенні GPS/ГЛОНАСС. Надана інформація про точність позиціонування відноситься виключно до ідеальних умов.

Метою статті є аналіз точносних характеристик та визначення чинників, що впливають на роботу навігаційних систем мікрокласу БпЛА, для розробки репрезентативної

статистичної моделі інерціальної навігаційної системи з GPS-модулем із урахуванням впливу невизначеного середовища.

Стаття складається з трьох основних розділів: у першому розділі проведено аналіз чинників, що впливають на роботу супутникової системи навігації БпЛА; в другому представлено результат імітаційного моделювання супутникової системи БпЛА мікрокласу із урахуванням математичної моделі шумового впливу; в третьому показано загальний алгоритм роботи допоміжної безплатформної інерціальної МЕМС навігаційної системи з GPS-модулем та проведено аналіз її похибок під час зникнення сигналів ГНСС.

Виклад основного матеріалу.

1. Аналіз чинників, що впливають на роботу ГНСС.

Основними джерелами похибки ГНСС позиціонування БпЛА [10; 11] є такі:

– дані ефемерида: виникнення помилки позиціонування БпЛА обумовлено тим, що місце розташування супутника під час передачі сигналу відомо з точністю від 1 до 5 метрів;

– годинник супутника: кожен супутник має на борту атомний годинник, помилка часу яких в 10 наносекунд, що може впливати на помилку відстані до 3 метрів;

– вплив іоносфери: при проходженні сигналу через іоносферу виникають завмирання сигналу. Рівень іонізації може варіюватися залежно від часу і місця спостереження. Похибка, що вноситься іоносферою, може становити від 2 до 50 метрів;

– ефект тропосфери: найбільший вплив на переданий навігаційний сигнал в тропосфері надають погодні умови: температура, тиск і вологість. Похибки, що вносяться тропосферою, складають близько 1 метра;

– відображення сигналів: помилки обумовлені викривленням відображення сигналу від великих об'єктів (будівель, дерев, гір тощо). Дані похибки становлять близько 1 метра;

– вимірювання приймача: похибки позиціонування, що вносяться приймачем, не перевищують 0,5 метра;

– перешкоди радіорелейних станцій. Випромінювання радіорелейних станцій, в тому числі стільникових операторів, спотворюють навігаційне поле. В результаті в смузі частот навігаційних сигналів формуються найбільш небезпечні для навігаційного приймача полігармонічні перешкоди, що збільшуються при наближенні до джерела перешкоди.

Окремо можна виділити навмисні перешкоди, такі як «спуфінг атаки», суть яких полягає у штучному нав'язуванні хибного місця розташування приймача ГНСС [12].

Також уразливість ГНСС до впливу активного подавлення перешкод обумовлена наступними факторами [12]:

– великою дальністю передачі сигналів (~ 20 000…22 000 км);

– обмеженою потужністю радіосигналу супутника (10…50 Вт);

– малим коефіцієнтом підсилення антени супутникового передавача (не перевищує 10–15 дБ).

– потужність радіосигналу супутника змінюється в діапазоні (P_{sat}) = {10…50} Вт;

– коефіцієнт підсилення антени супутникового передавача (G_{sat}) ≥{10…15} дБ.

У загальному вигляді джерела похибок, що впливають на точність позиціонування БпЛА, представлені на блок-схемі рисунку 1.

Рис. 1. Джерела похибок в супутниковому каналі зв'язку

2. Імітаційне моделювання системи навігації мікро-БпЛА.

Для аналізу впливу вище зазначених похибок ГНСС у процесі визначення навігаційних параметрів позиціонування мікро-БПЛА застосовується імітаційна модель Matlab – Simulink (GPS Sensor Noise to Multirotor Guidance Model l) (рис. 3, 4) [13], яка дозволяє моделювати навігаційні системи БпЛА мікрокласу. Для об'єднання даних навігаційних параметрів GPS та інерціальної навігаційної системи використовується типовий Fusion алгоритм Калмана.

На рисунку 2 у загальному вигляді представлена блок-схема навігаційної системи, що застосовується на рівні програмного апаратного рішення в БпЛА мікрокласу.

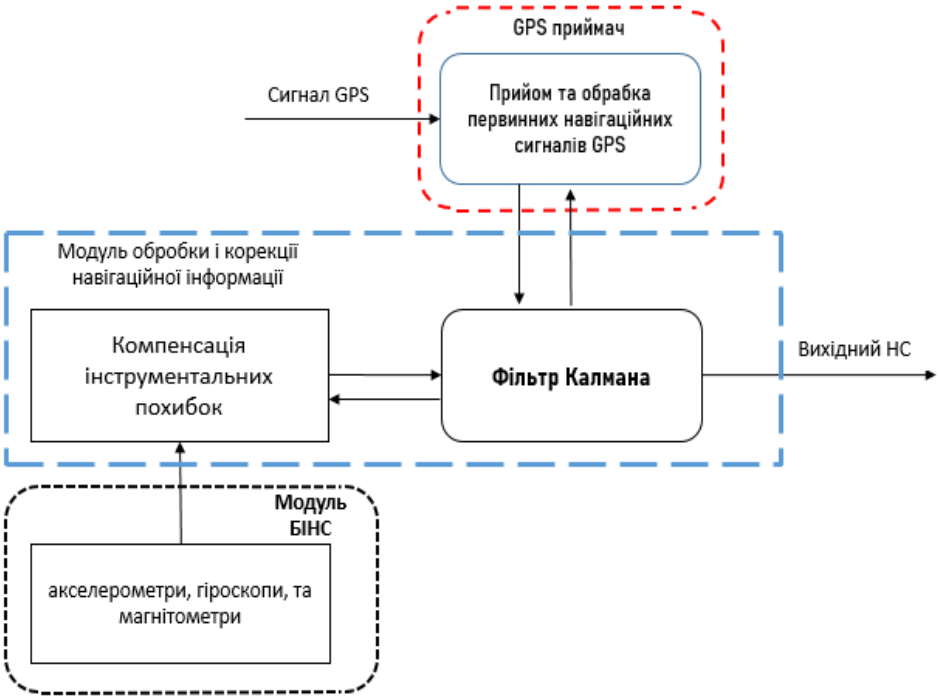


Рис. 2. Структурна схема типової навігаційної системи БпЛА мікрокласу

У дослідженні особлива увага акцентується на впливі шуму під час визначення похибки обчислення параметра вертикальної компоненти (висоти) та вертикальної компоненти швидкості БпЛА, так, зазвичай, науковцями досліджується загальна похибка на визначення навігаційних параметрів траєкторії довгота ***(Longitude),*** широта ***(Latitude)*** у двомірному просторі, що не дозволяє побудувати репрезентативну статистичну модель у процесі проєктування алгоритмів навігаційної системи БпЛА.

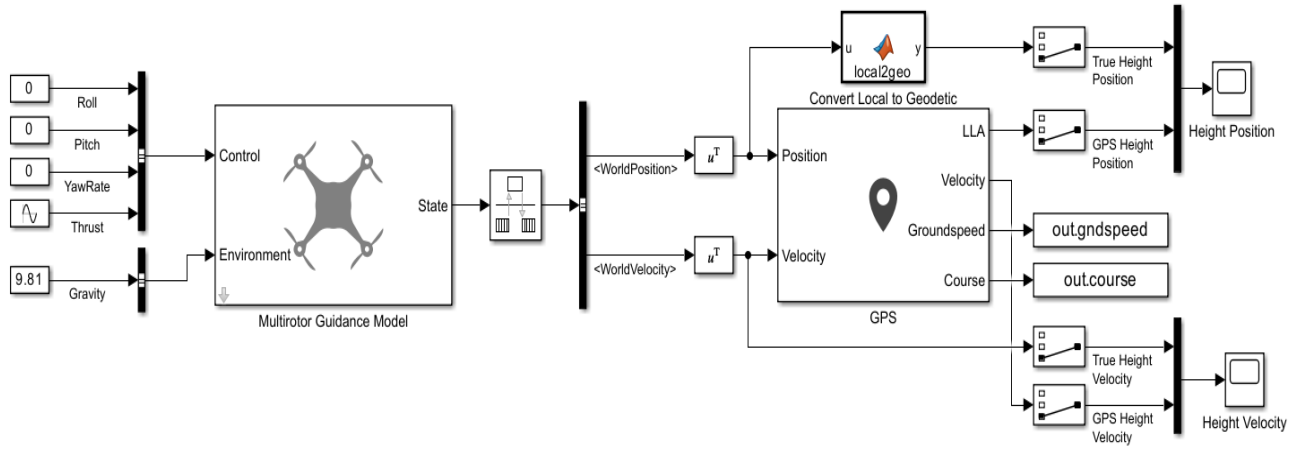


Рис. 3. Модель навігації БпЛА роторного типу

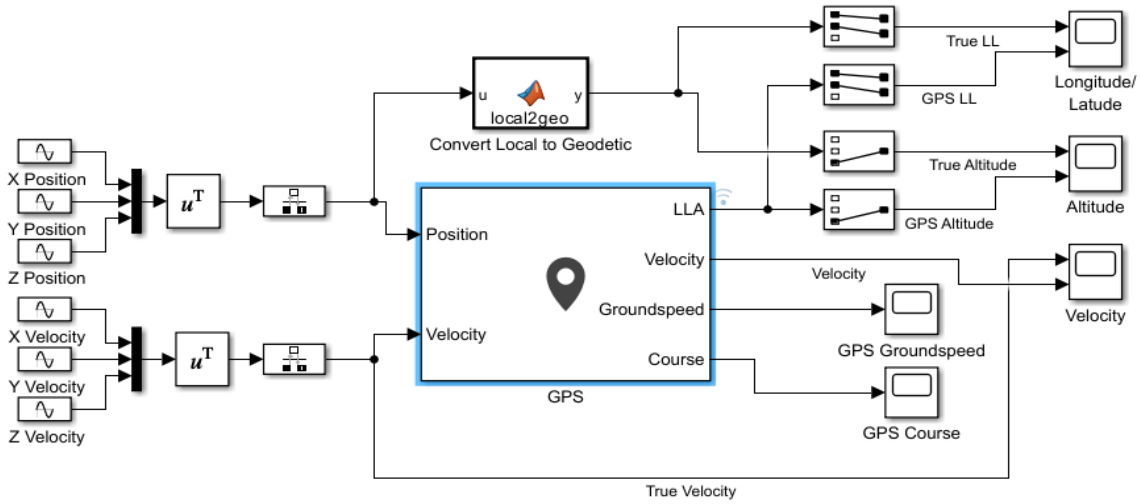


Рис. 4. Імітаційне моделювання шумових характеристик GPS

Фізико-математична інтерпретація моделі БпЛА являє собою вільне, тверде тіло, тобто точку в просторі, яке має шість ступенів свободи, динамічний рівень руху обумовлюється як центр мас відносно траєкторної системи координат, що наведено в системі рівняння (1):

$$\begin{cases} m\,\dot{V} = \sum F_{x_t}, \\ mV\dot{\vartheta} = \sum F_{y_t}, \\ -mV\dot{\varphi}\cos(\vartheta) = \sum F_{z_t} \end{cases}, \tag{1}$$

де m – сила тяжіння;

$\dot{V}$ – параметр швидкості;

F – сила тяги;

x' – сила опору;

y' – підйомна сила;

z' – бокова сила (моделюється як апроксимаційна функція для імітації впливу динамічного середовища, будується за законом нормального розподілу);

$\dot{\varphi}$ – керуючий параметр курсу БпЛА;

ϑ – тангаж.

Вхідні дані для імітаційного моделювання БпЛА в середовищі програмування Matlab – Simulink:

швидкість - V(БпЛА) = 25 м/с;

час польоту – t(БпЛА) = 10 хв;

висота - h(БпЛА) = 1000 м;

час дискретизації – Δt*(GPS/БпЛА) = 5 Hz.*

Математична модель оцінки впливу шуму на GPS-приймач БпЛА при обмеженні потужності радіосигналу супутника повинна враховувати наступні основні параметри та характеристики:

– *потужність радіосигналу – змінюється в діапазоні* (P_{sat}) = {10...50} Вт;

– *коефіцієнт підсилення антени* (G_{sat}) ≥{10…15} дБ;

– *термічний шум (N) – обумовлений температурою та шириною смуги пропускання, обчислюється як:* $Nsd\ (dBHz) + 10log\ 10\ (B)$.

На першому етапі необхідно визначити функцію відношення сигнал/шум (SNR) на вході GPS-приймача за допомогою наступного виразу (2):

$$SNR(GPS) = \frac{(P_{sat}G_{sat}G_{rx})}{N}, \quad (2)$$

де G_{rx} – коефіцієнт підсилення антени GPS-приймача;

N – термічний шум.

Однак, для врахування впливу спектральної щільності адитивного шуму, що наведено в рівнянні (6) [13] та потужності сигналу на вході антени приймача, необхідно адаптувати математичну модель із визначенням одиниць виміру (дБ) з наступними параметрами:

– *спектральною щільністю адитивного шуму* N_{sd} *– варіюється* {-200…-210} дБ Вт;

$$N(db) = N_{sd}(dbHz) - \log 10\ (B), \quad (3)$$

де B – ширина пропускання смуги приймача в Гц;

– *потужністю сигналу на вході антени:*

$$P_{sat}(db) = \log 10\ (P_{sat}); \quad (4)$$

– *мінімальним співвідношенням сигнал/шум* $SNR(min)$ *– варіюється* {-20...22} дБ Гц:

$$N_{sd}(dbHz) = N_{sd} - P_{rx}\ ; \quad (5)$$

– *спектральною щільністю адитивного шуму:*

$$N_0 = FkT, \quad (6)$$

де k – стала Больцмана ($1{,}38 \cdot 10^{-3}$);

T – температура в Кельвінах;

F – шум-фактор.

Після перетворень функцію SNR можна представити з урахуванням вище зазначених параметрів, як показано в рівнянні (7):

$$SNR(GPS)=P_{sat}+G_{sat}+G_{rx} - N. \quad (7)$$

Для моделювання процесу шумового впливу на приймач GPS БпЛА необхідно ввести обмеження (8):

$$SNR(GPS) \geq SNR(\min). \quad (8)$$

Результат моделювання роботи глобальної супутникової системи та приймача GPS представлено на прикладі мультироторного квадрокоптера мікрокласу БпЛА протягом польоту t = 10 хвилин із урахуванням математичної моделі шумового впливу, що показано на графіках (рис. 5–11).

Для оцінки результату моделювання алгоритмів навігаційної системи БпЛА використовується популярна метрика похибок root mean square error (RMSE).

На графіку (рис. 5) показано процес зміни мінімального співвідношення сигнал/шум залежно від спектральної щільності адитивного шуму. Математично – функція, що описує мінімальне значення SNR, при якому GPS-приймач задовольняє критеріям щодо процесу обміну даними в реальному часі. На графіку видно, що зі збільшенням спектральної щільності шуму мінімальний SNR збільшується, тому GPS-приймач БпЛА стає менш чутливим до сигналів глобальної навігаційної супутникової системи.

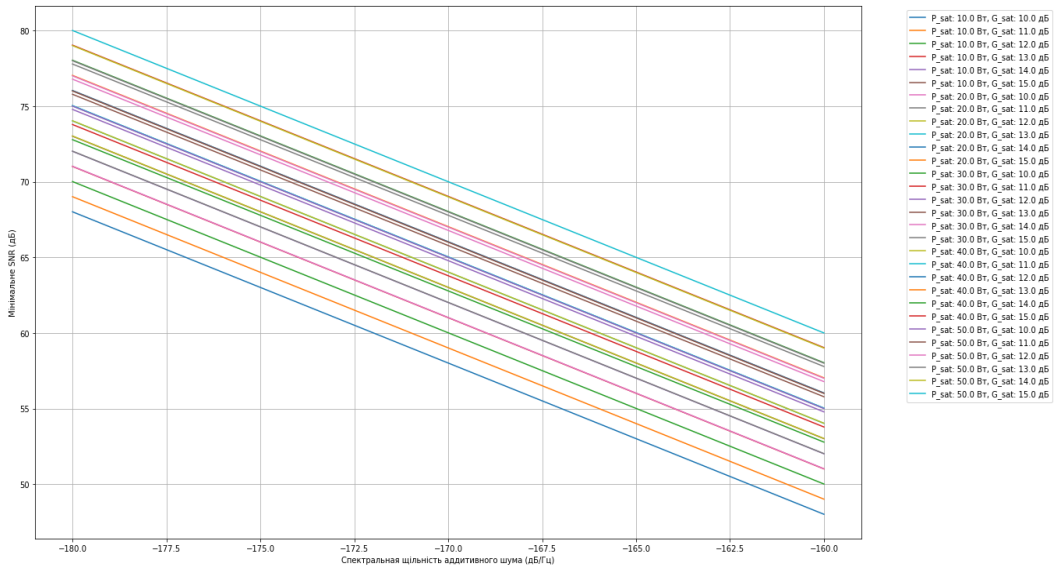


Рис. 5. Залежність мінімального SNR від спектральної щільності адитивного шуму

На графіку (рис. 6) показано кореляцію вибору коефіцієнта підсилення антени приймача БпЛА *Gr(x)* на вплив якості прийому та обробки навігаційних сигналів під час збільшення відстані відносно супутникового сигналу ГНСС. На графіку показано, що зі збільшенням коефіцієнта підсилення антени рівень шуму зменшується. Однак необхідно зазначити, що підвищення коефіцієнта підсилення призводить до збільшення габаритних параметрів антени, а також відповідно підвищення енергоспоживання, що не задовольняє вимогам масо-габаритних показників мікрокласу БпЛА.

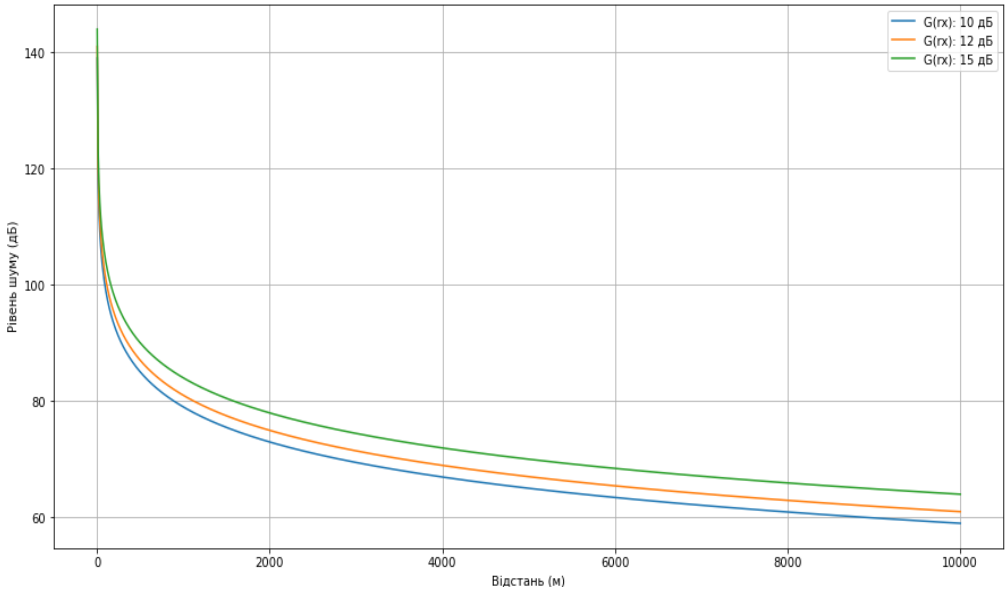


Рис. 6. Залежність рівня шуму (RMSE) від коефіцієнта підсилення GPS-приймача БпЛА

Нижче наведено результат імітаційного моделювання (див. рис. 5) середньоквадратичної помилки позиціонування БпЛА відносно впливу спектральної щільності адитивного шуму, значення якого варіюється в діапазоні від -200 дБВт до -210 дБВт. Із графіку видно, що за умови збільшення спектральної щільності шуму помилка позиціонування також збільшується.

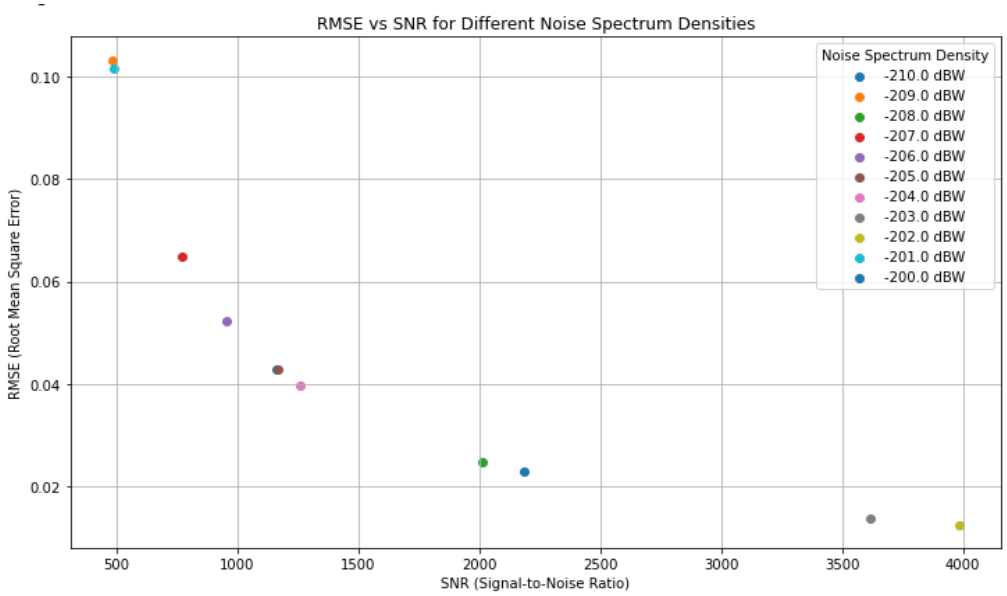


Рис. 7. Залежність середньої квадратичної помилки (RMSE) від спектральної щільності

На графіку (рис. 8) показано результат впливу шуму процесу обчислення помилки визначення навігаційного параметра вертикальної компоненти позиціювання *GPS height position* БпЛА відносно еталонного параметру – позначено червоною лінією *True GPS height position*. Із графіків видно, що із часом траєкторія БпЛА значно відхиляється від еталонної траєкторії, відхилення якої складає ≈ 2.12…1.9 м (табл. 1), що може свідчити про підвищення енергоспоживання під час стабілізації курсу і в результаті зменшення реального розрахункового параметру – часу дальності польоту.

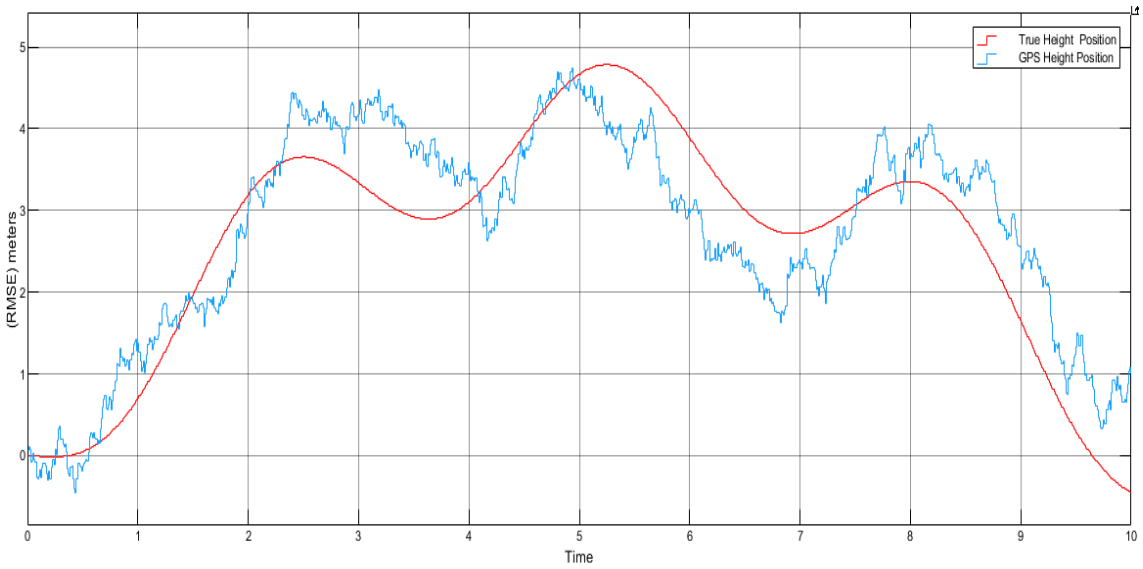


Рис. 8. Обчислення помилки в процесі визначення навігаційного параметра вертикальної компоненти позиціювання GPS *height position* БпЛА

На графіку (рис. 9) показано результат обчислення помилки географічних параметрів позиціювання БпЛА *Longitude, Latitude* відносно еталонних параметрів *true Longitude, true Latitude*. Із графіку видно, що відхилення географічних параметрів відносно невелике і складає ≈ -0.507…0.88 м (табл. 1).

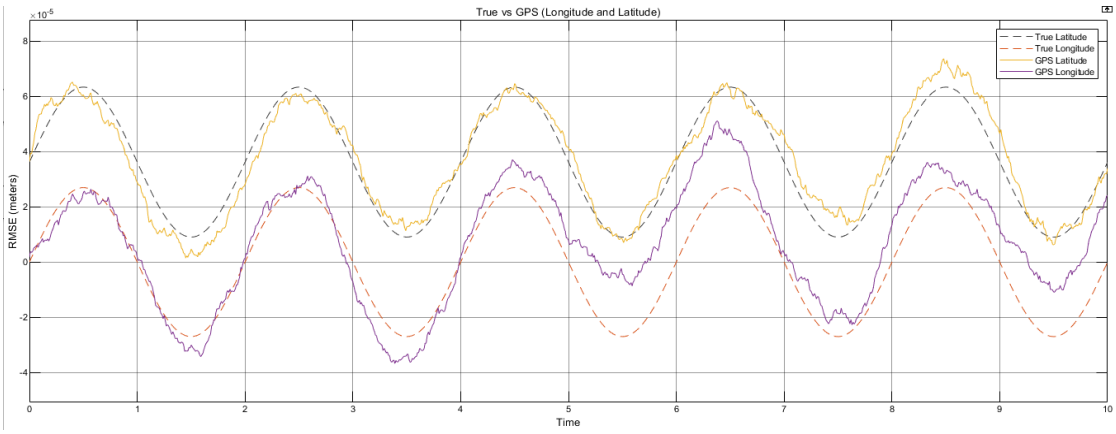


Рис. 9. Обчислення помилки в процесі визначення навігаційних параметрів позиціювання БпЛА *Longitude, Latitude*

На графіку (рис. 10) показано результат обчислення помилки географічних параметрів позиціювання висоти *Altitude* БпЛА відносно еталонних параметрів *true Altitude*. Із графіку видно, що відхилення географічного параметру відносно еталонних складає ≈ -2.2…2.4 м (табл. 1), що відповідно свідчить про суттєвий вплив шуму на GPS-приймач БпЛА під час визначення параметрів вертикальної компоненти.

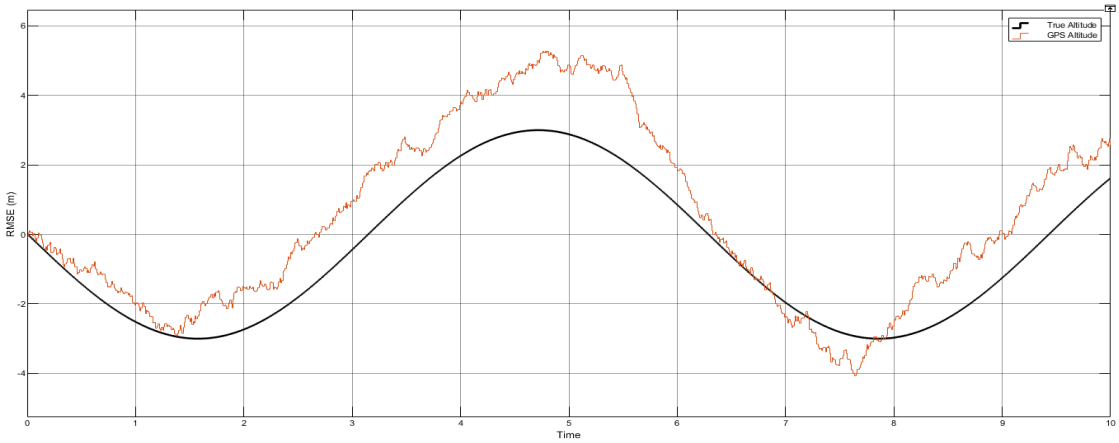


Рис. 10. Обчислення помилки в процесі визначення навігаційного параметра вертикальної компоненти позиціювання *Altitude* БпЛА

На графіку (рис. 11) показано результат обчислення помилки навігаційних параметрів позиціювання БпЛА вертикальної швидкості *Height velocity* відносно еталонних параметрів *true Height velocity*. Із графіку видно, що суттєве відхилення географічних параметрів складає ≈ -2.1…1.60 м (табл. 1).

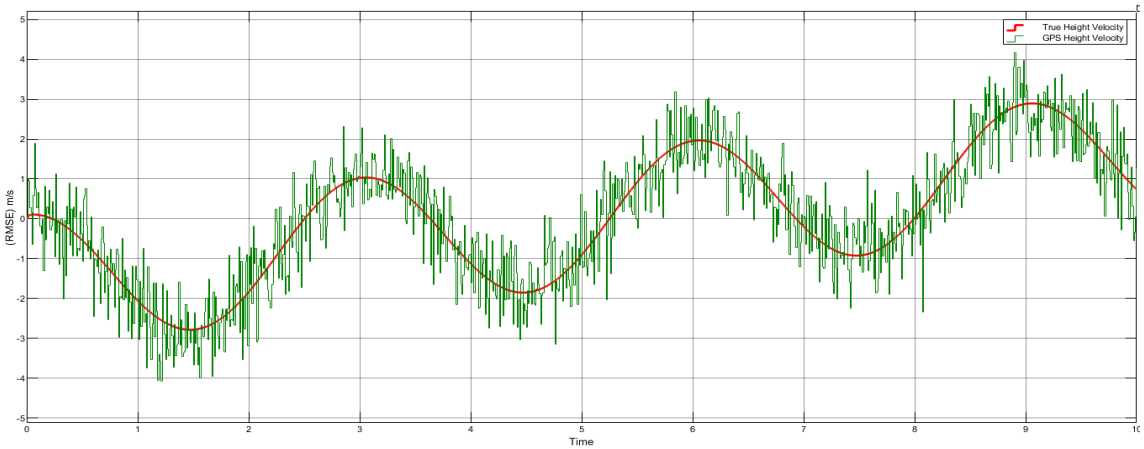


Рис. 11. Обчислення помилки в процесі визначення навігаційного параметра вертикальної компоненти швидкості *height velocity* GPS БпЛА

Таблиця 1

Похибки обчислення навігаційних параметрів позиціювання БпЛА

Географічні параметри траєкторії БпЛА	Похибка RMSE позиціювання БпЛА відносно еталонних параметрів
Latitude (широта)	≈ -0.507…0.60 (м)
Longitude (довгота)	≈ -0.57…0.88 (м)
Altitude (висота)	**≈ -2.2…2.4 (м)**
Height position	**≈ -2.42…1.9 (м)**
Height velocity	**≈ -2.1…1.60 (м)**

Таким чином, результат застосування вище зазначеної (≈ -2.2…2.4 м; -2.42…1.9 м, -2.1…1.60 м) математичної моделі для оцінки впливу шуму показав, що значну похибку навігаційна система БпЛА отримує в процесі визначення вертикальної компоненти: *altitude (висота), height position, height velocity*, що свідчить про підвищення енергоспоживання під час стабілізації курсу і зменшення реального розрахункового параметру, такого як час польоту. Також це може призвести до зменшення польотного завдання чи втрати БпЛА.

3. Робота алгоритму БІНС на основі МЕМС.

Додатковою системою позиціонування БпЛА є використання БІНС на основі МЕМС. Аналіз досліджень і розробок в області БІНС на основі МЕМС показав, що розвиток технології МЕМС спрямований на покращення точносних і тимчасових характеристик [15]. Однак як відомо в [16], БІНС на основі МЕМС, інтегрованих в системах мікро-БПЛА, має істотний недолік – зашумленість датчиків, яка збільшується в часі, що не дозволяє використовувати БІНС на основі МЕМС без допомоги ГНСС в якості основної навігації.

Класичний алгоритм БІНС містить модуль чутливих елементів: тріаду акселерометрів і тріаду датчиків кутової швидкості (гіроскоп). Структурна схема алгоритму БІНС представлена на рисунку 12, де БЧЕ – блок чутливих елементів (тріада датчиків кутової швидкості і тріада акселерометрів); $\vec{f}_B$ – вектор обчислення даних прискорення показників акселерометрів відносно локальної системи координат БпЛА; $\vec{f}_G$ – вектор прискорення на осі географічного тригранника, обчислений на основі проєкцій вектора$\vec{f}_B$; G_G^B – матриця направляючих косинусів, що показує взаємну орієнтацію локальної системи координат і географічного тригранника; $\vec{V}$ – лінійна швидкість об'єкта відносно глобальної системи координати Землі; $\vec{a}_E = \vec{\omega}_G\vec{V} - \vec{U}\vec{V}$ – коріолісове прискорення; $\vec{\omega}_G$ – абсолютна кутова швидкість географічного тригранника в проєкціях осі $R,\cdot\, \phi;\cdot\, R\lambda$ – радіуси Еліптичної моделі Землі; $\vec{U}$ – кутова швидкість добового обертання Землі, прискорення вільного падіння; $\vec{\omega}_B$– обчислення абсолютної кутової швидкості БпЛА, розрахована з показників датчика гіроскопа; $\vec{\omega}_B, \vec{\omega}_G$ – кососиметричні матриці відповідних векторів, $\vec{\omega}_B, \vec{\omega}_G;\cdot\, \varphi,\ \lambda,\cdot\, h$ –широта, довгота і висота центру мас об'єкта;$\cdot\, H,\ \theta,\ \gamma$ –– географічний курс, кут тангажу і кут крену відповідно; $E,\ N,\ Up$ – відповідають східній, північній та вертикальній осям географічного тригранника.

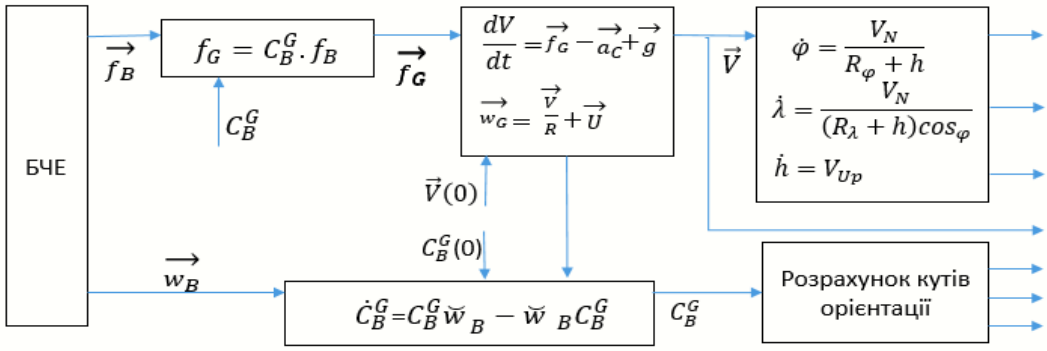


Рис. 12. Структурна схема алгоритму БІНС

У загальному вигляді процес роботи БІНС складається з наступних етапів:

1) обчислення абсолютної кутової швидкості об'єкта та даних прискорення за допомогою датчиків кутової швидкості (гіроскопа) і акселерометра;

2) побудова матриці переходу відносно географічного тригранника;

3) перерахунок показань акселерометрів на осі географічного тригранника;

4) інтегрування прискорень для визначення швидкості;

5) інтегрування отриманої швидкості для визначення координат (позиціонування) БпЛА.

Аналіз похибок безплатформної інерціальної МЕМС навігаційної системи. БІНС забезпечує безперервне обчислення інформації про курс, визначення координат, параметрів швидкості руху і кутової орієнтації платформи БпЛА. МЕМС дозволяють отримувати всю сукупність необхідних параметрів для управління об'єктом, включно з кутами орієнтації. При цьому типові системи повністю автономні, тобто для їх нормального функціонування не потрібно використання будь-якої інформації від інших систем, за винятком початку роботи, коли потрібно задати початкові умови за координатами і проєкцію швидкості.

Однак відомо [17], що похибка координати мікро-БпЛА в момент зникнення ГНСС на часовому інтервалі t = {1..5} хв в автономному режимі польоту може становити ≤ 550 м відхилення від цільової траєкторії. Особливо критично для коректної роботи МЕМС – це наявність в структурі похибок складових навігаційної системи БІНС, в період кореляції близький до періоду зникнення сигналу ГНСС (від 10 с до 300 с), при цьому алгоритм управління БпЛА в автономному режимі, як правило здійснює аварійну посадку, або здійснює розворот з використанням навігаційних параметрів БІНС в зону задовільного функціонування ГНСС з подальшою спробою виходу із зони спотворення/придушення, або відбувається втрата БпЛА.

Величина похибки координат БІНС на основі МЕМС, що вносяться гіроскопом, акселерометром під час автономного польоту БпЛА, розраховується на основі формул швидкої експрес-оцінки, отриманих в роботі [17] (табл. 2, 3).

Нижче наведені таблиці 2, 3, в яких представлено аналітичний розрахунок похибок датчиків МЕМС для моделювання процесів впливу динамічного середовища на визначення параметрів позиціонування БпЛА.

Таблиця 2

Вхідні параметри моделювання похибок МЕМС датчика гіроскопа БІНС

Види похибок гіроскопа	**Похибка координат** $\sigma_{\Delta x}^{gyro}$, м
Систематична складова $\sigma_{syst}^{gyro} = 4$, град/год	$\frac{g \cdot \sigma_{syst}^{gyro}, t^3}{6} = 856$
Нестабільність нуля гіроскопа (флікер шум), $\sigma_{BI}^{\Delta\omega} = 10$ град/год, *(при часовій кореляції* $T_c^{\Delta\omega} = > 1000$ *с)*	$\frac{3}{\sqrt{126}} \frac{g \cdot \sigma_c^{\Delta\omega}}{\sqrt{T_c^{\Delta\omega}}} t^{5/2} = 190$
Похибка масштабного коефіцієнта σ_{syst}^{gyro} ⍰ $= 4, \%$	$\sigma \frac{g \cdot \sigma_{\Delta k}^{gyro}, \dot{v}t^3}{600} = 11{,}6$
Випадкове блукання кута, $ARM = 0{,}2$ град/$\sqrt{r}$	$\frac{ARM}{2\sqrt{5}} t^{5/2} = 190$ $\frac{ARM}{2\sqrt{5}} t^{5/2} = 190$

Таблиця 3

Вхідні параметри моделювання похибок МЕМС датчика акселерометра БІНС

Види похибок акселерометра	**Похибка координат** $\sigma_{\Delta V_{XG}}^{scc}$, м
Систематична складова $\sigma_{syst}^{acc} = 10^{-3}, м/с^2$	$\frac{\sigma_{syst}^{acc} t^2}{2} = 45$
Похибка масштабного коефіцієнта $\sigma_{\Delta X}^{gyro} = 0{,}01, \%$	$\frac{\sigma_{syst}^{acc} \dot{V}_x t^2}{200} = 0{,}45$
Випадкове блукання кута, $1 \cdot /10^{-3}$ м/с^2/$\sqrt{Гц}$	$\frac{1}{\sqrt{3}} VRM \cdot / t^{3/2} = 3{,}3$
Нестабільність нуля (флікер шум), $\sigma_{BI}^{\Delta\omega} = 10^{-4} м/с^2$, *(при часовій кореляції* $E_c^{\Delta\omega} > 1000\ с$*)*	$\frac{3}{\sqrt{126}} \sigma_{BI}^{\Delta\omega} \frac{1}{\sqrt{T_c^{\Delta a}}} t^{5/2} = 15{,}3$

Як правило, у багатьох реалізаціях БІНС мікро-БпЛА застосовують класичні рішення алгоритмів фільтрації на основі Калмана, автори роблять припущення [18], що похибка прискорення руху присутня тільки на короткому інтервалі часу, однак на практиці в реальних умовах польоту БпЛА вплив вище зазначених похибок (табл. 3) є константою.

На графіках (рис. 13) показано результат обчислення датчиком акселерометра даних лінійного прискорення із урахуванням шумового впливу. Із графіку видно, що дані лінійного прискорення відмінні від даних з гравітаційною константою, що призводить до суттєвих похибок на визначення навігаційних параметрів позиціонування, а саме висоти та відповідно відхилення кута курсу БпЛА від цільової траєкторії в автономному режимі польоту, які зростають із часом.

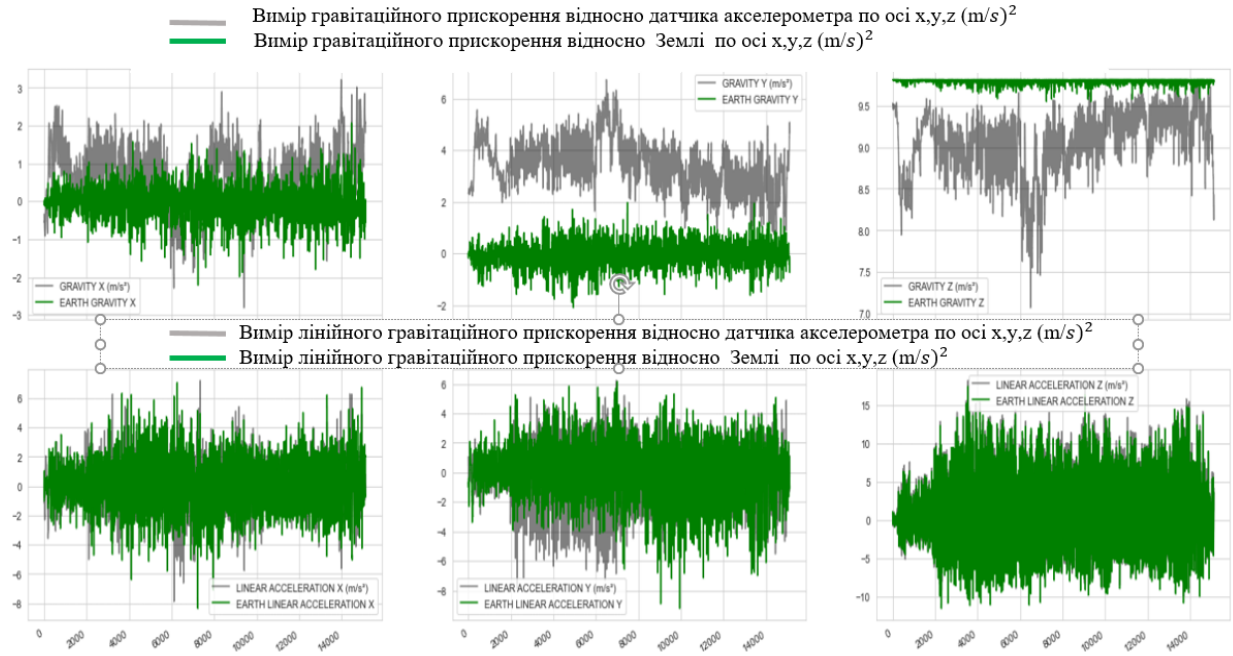


Рис. 13. Обробка даних прискорення МЕМС трьохосьового датчика акселерометра БІНС

Тому необхідно враховувати вплив шумів, які наведені в таблиці 3, на моделювання процесу роботи БІНС, а саме в момент зникнення сигналів глобальних супутникових систем на часовому інтервалі до 300 секунд, на визначення похибки обчислення параметра вертикальної компоненти (висота) та вертикальної швидкості БпЛА, що дозволить досліджувати вплив середовища при проєктуванні та розробки БпЛА мікрокласу.

Вхідні дані для імітаційного моделювання БІНС на основі МЕМС мікро-БпЛА в середовищі програмування Matlab – Simulink (рис. 14):

швидкість – V(БпЛА) = 25 м/с;

час польоту – t(БпЛА) = 10 хв;
час автономного польоту (зникнення GPS-сигналів) t = 300 с;
висота – h(БпЛА) = 1000 м;
час дискретизації – Δt(GPS БпЛА) = 5 Hz;
час дискретизації датчиків інерціальної системи навігації – Δt(IMU – БпЛА) = 50 Hz.

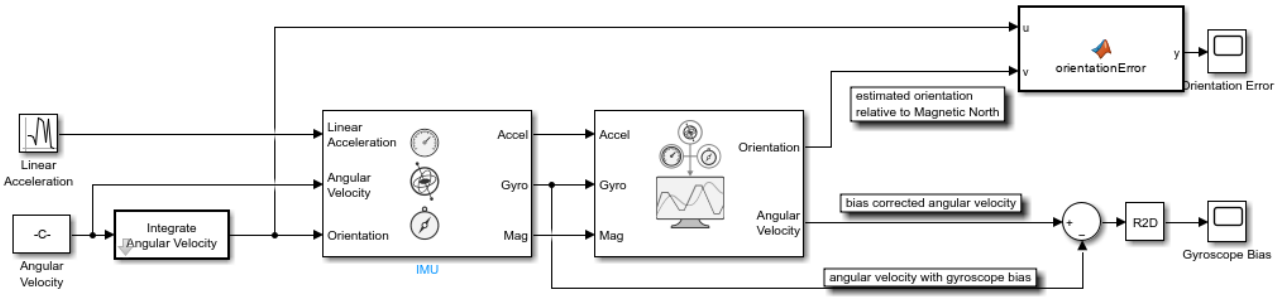


Рис. 14. Модель Simulink БІНС БпЛА

На графіку (рис. 15) показано результат моделювання шумового впливу на визначення параметра вертикальної швидкості позиціювання БпЛА в площині z-компоненти, оцінка здійснювалась відносно еталонних параметрів *true height velocity* в автономному режимі польоту під час зникнення ГНСС. Із графіку видно, що вплив лінійного прискорення датчика та шумової моделі похибок МЕМС акселерометра є суттєвим і складає ≈ 11.2…20.9 м.

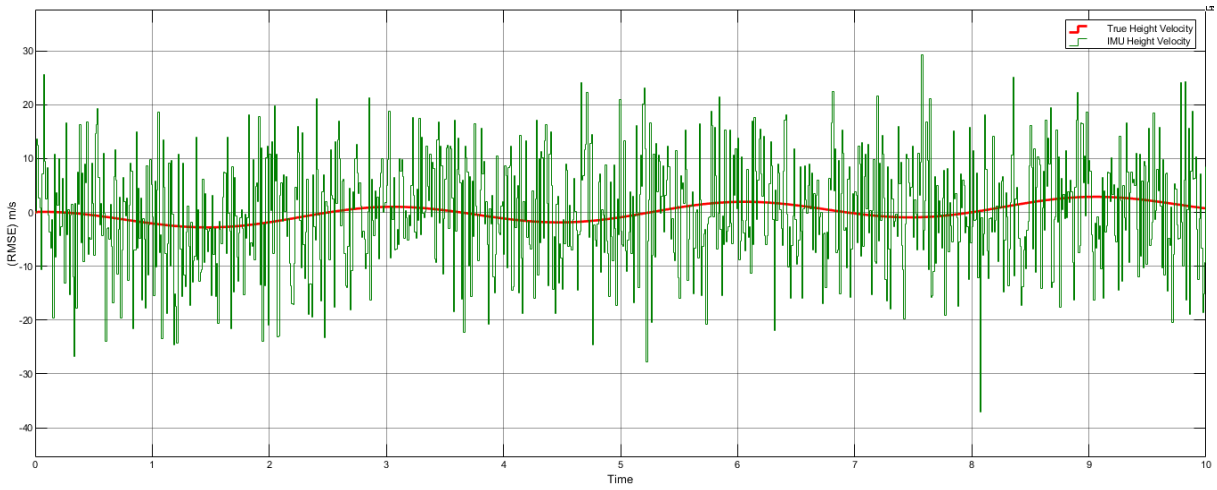


Рис. 15. Обчислення помилки МЕМС у процесі визначення навігаційного параметра вертикальної компоненти швидкості БпЛА

На графіку (рис. 16) показано результат моделювання шумового впливу на визначення параметра позиціювання *altitude* БпЛА, оцінка здійснювалась відносно еталонних параметрів *true altitude*, в автономному режимі, а саме під час зникнення сигналів ГНСС, що позначено двома вертикальними червоними лініями в часовому інтервалі з 2-ї хвилини по 6-ту хвилину польоту. Із графіку видно суттєвий вплив шумової моделі похибок МЕМС акселерометра БІНС, який складає ≈ 4.2…4.9 м.

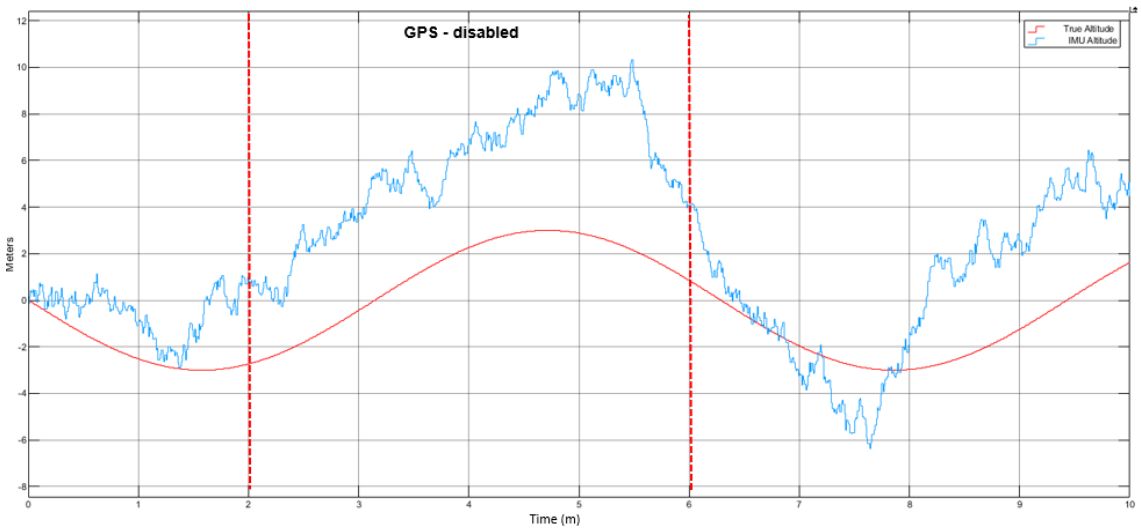


Рис. 16. Обчислення помилки в процесі визначення навігаційного параметра *altitude* вертикальної компоненти позиціювання БпЛА

Таблиця 4

Похибки обчислення навігаційних параметрів позиціонування БпЛА

Географічні параметри траєкторії БпЛА	**Похибка RMSE позиціювання БпЛА відносно еталонних параметрів**
Altitude (висота)	≈ 3.2…4.5 (м)
Height velocity	≈ 11.2…20.9 (м)

Висновок. Таким чином, за допомогою вдосконаленої розширеної математичної моделі в програмному середовищі Matlab – Simulink було досліджено вплив основних видів шумів, які виникають у процесі обміну навігаційною інформацією між GPS-приймачем БпЛА мікрокласу та ГНСС, що дозволяє побудувати репрезентативну статистичну модель у процесі проєктування алгоритмів навігаційної системи БпЛА.

Результат застосування математичної моделі для оцінки впливу шуму показав, що значну похибку навігаційна система БпЛА отримує в процесі визначення вертикальної компоненти: *altitude (висота)* ≈ -2.2…2.4, *height position* ≈ -2.42…1.9, *height velocity* ≈ -2.1…1.60, що може свідчити про підвищення енергоспоживання під час стабілізації курсу і зменшення реального розрахункового параметру – часу польоту. Також це може призвести до зменшення польотного завдання чи втрати БпЛА.

За допомогою моделювання процесу вибору коефіцієнта підсилення антени приймача БпЛА *G(rx)* на якість прийому та обробки навігаційних сигналів під час збільшення відстані відносно супутникового сигналу ГНСС було встановлено, що зі збільшенням коефіцієнта підсилення антени рівень шуму зменшується. Однак необхідно зазначити, що підвищення коефіцієнта підсилення призводить до збільшення габаритних параметрів антени, а також відповідно підвищення енергоспоживання, що не задовольняє вимогам щодо масо-габаритних показників БпЛА мікрокласу.

В результаті дослідження було встановлено:

орієнтація і навігація БпЛА в автономному польоті істотно залежать від випадкових похибок МЕМС датчиків БІНС, до них відносяться випадкові блукання кута (шумовий дрейф нуля до 30 % похибок);

вплив лінійного прискорення датчика акселерометра та шумової моделі похибок МЕМС на визначення параметра *height velocity* в автономному режимі польоту має суттєвий характер і складає ≈ 11.2…20.9 м.

Вище зазначені фактори призводять до помилкового визначення навігаційних параметрів БпЛА, таких як напрямок сили тяжіння, що дає потенційно помилкову оцінку висоти та впливає на точність (до 20 %) побудови траєкторії БпЛА в автономному режимі польоту.

Напрямок подальших досліджень. Для розширення дослідження необхідно побудувати математичну модель із урахуванням впливу динамічного середовища, таких як погодні умови, пориви вітру тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Класифікація UAVs International. URL: http://helpiks.org/6-70010.html.

2. Бєляков Р. О. Моделювання системи розрахунку потреб підрозділів із забезпечення безпілотними літальними апаратами // Системи і технології зв’язку, інформатизації та кібербезпеки. Київ, 2022. Вип. 1 (1). С. 133–138.

3. GPS Signals Are Being Disrupted in Russian Cities 2022. URL: https://www.wired.com/story/gps-jamming-interference-russia-ukraine.

4. Desta Ekaso, Francesco Nex. Accuracy assessment of real-time kinematics (RTK) measurements on unmanned aerial vehicles (UAV) for direct geo-referencing Geo-spatial Information Science Volume 23, 2020 - Issue 2 PP(99):1-15.

5. S. Ögütçü and İ. Kalaycı, “Accuracy and precision of network-based RTK techniques as a function of baseline distance and occupation time,” *Arabian Journal of Geosciences*, vol. 11, no. 13, 2018.

6. Krzykowska, K.; Siergiejczyk, M.; Rosiński, A. Influence of selected external factors on satellite navigation signal quality. In *Safety and Reliability — Safe Societies*; Haugen, S., Barros, A., van Gulik, C., Kongsvik, T., Vinnem, J.E., Eds.; Taylor & Francis Group: London, UK, 2018; pp. 701–705. [Google Scholar] [CrossRef].

7. Aggarwal and Kumar. Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges. Computer Communications, 149 (2020), pp. 270–299, 10.1016/j.comcom.2019.10.014.

8. Xiaoji Niu, Sameh Nassar, Naser El-Sheimy. An accurate land-vehicle MEMS IMU/GPS navigation system using 3D auxiliary velocity updates. September 2017 Navigation 54(3): 177–188. DOI: 10.1002/j.2161-4296.2007.tb00403.x.

9. H. Yonghui, Y. Yong, L. Jianhong and W. Lijuan, "A miniature low-cost MEMS AHRS with application to posture control of robotic fish", *IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, pp. 192-1395, 2018.

10. Sharat Chandra Bhardwaj, S. Shekhar. Satellite Navigation and Sources of Errors in Positioning: Computer Science 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM).

11. GNSS Error Sources. URL: (PDF) GNSS Error Sources (researchgate.net).

12. Yueyan Zhi, Zhangjie Fu, Xingming Sun,Jingnan Yu. Security and Privacy Issues of UAV: A Survey *Mobile Networks and Applications* volume 25, pages 95–101 (2020).

13. Add GPS Sensor Noise to Multirotor Guidance Model. URL: https://www.mathworks.com/help/uav/ug/add-gps-sensor-noise-to-guidance-model.html.

14. Pengda Huang, Ilir F. Progri / GPS Signal Detection under Multiplicative and Additive Noise. July 2013.Journal of Navigation 66 (04).

15. Gongmin Yan, Qiang wen Fu, Jun Weng. Special Issue "Accuracy Improvement Methods and New Applications of Inertial-Based Navigation System". A special issue of *Sensors* (ISSN 1424-8220), "Navigation and Positioning". (31 December 2022) Viewed by 8539.

16. Henry Martin, Paul Groves, Mark Newman. The Limits of In-Run Calibration of MEMS Inertial Sensors and Sensor Arrays/First published: 23 June 2016.

17. Principles of GNSS. URL: Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems | Artech books | IEEE Xplore.

18. A. Fakharian, T. Gustafsson, M. Mehrfam, “Adaptive kalman filtering based navigation: an IMU/GPS integration approach” IEEE conference on networking, sensing and control 2018, pp. 181–185.

19. Фесенко О., Бєляков Р., Радзівілов Г. Імітаційне моделювання безплатформної інерціальної навігаційної системи БПЛА на основі нейромережевих алгоритмів // Системи і технології зв’язку, інформатизації та кібербезпеки. Київ, 2022. Вип. 2 (2). С. 63–69.

DOI: 10.58254/viti.3.2023.16.143

УДК 004.056.57

доктор філософії Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Кисиленко Д. Ю. ORCID: 0000-0001-5491-6231 (ВІТІ ім. Героїв Крут)
доктор філософії Нестеров О. М. ORCID: 0000-0001-5092-6205 (ВІТІ ім. Героїв Крут)

АНАЛІЗ СПРОМОЖНОСТІ ІСНУЮЧИХ СИСТЕМ АНТИВІРУСНОГО ЗАХИСТУ ТА ПОКЛАДЕНИХ У ЇХНЮ ОСНОВУ МЕТОДІВ ДО ВИЯВЛЕННЯ НОВОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті вирішується завдання аналізу спроможності існуючих антивірусних систем та покладених у їх основу методів до виявлення нового шкідливого програмного забезпечення в інформаційних системах критичної інфраструктури, зокрема сектору сил оборони держави. Зазначено, що офіційні дані розробників антивірусних систем часто не підтверджують задекларований рівень точності виявлення нового шкідливого програмного забезпечення на практиці. До того ж, у більшості випадків задекларований показник точності виявлення нового шкідливого програмного забезпечення є вищим за аналогічний показник виявлення відомого шкідливого програмного забезпечення, що свідчить про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

Описано властивості нового шкідливого програмного забезпечення з метою пошуку найбільш відповідного йому класу комп'ютерних вірусів. Класи поліморфних (олігоморфних) та метаморфних вірусів демонструють найбільш повну відповідність зазначеним властивостям, що дозволяє стверджувати про їх значну частку у застосуванні нового шкідливого програмного забезпечення.

Наведено характеристику методів виявлення шкідливого програмного забезпечення, які завдяки своїм властивостям спроможні певною мірою адаптуватися до метаморфної (поліморфної) їх природи. Найбільш повну відповідність демонструють методи, в основу яких покладено теорію нечіткої логіки.

Запропоновано напрям удосконалення існуючих антивірусних систем щодо підвищення адаптивності до виявлення нових (поліморфних, метаморфних) класів шкідливого програмного забезпечення. Отримані результати доцільно розглядати, як підґрунтя для реалізації нових підходів до виявлення шкідливого програмного забезпечення з метою ідентифікації раніше невідомих його екземплярів, що дозволить значно підвищити ефективність забезпечення кібербезпеки сучасних інформаційних систем та мереж.

Ключові слова: *шкідливе програмне забезпечення, комп'ютерний вірус, поліморфні віруси, метаморфні віруси, антивірус, нечітка логіка, кіберзахист.*

V. Fesokha, D. Kysylenko, O. Nesterov Analysis of the capacity of existing anti-virus protection systems and their based methods for detecting new malware in military information systems.

The article solves the task of analyzing the ability of existing anti-virus systems and the methods based on them to detect new malicious software in information systems of critical infrastructure, in particular, the sector of the state defense forces. It is noted that the official data of the developers of antivirus systems often do not confirm the declared level of accuracy of detecting new malicious software in practice. In addition, in most cases, the declared accuracy rate of detecting new malware is higher than the similar rate of detection of known malware, which indicates that the antivirus systems in question are tested in specific conditions that are too different from real ones.

The properties of new malicious software are described in order to find the most suitable class of computer viruses. Classes of polymorphic (oligomorphic) and metamorphic viruses demonstrate the most complete compliance with the specified properties, which allows us to assert their significant share in the use of new malicious software.

The characteristics of malicious software detection methods are given, which due to their properties are able to adapt to a certain extent to their metamorphic (polymorphic) nature. Methods based on the theory of fuzzy logic demonstrate the most complete correspondence.

The direction of improvement of the existing anti-virus systems in order to increase the adaptability to the detection of new (polymorphic, metamorphic) classes of malicious software is proposed. The obtained results should be considered as a basis for the implementation of new approaches to the detection of malicious software in order to identify previously unknown instances of it, which will allow to significantly increase the effectiveness of ensuring cyber security of modern information systems and networks.

Keywords: *malware, computer virus, polymorphic viruses, metamorphic viruses, antivirus, fuzzy logic, cyber protection.*

Актуальність та постановка завдання в загальному вигляді. В існуючих умовах ведення кібервійни залишає не вирішеним завдання ефективного кіберзахисту інформаційних систем (ІС) критичної інфраструктури держави, зокрема ІС військового призначення, оскільки багато в чому забезпечення національної безпеки, захист територіальної цілісності та управління військами реалізується їх засобами [1].

Об'єктивно, сторона кібервпливу завжди має перевагу, оскільки ентропія комплексу її заходів для сторони кіберзахисту є досить високою, що у свою чергу, не дозволяє досягти хоча б ситуації паритету у процесі протиборства у кіберпросторі в режимі реального часу. Одним із основних підходів до реалізації описаної переваги є застосування нового шкідливого програмного забезпечення (ШПЗ), боротьба з яким, як правило, можлива не раніше стадії ліквідації його наслідків, а численні факти деструктивного впливу на ІС демонструють неспроможність існуючих систем антивірусного захисту виявляти та протидіяти їм достатньою мірою, внаслідок чого зростають вимоги до існуючих антивірусних програм [2].

За даними [3] міжнародної компанії AV-TEST (незалежна організація, яка вивчає та оцінює антивірусне ПЗ та пакети безпеки для популярних операційних систем (ОС) за різними критеріями) за останнім часом приріст нових комп'ютерних вірусів сягає нових рекордів. Зокрема для ОС Windows з'явилося близько 70 мільйонів нових зразків ШПЗ, що значно перевищує показник ОС macOS, для якої було зафіксовано лише близько 12 000 нових вірусів. Для ОС Linux зловмисники створили близько 2 мільйонів шкідливих програм. Причому динаміка появи нових видів (типів) ШПЗ ілюструє зміну вектора його застосування з добування криптовалюти на вимагання коштів від постраждалих, внаслідок деструктивної діяльності ШПЗ, а з початку 2022 року значно зріс відсоток інформаційно-руйнівного впливу на критичну інфраструктуру України з боку росії з метою викрадення інформації, що є особливо пріоритетним для забезпечення кібербезпеки ІТ-інфраструктури сил оборони і безпеки держави під час воєнного стану.

Нижче наведено стислий опис деяких деструктивних впливів на інформаційні сервіси різних держав засобами ШПЗ, які набули широкого розголосу протягом останнього часу.

1. 02 березня 2022 року фахівці центру виявлення загроз Threat Intelligence Center корпорації Microsoft виявили небезпечний вірус, так званий "FoxBlade" ("Fox" – лисиця і "Blade" – клинок), націлений на фінансові установи та міністерства України. Згідно із заявою [4] даний вірус реалізував деструктивний вплив на цифрову інфраструктуру України, зокрема банки, військові об'єкти, державні установи та промислові підприємства. Шляхом видалення даних із комп'ютерів, підключених до мережі Інтернет.

2. 02 червня 2022 року низку державних організацій України було атаковано ШПЗ Cobalt Strike Beacon, що призвело до численних перебоїв у їх роботі на певний час. Розповсюдження ШПЗ здійснювалося засобами електронної пошти через файл "Зміни оплата праці з нарахуваннями.docx". Відкриття файлу ініційовувало завантаження та виконання шкідливого скрипту засобами додатка MS Office. Також реалізація деструктивного впливу зловмисниками передбачала застосування експлойтів, сценарії яких використовували вразливість Microsoft Trident – функціонального ядра браузера Internet Explorer. Наявні системи антивірусного захисту не змогли перешкодити цьому деструктивному впливу [5].

3. 10 жовтня 2022 року компанії в Україні та Польщі було атаковано засобами ШПЗ Prestige [6]. Програма отримує доступ до облікових записів користувачів з метою шифрування файлів, додає розширення "enc", а також вимагає викуп в обмін на інструмент для розшифровування. Microsoft виділила кілька особливостей вірусу Prestige, які раніше не зустрічалися експертам з кібербезпеки. Незважаючи на подібні методи розгортання, кампанія Prestige відрізняється від недавніх руйнівних кібератак з використанням AprilAxe (ArguePatch)/CaddyWiper або Foxblade (HermeticWiper), які протягом останніх двох тижні до інциденту стосувалися кількох критично важливих об'єктів інфраструктури України. Вірус використовує бібліотеку CryptoPP C++ для шифрування AES кожного відповідного файлу. У процесі шифрування одна версія програми-вимагача використовує наступний

запрограмований відкритий ключ RSA X509 (кожна версія Prestige може мати унікальний відкритий ключ).

4. 17 грудня 2022 року урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження засобами електронної пошти (з використанням скомпрометованої електронної адреси одного зі співробітників оборонного відомства), а також, мессенджерів, повідомлення щодо необхідності оновлення сертифікатів у системі “Delta” (спеціалізоване програмне забезпечення (ПЗ) для ситуаційної обізнаності про противника). ШПЗ у розширенні pdf повністю імітувало легітимні дайджести одного з підрозділів, але містило посилання на zip-архів зі шкідливим вмістом. При переході за посиланням на комп’ютер завантажувався архів, який містив виконуваний файл деструктивного впливу, що захищений за допомогою VMProtect (спосіб захисту від аналізу та зламу). Після запуску виконуваного файлу на комп’ютері створювалося декілька dll-файлів з метою імітації процесу встановлення сертифіката. У результаті на комп’ютері здійснювався запуск ШПЗ RomCom, яке, у свою чергу, забезпечувало виконання інших шкідливих програм: FateGrab (викрадення файлів) та StealDeal (отримання та збереження даних браузерів у відповідних файлах з метою їх подальшої несанкціонованої передачі [7].

5. 10 лютого 2023 року російська хакерська група, яка стояла за руйнівними кібератаками з використанням ШПЗ WhisperGate, знову націлилась на українські організації з метою крадіжки інформації засобами нового ШПЗ [8]. Зловмисники націлені в першу чергу на Україну, але також атакували країни – члени НАТО в Північній Америці та Європі. ШПЗ маскується під програми-вимагачі, але робить цільові пристрої повністю непрацездатними та нездатними відновлювати файли, навіть якщо виплачується викуп. Під час нової хвилі кібератак зловмисники використовують раніше невідоме ШПЗ для крадіжки інформації під назвою Graphiron, яке використовувалося принаймні до середини січня 2023 року.

6. 20 березня 2023 за інформацією Держспецзв’язку [9], російські хакери поширюють шкідливі файли за допомогою безкоштовного доступу на торент-трекерах. Зокрема, якщо встановити такі файли на комп’ютер, зловмисники отримують доступ до вмісту комп’ютера й довгий час залишаються непомітними. У Держспецзв’язку зазначають, що жертвою хакерів можуть стати пересічні українці, які встановлюють неліцензійне програмне забезпечення (ПЗ) з неофіційних джерел та торентів.

Описані факти обумовлюють актуальність проведення подальших наукових досліджень щодо підвищення ефективності існуючих систем антивірусного захисту ІС військового призначення у процесі виявлення нового ШПЗ.

Аналіз останніх публікацій. Дослідженню ефективності застосування методів виявлення ШПЗ з метою пошуку напрямків вдосконалення існуючих систем антивірусного захисту присвячена значна кількість робіт [6–9], аналіз основних із яких викладено нижче.

У роботі [10] запропоновано підхід до аналізу методів виявлення ШПЗ на основі виокремлення критеріїв класифікації, які дозволять підвищити ефективність та достовірність виявлення нового ШПЗ: характер отриманих даних, ознаки, що виступають об’єктом пошуку та дослідження, методи аналізу, алгоритм прийняття рішень, очікуваний результат та оцінка класифікації. Даний підхід розширює існуючу класифікацію методів виявлення ШПЗ, однак не дозволяє класифікувати їх по найбільш повній відповідності характеристикам, властивим новому ШПЗ.

У роботі [11] виконано дослідження сигнатурного та евристичного методів виявлення ШПЗ. Наведено порівняльну характеристику методів машинного навчання, графічної візуалізації, евристичних методів виявлення ШПЗ та систематизовано їх за значеннями точності пошуку. Для ефективного виявлення нового ШПЗ запропоновано комбінувати всі сучасні методи, способи і засоби, враховуючи особливості їх використання. Даний підхід не дозволяє краще зрозуміти принципи застосування нового ШПЗ.

У роботі [12] розглянуто динаміку розвитку ШПЗ, а також здійснено огляд ряду методів виявлення програм, які можуть становити загрозу для комп’ютерних систем. Проаналізовано сигнатурні та поведінкові підходи. Окреслено недоліки існуючого

методологічного апарату. Основну увагу приділено евристичним методам на основі викликів API, N-грам та опкодів. Визначено шляхи подальших досліджень у напрямі комплексування досліджених методів з графами контролю потоків (CFG) та використання методів штучного інтелекту. Даний підхід також не дозволяє краще зрозуміти принципи застосування нового ШПЗ.

У роботі [13] наведений детальний огляд типів шкідливих програм, досліджуються та порівнюються методи їх аналізу та виявлення. Серед особливостей нового ШПЗ зазначено їх здатність до самомодифікації. Запропоновано підхід до виявлення поліморфного ШПЗ на основі поєднання переваг евристичних методів та методів машинного навчання. Даний підхід не дозволяє краще зрозуміти принципи застосування нового ШПЗ у повній мірі, оскільки не враховує усю множину властивостей нового ШПЗ.

Наявність недоліків у наведених наукових працях, а також численні факти вдалих спроб здійснення деструктивного впливу [4–9] на ІС демонструють неспроможність існуючих систем антивірусного захисту в силу обмеженості покладених у їх функціональне ядро алгоритмів, способів, моделей, методів та методик ідентифікації ШПЗ виявляти та протидіяти їм повною (достатньою) мірою, внаслідок чого зростають вимоги до існуючих систем антивірусного захисту ІС.

У зв’язку з цим, виникає завдання аналізу спроможності існуючих систем антивірусного захисту та покладених у їх основу методів виявлення ШПЗ до виявлення нових його екземплярів у військових ІС.

Метою статті є аналіз спроможності існуючих систем антивірусного захисту та покладених у їх основу методів виявлення ШПЗ до ідентифікації нового ШПЗ у військових ІС.

Спроможність рейтингових антивірусних систем до виявлення нового ШПЗ. Під спроможністю антивірусних систем та покладених у їх основу методів до виявлення нового ШПЗ будемо розуміти точність його виявлення.

Відповідно до офіційних даних [14–19] розробників популярного антивірусного ПЗ спроможність запропонованих ними програмних систем до виявлення екземплярів відомого ШПЗ є майже бездоганною за показником точності (не нижче 95 %), тоді як виявлення нових типів ШПЗ, зокрема вірусів, демонструє точність не нижче 98 %. Однак офіційні дані розробників антивірусного ПЗ часто не підтверджують задекларований рівень точності та/або достовірності виявлення нового ШПЗ на практиці, про що свідчить вищезазначена фактологія [4–9]. До того ж у більшості випадків задекларований показник точності виявлення нового ШПЗ є вищим за аналогічний показник виявлення відомого ШПЗ, що неприпустимо, оскільки метод сигнатурного аналізу, який покладено у основу їх модулів виявлення відомого ШПЗ є ефективнішим. В таблиці 1 наведено офіційну характеристику спроможності популярних антивірусних програм до виявлення відомого і нового ШПЗ [14–19].

Таблиця 1

Стисла характеристика спроможності популярних антивірусних програм до виявлення відомого і нового ШПЗ

№ з/п	Найменування антивірусного ПЗ	Відоме ШПЗ		Нове ШПЗ		
		Методи виявлення	Точність (%)	Методи виявлення	Точність «0-day» (%)	Точність виявлення нового ШПЗ (%)
1	Avira Antivirus	Сигнатурний аналіз Евристичний аналіз	95	Машинне навчання	99,6	–
2	ESET NOD 32	Сигнатурний аналіз Аналіз поведінки	100	Машинне навчання Евристичний аналіз	98	–
3	Panda	Сигнатурний аналіз Аналіз поведінки	99,7	Нейронні мережі	100	–
4	Avast Free Antivirus	Сигнатурний аналіз Аналіз поведінки	99,8	Нейронні мережі Евристичний аналіз	100	–

Avira Antivirus декларується як одна з кращих антивірусних програм для захисту кінцевих пристроїв. За результатами досліджень інституту AV-Test Avira отримала нагороду 2022 року в тестовій категорії "Найкращий захист споживачів під Windows". Захист споживачів від ШПЗ під управлінням платформи Windows є пріоритетним завданням, адже це найбільша група користувачів у світі [14; 15].

ESET NOD 32 є антивірусним ПЗ, що використовується для захисту кінцевих пристроїв від різних типів загроз. Має широкі можливості сканування файлів перед їх виконанням, що дає змогу певною мірою виявляти та блокувати навіть нові загрози [16]. Використовується у ІС та мережах Збройних Сил України.

Антивірусна програма ***Panda*** декларується як краща програма для захисту у реальному часі. Додаткові функції: захист від фішингу, захист Wi-Fi, фаєрвол, захист від програм-вимагачів та захист USB-пристроїв. Особливості: мінімальний вплив на систему [17].

Avast Free Antivirus декларується як одна з кращих програм антивірусного захисту із найменшим завантаженням ОС. Додаткові функції: інструменти управління паролями, оптимізація системи та VPN [18]. Антивірус Avast після отримання нагород в трьох тестових категоріях: "Найкращий захист для споживачів під Windows", "Найкращий захист Android для споживачів", "Найкращий захист macOS для споживачів " визнаний найкращим продуктом в галузі ІТ-безпеки 2022 року [19].

На основі проведеного аналізу популярних систем антивірусного захисту за спроможністю до виявлення відомого і нового ШПЗ можна зробити такі висновки:

1. Задекларована спроможність розглянутих систем антивірусного захисту є майже бездоганною, що досягається засобами покладених у їх основу методів виявлення ШПЗ, проте цей факт потребує додаткового вивчення. Так, декларація спроможності виявлення нових типів ШПЗ представлена статистикою виявлення вірусів нульового дня (0-day), тоді як вірус нульового дня та новий вірус – кардинально різні поняття. Новий комп'ютерний вірус – новий тип ШПЗ, який, як правило, становить собою модифікацію існуючого вірусу (поліморфізм/метаморфізм) з новими функціями або абсолютно нове ШПЗ, яке реалізує раніше невідомі способи (алгоритми) здійснення інформаційно-руйнівного впливу. Вірус 0-day – вразливість у ПЗ, яка ще не була виявлена розробниками антивірусних програм.

2. Ураховуючи багаторічний світовий досвід наукової спільноти щодо виявлення ШПЗ, отримані показники точності наведених результатів в аспекті виявлення нового ШПЗ у порівняно з відомим ШПЗ свідчать про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

3. У зв'язку з відсутністю офіційних даних про результати виявлення нового ШПЗ [14–19], а також пошуку причин недостатньої ефективності застосування існуючих систем антивірусного захисту [4–9] виникає необхідність дослідження властивостей застосування нового ШПЗ, а також методів, спроможних його виявляти.

Дослідження властивостей нового ШПЗ. Характерні особливості нового ШПЗ можуть змінюватися залежно від його типу та вектора впливу на об'єкт атаки. Серед 22 типів ШПЗ [20] найпоширенішим є *комп'ютерні віруси* (англ. computer virus) – спеціалізовані програми, що володіють здатністю до самовідтворення і, як правило, здатні здійснювати дії, які можуть порушити функціонування комп'ютерної системи і/або зумовити порушення її політики безпеки.

У зв'язку з цим, пропонується порівняльний аналіз існуючих типів комп'ютерних вірусів за наступними критеріями на предмет відповідності властивостям нового ШПЗ:

нові методи інфікування;

шифрування власного коду (тіла) для захисту від виявлення та аналізу;

нові методи обходу антивірусних програм та інших відомих заходів (політик) захисту;

збільшення функціональності;

підвищення ефективності маскування;

використання технологій штучний інтелекту, блокчейну;

використання нових вразливостей ПЗ (0-day) тощо.

Дослідження характерних ознак наведено множини типів комп'ютерних вірусів на предмет відповідності вищезазначеним властивостям нового ШПЗ показало найбільш повну відповідність властивостей з поліморфними (олігоморфними) та метаморфними вірусами. Так, всі перераховані віруси є представниками типу, що відрізняється від решти типів алгоритмом дій та реалізують: нові методи обходу антивірусних програм та інших заходів відомих захисту у тому числі шляхом шифрування власного коду для захисту від виявлення та аналізу. У таблиці 2 наведено результати аналізу властивостей комп'ютерних вірусів.

Таблиця 2

Результати аналізу властивостей існуючих комп'ютерних вірусів

Віруси	**Нові методи інфікування**	**Шифрування власного коду**	**Нові методи обходу засобів захисту**	**Збільшення функціональності**	**Підвищення ефективності маскування**	**Використання передових технологій**	**Використання нових вразливостей ПЗ (0-day)**
1	2	3	4	5	6	7	8
За деструктивними можливостями							
Безпечні	–	–	–	+	–	–	–
Нешкідливі	–	–	–	+	–	–	–
Небезпечні	–	–	–	+	–	–	–
Руйнівні	+	–	–	+	–	–	+
За способом зараження							
Резидентні	+	–	–	+	–	–	+
Нерезидентні	+	–	–	+	–	–	+
За середовищем існування							
Файлові	+	–	–	+	–	+	–
Мережеві	+	–	–	+	–	+	+
Завантажувальні	–	–	–	+	–	–	+
Flash-віруси	–	–	–	+	–	–	–
Макровіруси	–	–	–	+	–	–	–
За особливостями алгоритму дій							
1	2	3	4	5	6	7	8
«Стелс»-віруси (віруси-невидимки)	+	–	+	+	+	–	+
Паразитичні	+	–	–	+	–	–	–
Поліморфні (олігоморфні)	+	+	+	+	+	+	+
Метаморфні	+	–	+	+	+	+	+
Віруси-супутники	+	–	–	–	–	–	–

Так, у випадку самомодифікації поліморфного (олігоморфного) ШПЗ частина його коду змінюється [20], зберігаючи початковий алгоритм неушкодженим (вектор і тіло програми), в якому закладено основний сценарій реалізації деструктивної діяльності. На рисунку 1 представлено узагальнену структуру поліморфних вірусів.

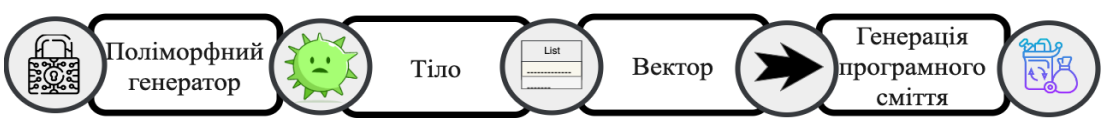


Рис. 1. Типова структура поліморфного вірусу

Виявлення такого типу вірусів можливе лише після розробки його сигнатури, а факт незмінності функціонального призначення тіла вірусу, що реалізує його вектор, дає підставу для виявлення нового ШПЗ на основі ідентифікації спільних структур вже класифікованих їх типів. Поліморфні та метаморфні віруси становлять основну частку нового ШПЗ, оскільки нові комп’ютерні віруси у своїй більшості являють собою модифіковані версії існуючого ШПЗ [21].

Метаморфні віруси можуть змінювати свою структуру і код таким чином, що вони стають абсолютно новим вірусом, який не може бути виявлено антивірусною програмою за сигнатурою попереднього екземпляра (перетворення коду, мутація, зміна порядку виконання). На рисунку 2 наведено узагальнену типову структуру метаморфних вірусів.

Рис. 2. Типова структура метаморфного вірусу

У зв’язку з наявністю властивості метапрограмування з метою уникнення виявлення антивірусними системами поліморфні (олігоморфні) та метаморфні віруси є особливо небезпечними для комп’ютерних систем та мереж військового призначення. До того ж поліморфні та метаморфні віруси становлять основну частку нового ШПЗ, оскільки нові комп’ютерні віруси у своїй більшості являють собою модифіковані версії існуючого ШПЗ [18].

Оцінка спроможності виявлення нового ШПЗ існуючими методами. Із множини існуючих підходів до аналізу ШПЗ найбільш доцільним є динамічний аналіз, оскільки дозволяє виявляти деструктивну діяльність різних програм безпосередньо під час виконання. Динамічний аналіз ШПЗ виділяє методи, спроможні певною мірою виявляти нове ШПЗ, завдяки властивості адаптації [22]. Крім того, внаслідок зростання вимог до антивірусних систем [22], порівняння методів виявлення ШПЗ має ґрунтуватись на властивостях верифікованості та спроможності до виявлення нового ШПЗ: *наявність невідомих унікальних характеристик, рівень хибних спрацьовувань, розмитість досліджуваних даних* (табл. 3).

Таблиця 3

Результати аналізу методів виявлення нового ШПЗ за визначеними критеріями

Метод	**Верифікованість**	**Спроможність виявляти нове ШПЗ за характеристиками**		
		Наявність невідомих унікальних характеристик	**Рівень хибних спрацьовувань**	**Шум (розмитість) досліджуваних даних**
Поведінкові методи:				
Спектральний аналіз	–	низька	середній	низька
Фрактальний аналіз	–	низька	низький	низька
Аналіз ентропії	+	низька	середній	середня
На основі знань:				
Графи сценаріїв	+	низька	середній	низька
Методи на сплайнах	–	низька	середній	середня
Евристичний аналіз	+	середня	низький	середня
Статистичний аналіз	–	низька	середній	середня
Експертні системи	+	низька	низький	низька
Методи штучного інтелекту:				
Нейронні мережі	–	середня	низький	середня
Генетичні алгоритми	–	середня	низький	низька
Нечітка логіка	+	середня	низький	висока
Імунні системи	–	середня	низький	середня
Опорні вектори	–	низька	середній	низька
Роєві алгоритми	+	середня	низький	низька
Методи машинного навчання:				
Алгоритми регресії	–	низька	середній	середня
Кластеризація	–	низька	середній	середня
Байєсівські мережі	–	низька	середній	середня
Байєсівський метод	–	низька	середній	середня

На основі проведеного аналізу методів виявлення нового ШПЗ можна зробити такий висновок.

Жоден з досліджуваних методів в силу своїх властивостей неспроможний у повному обсязі забезпечити виявлення одного з найнебезпечніших типів ШПЗ – комп'ютерних вірусів, здатних до метапрограмування власного коду з метою реалізації способу приховування від існуючих антивірусних систем. До такого типу вірусів належать поліморфні (олігоморфні) і метаморфні віруси. Так, кожен із класів існуючих методів (на основі знань, штучного інтелекту, машинного навчання, поведінкові) спроможний вирішувати це завдання тією чи іншою мірою, проте в умовах певних обмежень. Результати порівняльного аналізу за описаними критеріями демонструють, що серед них можливо виділити методи, які показали найбільш повну їм відповідність, – методи на основі теорії нечіткої логіки. Так, формалізація неточних знань та виконання наближених міркувань в області виявлення ШПЗ дозволяє виявляти його деструктивну діяльність в умовах певної нечіткості інформації про стан ІС з можливістю адаптації до виявлення подібних типів ШПЗ.

Напрям удосконалення існуючих систем. На сьогодні існує дві стратегії до виявлення нового ШПЗ [22]: виявлення аномальної діяльності на підставі аудиту сценаріїв функціонування, виявлення з урахуванням набутого досвіду боротьби з відомим ШПЗ. Для ефективного виявлення нового ШПЗ доцільно використовувати другий підхід, заснований на досвіді боротьби з уже відомим ШПЗ, оскільки кількість нових його екземплярів, які характеризуються принципово новою множиною ознак, досить мала.

Пріоритетним напрямом удосконалення існуючого антивірусного ПЗ є доповнення існуючого функціоналу методом, в основу якого покладено теорію нечіткої логіки. Причому застосування обраного методу має передбачати визначення поліморфної (метаморфної) компоненти ШПЗ для кожного відомого його типу, що забезпечить ефективне виявлення нового ШПЗ на основі ідентифікації поліморфних (метаморфних) структур уже існуючих вірусів в умовах деякої неточності (розмитості) інформації про стан ІС.

Висновки. У статті вирішується завдання аналізу спроможності існуючих антивірусних систем та покладених у їх основу методів до виявлення нового шкідливого програмного забезпечення. Офіційні дані розробників антивірусних систем часто не підтверджують задекларований рівень точності виявлення нового шкідливого програмного забезпечення на практиці, що свідчить про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

Проведено аналіз існуючих типів ШПЗ, серед них виділено поліморфні (олігоморфні) та метаморфні віруси, як особливо небезпечне ШПЗ для сучасних комп'ютерних систем. Поліморфні та метаморфні віруси становлять основну частку нового ШПЗ, оскільки нові комп'ютерні віруси у своїй більшості являють собою модифіковані версії існуючого ШПЗ.

Результати аналізу методів виявлення ШПЗ демонструють, що серед них можливо виділити методи, які показали найбільш повну відповідність поставленим до них вимогам (адаптивність, верифікованість, наявність невідомих унікальних характеристик, рівень хибних спрацьовувань, розмитість досліджуваних даних), – методи на основі теорії нечіткої логіки.

Запропоновано напрям удосконалення існуючих антивірусних систем щодо підвищення спроможності до виявлення нових типів шкідливого програмного забезпечення. Причому застосування обраного методу має передбачати визначення поліморфної (метаморфної) компоненти ШПЗ для кожного відомого його класу, що дозволить виявляти нове ШПЗ на основі ідентифікації поліморфних (метаморфних) структур уже існуючих вірусів в умовах деякої неточності (розмитості) інформації про стан ІС.

Таким чином, отримані результати є підґрунтям для реалізації нових підходів до виявлення нового ШПЗ, що дасть можливість підвищити ефективність кібербезпеки військових ІС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 17.08.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Фесьоха В. В., Кисиленко Д. Ю., Турчак О. Р. Перспективи удосконалення існуючих рішень виявлення шкідливого програмного забезпечення в інформаційних системах військового призначення. Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: матеріали ІІ міжнар.наук.-практ. конф., 01 грудня 2022. Київ: ВІТІ ім. Героїв Крут. С. 216.

3. ГайдамашкоО. Кількість шкідливих програм для Windows у 5000 разів вища, ніж на macOS. *24 Канал*. URL: https://24tv.ua/tech/2022-rotsi-dlya-windows-stvorili-70-milyoniv-virusiv_n2226891.

4. Smith B. Digital technology and the war in Ukraine - Microsoft On the Issues. *Microsoft On the Issues*. URL: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattack.

5. Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon та експлойтів до вразливостей CVE-2021-40444 і CVE-2022-30190 (CERT-UA#4753). *cert.gov.ua*. URL: https://cert.gov.ua/article/40559.

6. New “Prestige” ransomware impacts organizations in Ukraine and Poland - Microsoft Security Blog. *Microsoft Security Blog*. URL: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

7. Кібератака на користувачів системи DELTA з використанням шкідливих програм RomCom/FateGrab/StealDeal (CERT-UA#5709). *cert.gov.ua*. URL: https://cert.gov.ua/article/3349703.

8. Page C. Russian 'WhisperGate' hackers are using new data-stealing malware to target Ukraine. *TechCrunch*. URL: https://techcrunch.com/2023/02/08/whispergate-hackers-data-stealing-malware-ukraine/.

9. Викриття: (Російські спецслужби розповсюджують шкідливе програмне забезпечення за допомогою торент-трекерів). *#DisinfoChronicle. Кремлівська дезінформація щодо військового наступу на Україну – Детектор медіа.* URL: https://disinfo.detector.media/post/rosiiski-spetssluzhby-poshyriuiut-shkidlyve-prohramne-zabezpechennia-za-dopomohoiu-torent-trekeriv.

10. Савенко О. С. Критерії класифікації методів виявлення шкідливого програмного забезпечення. *Вісник Хмельницького національного університету*. № 1. С. 23–27.

11. Жульковська І. І., Плужник А. В., Жульковський О. А. Сучасні методи виявлення шкідливих програм. *Математичне моделювання*. № 1. С. 46–54.

12. Лисенко С. М., Щука Р. В. Аналіз методів шкідливого програмного забезпечення в комп’ютерних системах. *Вісник Хмельницького національного університету*. № 2. С. 101–107.

13. Rabia Tahir. A Study on Malware and Malware Detection Techniques. I.J. Education and Management Engineering, p. 20–30.

14. Поліщук Н. Avira огляд 2023: чи варто купувати? *WizCase*. URL: https://uk.wizcase.com/antivirus/avira.

15. Selinger M. AV-TEST Award 2022 for Avira. *AV-TEST |Unabhängige Tests von Antiviren- & Security-Software*. URL: https://www.av-test.org/en/news/av-test-award-2022-for-avira/.

16. Унікальна технологія ESET для сучасного захисту. *ESET*. URL: https://www.eset.com/ua/about/technology/.

17. Олеч Ю. Огляд антивірусу Panda у 2023: чи варто купувати?. *WizCase*. URL: https://uk.wizcase.com/antivirus/panda.

18. Поліщук Н. Avast огляд 2023: чи варто купувати?. *WizCase*. URL: https://uk.wizcase.com/antivirus/avast.

19. Selinger M. AV-TEST Award 2022 for Avast. *AV-TEST|Unabhängige Tests von Antiviren- & Security-Software*. URL: https://www.av-test.org/en/news/av-test-award-2022-for-avast/.

20. Tunggal A. T. 22 Types of Malware and How to Recognize Them in 2023 | UpGuard. *Third-Party Risk and Attack Surface Management Software | UpGuard*. URL: https://www.upguard.com/blog/types-of-malware.

21. Zero-day polymorphic cyberattacks detection using fuzzy inference system / V. V. Fesokha et al. *Austrian Journal of Technical and Natural Sciences*. p. 8–13. URL: https://doi.org/10.29013/ajt-20-5.6-8-13.

22. Субач І., Фесьоха В., Фесьоха Н. Фесьоха Н. О. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі. *Information Technology and Security*. 2017. Т. 5, № 1. С. 29–41.

DOI: 10.58254/viti.3.2023.17.152

УДК 004.056.53

доктор філософії Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Фесьоха Н. О. ORCID: 0000-0002-1527-1474 (ВІТІ ім. Героїв Крут)

МЕТОД РЕГУЛЯРИЗАЦІЇ ОЗНАКОВОГО ПРОСТОРУ БІОМЕТРИЧНОЇ МОДЕЛІ КЛАВІАТУРНОГО ПОЧЕРКУ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ФАКТОРНОГО АНАЛІЗУ

У статті вирішується актуальне наукове завдання регуляризації ознакового простору біометричної моделі клавіатурного почерку користувачів інформаційних систем військового призначення з метою підвищення ефективності процедури автентифікації користувачів системами контролю і розмежування доступу. Постановка даного наукового завдання зумовлена наявністю наступних недоліків існуючих біометричних моделей клавіатурного почерку користувачів: при збільшенні числа користувачів у системі зростає складність їх класифікації; складність формалізації унікальності користувачів; надто складна реалізація визначення факту підміни уже авторизованого користувача; ознаковий простір існуючих біометричних моделей є незначним в силу обмеження множини властивостей сучасної клавіатури, що негативно впливає на показник точності процедури автентифікації. Обрано біометричну модель клавіатурного почерку, особливістю якої є формалізація унікальності користувача інформаційної системи на основі виявлення властивих йому закономірностей клавіатурного почерку нечіткими правилами. Запропоновано удосконалений метод регуляризації ознакового простору біометричної моделі клавіатурного почерку користувачів інформаційних систем військового призначення. Суть запропонованого методу, яка відрізняє його від існуючих, полягає у тому, що збільшення множини ознак біометричної моделі досягається шляхом додавання до неї виявлених прихованих фактів із множини власних ознак на основі факторного аналізу із найбільшим показником їх мінливості. Застосування запропонованого методу дозволяє вирішити завдання нелінійної сепарабельності n-вимірного ознакового простору біометричної моделі клавіатурного почерку, що у свою чергу дозволяє підвищити показники точності та достовірності процедури автентифікації системами контролю і розмежування доступу інформаційних систем військового призначення.

Ключові слова: *регуляризація, біометрична модель, поведінкова біометрія, клавіатурний почерк, інформаційні системи, автентифікація, несанкціонований доступ, факторний аналіз.*

V. Fesokha, N. Fesokha The method of regularizing the sign space of the biometric model of the keyboard handwriting of users of military information systems on the basis of factor analysis.

The article addresses the current scientific task of regularizing the feature space of the biometric model of the keyboard handwriting of users of military information systems in order to increase the effectiveness of the user authentication procedure by access control and demarcation systems. The setting of this scientific task is due to the presence of the following shortcomings of the existing biometric models of users' keyboard handwriting: when the number of users in the system increases, the complexity of their classification increases; the complexity of formalizing the uniqueness of users; the implementation of determining the fact of replacing an already authorized user is too complex; the feature space of the existing biometric models is insignificant due to the limitation of the set of properties of the modern keyboard, which negatively affects the accuracy of the authentication procedure. A biometric model of keyboard handwriting was chosen, the feature of which is the formalization of the uniqueness of the user of the information system on the basis of the detection of the regularities of the keyboard handwriting by fuzzy rules. An improved method of regularization of the feature space of the biometric model of keyboard handwriting of users of military information systems is proposed. The essence of the proposed method, which distinguishes it from the existing ones, is that the increase in the set of features of the biometric model is achieved by adding to it discovered hidden facts from the set of own features based on factor analysis with the highest rate of their variability. The application of the proposed method allows solving the problem of non-linear separability of the n-dimensional feature space of the biometric model of keyboard handwriting, which in turn allows to increase the accuracy and reliability of the authentication procedure by control systems and access demarcation of military information systems.

Keywords: *regularization, biometric model, behavioral biometrics, keyboard handwriting, information systems, authentication, unauthorized access, factor analysis.*

Актуальність та постановка завдання в загальному вигляді. Існуючі умови технологічної ескалації у кіберпросторі залишають не вирішеним завдання ефективного забезпечення конфіденційності, доступності та цілісності даних інформаційних систем (ІС) критичної інфраструктури, зокрема ІС військового призначення [1–4].

Одним із основних напрямків вирішення даного завдання є організація виявлення фактів несанкціонованого доступу до інформаційних ресурсів (секретних даних,

конфіденційної інформації, оперативної обстановки військ у зоні бойових дій, місць дислокації засобів протиповітряної оборони, радіолокаційних станцій і т. д.), розголошення яких може призвести до непередбачуваних наслідків. Поряд з цим, існуючі алгоритми, способи, методи, методики автентифікації, як підґрунтя основного етапу процедури контролю доступу користувачів ІС не здатні повною мірою забезпечити ефективний кіберзахист інформаційних ІС, про що свідчать численні факти компрометації безпеки ІС та несанкціонованих втручань [2; 5].

Це обумовлює актуальність подальших наукових досліджень щодо підвищення ефективності процедури автентифікації користувачів ІС військового призначення.

Аналіз наукових публікацій показав ефективність використання процедури автентифікації користувачів ІС, в основу якої покладено аналіз їхньої поведінкової біометрії, зокрема клавіатурного почерку (КП), оскільки дозволяє здійснювати класифікацію (розпізнавання) користувачів за їх індивідуальними (унікальними) підсвідомими характеристиками (сенсорними і руховими навичками), які практично неможливо (повністю неможливо) фальсифікувати [2; 3]. Так, автентифікація користувачів відповідно до пред'явленого ідентифікатора здійснюється на основі аналізу значень показників машинного набору тексту (швидкість друку, ритм друку, сила натискання, тривалість натискання, час між натисканням клавіш) під час виконання процесу, що підлягає дослідженню (введення пароля, контрольного тексту).

Поряд з цим, існуючі системи біометричної автентифікації за КП, часто характеризуються досить низькою достовірністю (точністю) автентифікації осіб [6]. У переважній більшості наукових праць [3; 6–14], які присвячені вивченню даного питання, на відміну від завдання вибору науково-методичного апарату для подальшої побудови класифікатора, недостатньо уваги приділяється формалізації унікальності (індивідуальних підсвідомих характеристик) користувачів ІС, що зі свого боку негативно впливає на адекватність їхньої біометричної моделі (профілю) КП. Як правило, синтез біометричної моделі (профілю) КП здійснюється на основі наступних підходів:

шляхом визначення персонального ознакового простору для кожного користувача ІС;

шляхом зведення множини досліджуваних ознак КП користувачів ІС у спільний ознаковий простір.

Перший підхід передбачає формалізацію індивідуальних підсвідомих характеристик користувача досить вузько, оскільки характеризує конкретну послідовність натискання клавіш користувачем (контрольного тексту, пароля), що не відповідає реальній криміналістичній експертизі рукописного почерку людини [15]. Другий підхід, навпаки, дозволяє синтезувати біометричні моделі користувачів на основі їх спільного ознакового простору із забезпеченням можливості аналізу натискання довільних послідовностей клавіш клавіатури користувачем, що у значно більшій мірі відповідає реальній криміналістичній експертизі рукописного почерку користувача [15]. До того ж, такий підхід дозволяє виявляти підміну користувача ІС за іншим наявним ідентифікатором у системі.

Підходи до синтезу біометричних моделей КП шляхом визначення персонального ознакового простору для кожного користувача представлено значною кількістю наукових досліджень [3; 6–14], у переважній більшості яких [6–14] формування ознакового простору обмежується лише статистичними даними роботи з клавіатурою, що породжує низку недоліків:

при збільшенні числа користувачів у системі зростає складність їх класифікації;

складна реалізація формалізації унікальності користувачів ІС;

надто складна реалізація визначення факту підміни уже авторизованого користувача;

ознаковий простір існуючих біометричних моделей (профілів) є досить незначним в силу обмеження множини властивостей сучасної клавіатури, що негативно впливає на показник точності (достовірності) процедури автентифікації.

У роботі [3] запропоновано підхід до синтезу біометричної моделі КП користувача ІС, який ґрунтується на використанні математичного апарату теорії нечіткої логіки. Так,

додавання нових ознак ґрунтується на основі інженерії поведінкових закономірностей роботи користувача з клавіатурою у вигляді нечітких правил на множині досліджуваних ознак, що дозволяє певною мірою описати його унікальність. Даний підхід передбачає формування спільного ознакового простору для всіх біометричних моделей користувачів, однак не вирішує питання його нелінійної сепарабельності.

Представлені недоліки розглянутих наукових досліджень обумовлюють доцільність регуляризації ознакового простору існуючих біометричних моделей користувачів ІС, що дозволить підвищити ефективність їх класифікації (розпізнавання) на етапі процедури автентифікації.

Регуляризація (англ. *regularization* – метод додавання деяких додаткових даних до умови з метою вирішення некоректно поставленого завдання або додаткових обмежень до умови з метою запобігти перенавченню [16]). У контексті поставленого наукового завдання – метод додавання певних додаткових ознак до ознакового простору біометричної моделі КП користувача ІС [3].

У зв'язку з цим, виникає актуальне наукове завдання регуляризації ознакового простору біометричної моделі КП користувачів ІС військового призначення.

Метою статті є розробка методу регуляризації ознакового простору біометричної моделі КП користувачів ІС військового призначення.

Біометрична модель КП користувачів ІС. У статті розглядається біометрична модель КП користувача ІС, запропонована у [3], синтез якої передбачає формування єдиного ознакового простору для всіх користувачів, що дозволяє виявляти підміну ідентифікованого користувача за іншим наявним ідентифікатором у системі. Застосування даної біометричної моделі КП дозволяє визначати притаманні конкретному користувачу підсвідомі унікальні поведінкові риси, присутні у різних психоемоційних станах, що у свою чергу дозволяє позбутися множини опису станів кожного облікового запису та зменшити кількість хибних спрацювань системою контролю та розмежування доступу у процесі автентифікації особи в умовах деякої нечіткості управляючої інформації.

Так, у відповідності до [3] із множини статистичних параметрів КП:

Δt_k^r – тривалість утримання (*retention*) клавіш k клавіатури;

Δt_{kl}^p – час натискання (*pause*) між клавішами (k та l);

pow – сила натискання клавіш (для сенсорної клавіатури);

sq – площа, що займається під час натискання клавіші (для сенсорної клавіатури), першим кроком є синтез початкового спільного для всієї множини користувачів $u_i \in U$ n-вимірного ознакового простору КП S_{start}, де:

p – загальний відсоток попадання часового інтервалу утримання кожною клавішею послідовності у еталонні діапазони значень на основі відстані Махаланобіса [17; 18];

d – динаміка друку – час між натисканням клавіш і часом їх утримання;

v – швидкість друку – кількість натиснутих клавіш розділена на час друку;

i – ідентифікатор користувача ІС.

Другим кроком формування біометричної моделі є додавання до початкового ознакового простору S_{start} підмножини нових ознак S_{new}, створених на основі знайдених поведінкових закономірностей зі статистичного набору даних роботи користувача ІС u_i за клавіатурою. Реалізація способу інженерії закономірностей передбачає опис послідовності часових інтервалів утримання клавіш Δt_k^r клавіатури відповідною їй функцією $f(\Delta t_1^r, \Delta t_2^r, \dots, \Delta t_n^r)$. Для прикладу, на рисунку 1 зображено графік функції поведінкової закономірності КП першого автора при введенні контрольного тексту (2 спроби) із 12 символів (Δt_k^r у мілісекундах). По горизонтальній осі представлено загальний час введення контрольної фрази у мілісекундах, по вертикальній – Δt_k^r даної послідовності у мілісекундах.

Як видно з рисунку 1, наявна закономірність тривалості утримання клавіш Δt_k^r виражена наближеними формами кривих, які описують її у 12 точках із відповідними значеннями, що є справедливим і для значної кількості таких спроб.

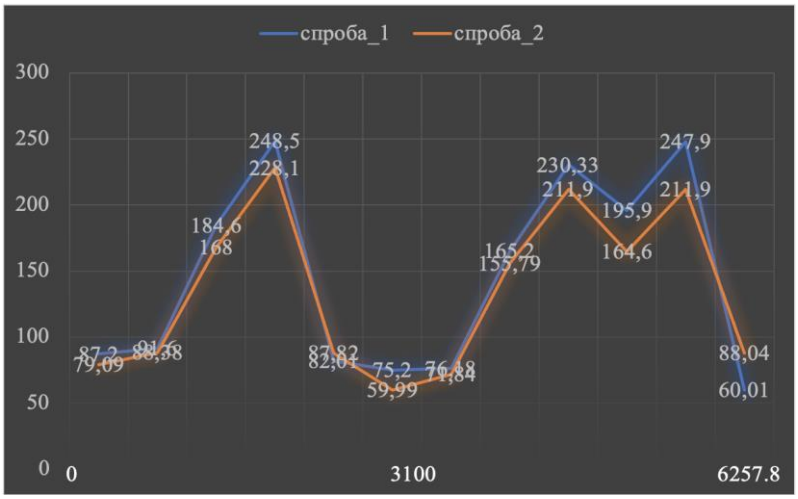


Рис. 1. Графік функції поведінкової закономірності КП першого автора при введенні контрольної фрази (Δt^r_{1-12})

Відповідно до [3] необхідно визначити додаткові ознаки КП користувача на основі знайденої закономірності з метою формування остаточного ознакового простору біометричної моделі КП M_{u_i} у поєднанні із початковим S_{start}. Так, представлена послідовність декомпозується на часові вікна t_i^w, які формують додаткову підмножину ознак КП S_{new} (рис. 2). Кількість часових вікон – 10, що у середньому відповідає інтервалу 500 мілісекунд. Час введення власних паролів різними користувачами під час проведення експериментів не перевищував 10 секунд.

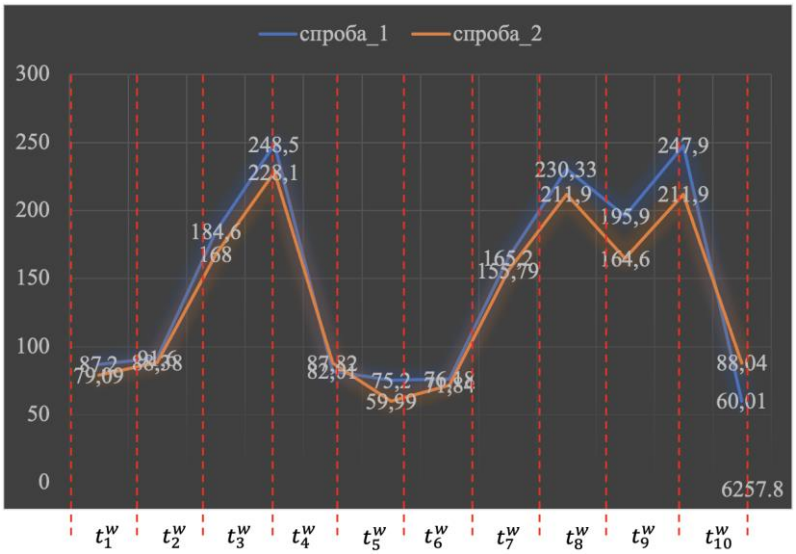


Рис. 2. Графічне представлення декомпозиції досліджуваної послідовності натискання клавіш користувачем u_i на часові вікна t^w_{1-10}.

Так, у кожному часовому вікні t_i^w присутні частини інтервалів (кусково-лінійні функції) виявленої закономірності. Вибір даного способу інженерії ознак зумовлено необхідністю інтерпретації послідовності утримання клавіш Δt_k^r клавіатури під час відтворення процесу, що підлягає обробці однаковою їх кількістю для різних користувачів u_i.

Заключним кроком синтезу біометричної моделі користувача є апроксимація функції $f(\Delta t_1^r, \Delta t_2^r, \dots, \Delta t_n^r)$, що описує швидкість зміни виявленої закономірності у вигляді кривої (геометричний сенс диференціювання функцій) нечіткими правилами у часових вікнах t^w_{1-10} (терм-множини: зростання (дуже високе, високе, середнє, мале, дуже мале); спадання (дуже високе, високе, середнє, мале, дуже мале). При чому, визначення значення похідної

для будь-якої точки на кривій, що описує закономірність Δt_k^r ґрунтується на визначенні кута між горизонтальною віссю та дотичною до обраної точки.

Аналітичний вираз описаної біометричної моделі КП засобами теорії нечіткої логіки представлено аналітичним виразом (1) [3]:

$$M_{u_i} = (S_{start} = \{p, d, v\} \cup S_{new} = \{t_1^w, \dots, t_{10}^w\}) \rightarrow \{p, d, v, t_1^w, \dots, t_{10}^w\}. \quad (1)$$

Очевидно, що найбільш впливовим негативним чинником застосування даної моделі M_{u_i} для автентифікації користувачів ІС системами контролю і розмежування доступу є фактор нелінійної сепарабельності її ознакового простору КП, походження якого зумовлено залежністю складної нелінійної функції від кількох змінних, розподіл значення яких досить складно (неможливо) знайти. Іншими словами, немає таких функцій, які можуть розділити ці змінні на незалежні групи лінійно. На рисунку 3 представлено завдання класифікації векторів (червоні, сині), множини яких не можуть бути лінійно розділені на площині (рис. 3, *а* – випадок двох множин, рис. 3, *б* – випадок двох класів (кластерів)) [19].

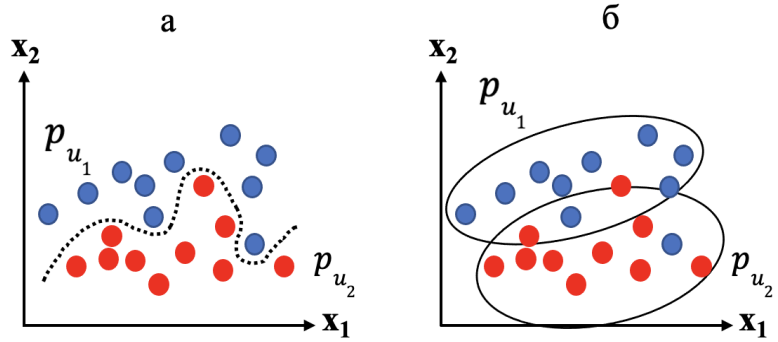


Рис. 3. Графічне представлення випадку нелінійної сепарабельності множин (кластерів) векторів: *а* – випадок двох множин; *б* – випадок двох класів (кластерів)

Рішення такого роду завдань існуючими підходами: методи оптимізації (градієнтний спуск, оптимізація на основі еволюційних алгоритмів); методи поділу змінних (лінійна регресія, аналіз головних компонент); методи на основі штучних нейронних мереж; ядрові методи, полягає у відображенні цільових вхідних даних на збільшеному просторі ознак з метою пошуку такої гіперплощини, яка дозволить розділити їх лінійно. На рис. 4, *а* зображено завдання та ідеальний результат його рішення (рис. 4, *б*) на збільшеному просторі ознак.

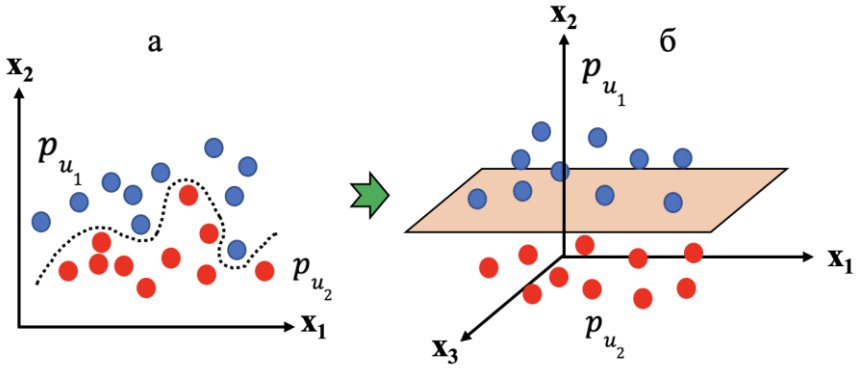


Рис. 4. Графічне представлення результату рішення завдання нелінійної сепарабельності у збільшеному просторі ознак: *а* – завдання; *б* – ідеальний результат його рішення

Застосування вищезазначених методів дозволяє вирішити завдання нелінійної сепарабельності ознакового простору лише частково, оскільки піднімає, як питання оптимального відбору інформативних ознак у процесі зменшення його розмірності, так і

трансформації досліджуваних векторів з метою вирішення завдання їх класифікації на новому просторі ознак. Даний факт спричиняє необхідність пошуку такого підходу до регуляризації ознакового простору біометричної моделі, який дозволить вирішити завдання нелінійної сепарабельності у цілому.

Метод регуляризації ознакового простору біометричної моделі КП. На основі викладеного пропонується удосконалення методу регуляризації біометричної моделі КП користувачів ІС військового призначення на основі факторного аналізу. Суть запропонованого методу, що відрізняє його від існуючих [3; 6–14] полягає у тому, що збільшення множини ознак біометричної моделі досягається шляхом додавання до неї виявлених нових прихованих фактів із множини власних ознак на основі факторного аналізу із найбільшим показником їх мінливості. Так, у результаті визначення структури взаємозв'язків досліджуваних змінних у вигляді ознак їх підмножина не заміщує досліджуваний ознаковий простір моделі, а використовуються для збільшення його вимірів.

Вибір факторного аналізу для вирішення завдання нелінійної сепарабельності ознакового простору зумовлено забезпеченням можливості формалізації взаємозв'язків змінних без поділу на результативні та факторні ознаки, наприклад, на відміну від регресійного аналізу, а також дисперсійного та дискримінантного у аспекті відсутності необхідності визначення заздалегідь управляючих даних.

Методом факторного аналізу обрано метод головних компонент [20] (англ. *Principal component analysis,* PCA) – метод факторного аналізу, який використовує ортогональне перетворення множини спостережень з пов'язаними змінними (сутностями, кожна з яких набуває різних числових значень) у множину змінних без лінійної кореляції, які називаються головними компонентами. Вибір методу PCA обумовлено тим фактом, що в аналізі головних компонент передбачається використання всієї мінливості змінних, тоді як, наприклад, в аналізі головних факторів використовується тільки мінливість конкретної змінної. До того ж, на практиці, PCA демонструє найкращі результати, як метод зменшення розмірності даних, тоді як інші методи краще застосовувати для визначення структури даних.

Формальна постановка завдання [21; 22]:

Дано центрований набір векторів даних $x_i \in R^n$ $(i = 1, \dots, m)$ (середнє арифметичне значення дорівнює нулю). Вибіркова дисперсія даних вздовж напрямку, заданого нормованим вектором a_k, це (2):

$$S_m^2\,[(X, a_k)] = \frac{1}{m}\sum_{i=1}^{m}(a_k, x_i)^2 = \frac{1}{m}\sum_{i=1}^{m}\left(\sum_{j=1}^{n} x_{ij}a_{kj}\right)^2. \qquad (2)$$

Оскільки дані центровані, вибіркова дисперсія збігається із середнім квадратом відхилення від нуля. Рішення задачі найкращої апроксимації дає ту саму множину головних компонентів $\{a_i\}$, що і пошук ортогональних проекцій з найбільшою дисперсією у зв'язку з тим, що перший доданок не залежить від a_k, а також $||x_i - a_k(a_k, x_i)||^2 = ||x_i||^2 - (a_k, x_i)^2$.

Вихідні дані:

M_{u_i} – біометрична модель КП користувачів u_i ІС;

u_i – користувач ІС із множини усіх користувачів U ІС;

$\{p, d, v, t_1^w, \dots, t_{10}^w\}$ – 13-ознаковий простір M_{u_i}, на основі аналізу значень якого виконується завдання класифікації (розпізнавання) $u_i \in U$;

набір статистичних даних, на основі яких здійснювався синтез моделі M_{u_i}.

Розглядається процес регуляризації ознакового простору M_{u_i} з метою вирішення завдання його нелінійної сепарабельності.

Обмеження та допущення:

ознаковий простір M_{u_i} є спільним для усієї множини користувачів U у системі;

біометрична модель M_{u_i} описує роботу користувачів $u_i \in U$ із звичайною (традиційною) клавіатурою;

у випадку застосування сенсорної клавіатури до початкового ознакового простору M_{u_i} необхідно додати ознаки: сили натискання клавіш та площі, що займається під час натискання клавіш.

Необхідно:

знайти таке ортогональне перетворення (проєкцію) ознакового підпростору M_{u_i} в нову систему координат S_{sub}, для якого були б справедливі наступні умови:

вибіркова дисперсія даних уздовж першої координати максимальна (перша головна компонента);

вибіркова дисперсія даних уздовж другої координати максимальна за умови ортогональності першої координати (друга головна компонента);

вибіркова дисперсія даних уздовж значень k-ї координати максимальна за умови ортогональності першим $k-1$ координатам.

Метод регуляризації ознакового простору біометричної моделі КП користувачів ІС представлено наступною функціональною схемою, яка передбачає реалізацію наступних етапів (рис. 5):

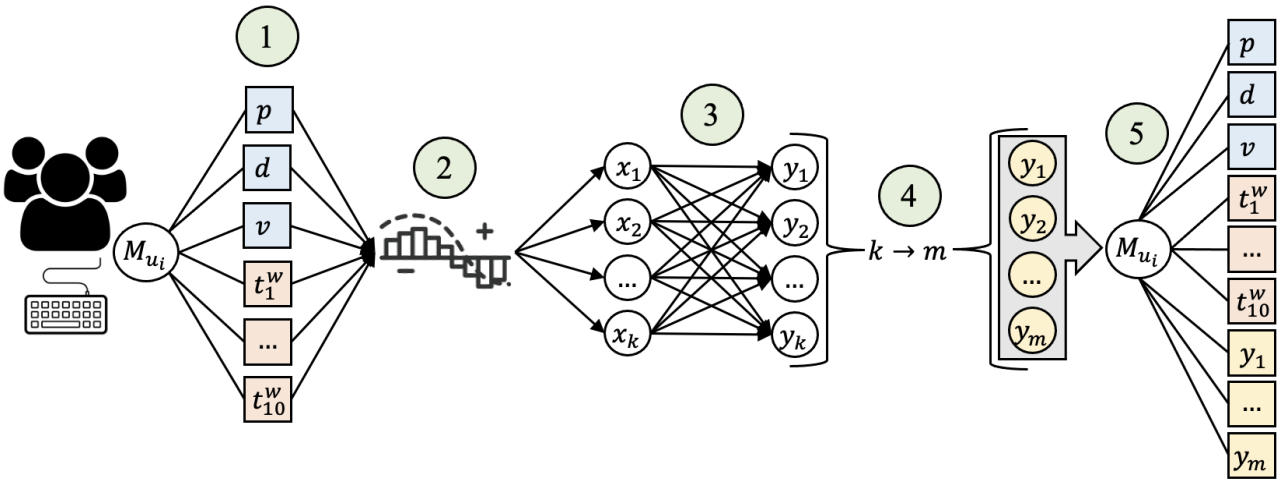


Рис. 5. Функціональна схема методу регуляризації ознакового простору біометричної моделі КП користувачів ІС

1. Отримання множини ознак біометричної моделі КП користувача ІС.

На даному етапі ініціалізується множина ознак біометричної моделі M_{u_i} потужністю 13, якою описуються користувачі ІС з метою ортогональної її проєкції на ознаковий простір зменшеної розмірності S_{sub}.

Для конструювання основних компонентів використовується лінійна модель для стандартизованих змінних [23] (3):

$$y_i = \sum_{j=1}^{k} a_{i,j} x_j, \tag{3}$$

де y_i – головна компонента за номером $i (i = 1, \dots, m)$;

x_j – стандартизована вихідна змінна z_j;

$\overline{z_j}$ – середнє арифметичне ознаки $(j = 1, \dots, k)$;

$a_{i,j}$ – коефіцієнт відображення значущості ознаки x_j у головну компоненту y_i.

2. Стандартизація значень вихідного ознакового простору.

На даному етапі здійснюється перехід від вихідного простору ознак $\{p, d, t_s, t_1^w, \dots, t_{10}^w\}$ до простору стандартизованих змінних $x_1, \dots, x_k$ у відповідності до аналітичної моделі центрування (4):

$$\left(x_i = \frac{z_j - \overline{z_j}}{s_j} \right), (j = 1, \dots, k). \tag{4}$$

Середнє арифметичне стандартизованих змінних дорівнює нулю ($x_j = 0$), дисперсія та стандартне відхилення дорівнюють одиниці ($s_1^2 = s_j = 1$) Отже, стандартизовані змінні $x_1, \dots, x_k$ мають однаковий рівень інформативності, а сумарний обсяг інформації, що в них міститься дорівнює (5):

$$k\left(\sum_{j=1}^{k} s_j^2 = k\right). \tag{5}$$

Однак, перед здійсненням стандартизації ознак необхідно реалізувати кодування значень векторів, оскільки біометрична модель M_{u_i} синтезована засобами теорії нечіткої логіки. Так, значення векторів конкретного користувача $u_i \in U$, що представляють собою терми нечіткої множини є категоріальними, а пошук прихованих взаємозв'язків у даних вимагають наявність числових значень.

3. Лінійне перетворення стандартизованого простору ознак.

На даному етапі здійснюється лінійне перетворення стандартизованого простору ознак з метою побудови нового ортогонального простору $y_1, y_2, \dots, y_k$ у відповідності до (6):

$$y_i = \sum_{j=1}^{k} a_{i,j} x_j, (i = 1, \dots, k), \tag{6}$$

де y_i – нова змінна за номером i $(i = 1, \dots, k)$;

x_j – стандартизована змінна за номером j $(j = 1, \dots, k)$;

$a_{i,j}$ – коефіцієнти переходу від набору змінних $x_1, x_2 \dots, x_k$ до $y_1, y_2, \dots, y_k$.

Лінійну модель для стандартизованих змінних на даному етапі доцільно представити у вигляді системи рівнянь (7):

$$\begin{cases} y_1 = a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,k}x_k \\ \dots \\ y_k = a_{k,1}x_1 + a_{k,2}x_2 + \dots + a_{k,k}x_k \end{cases} \tag{7}$$

Коефіцієнти $a_{i,j}$ розраховуються із врахуванням наступних умов:

значення дисперсії нових змінних y_i кількісно рівні власним значенням вихідної матриці кореляцій $s^2(y_i) = \lambda_i$. Сума власних значень матриці кореляцій дорівнює k, а отже, інформація, що міститься в множині стандартизованих змінних $x_1, x_2 \dots, x_k$, повністю зберігається у наборі нових змінних $y_1, y_2, \dots, y_k$;

змінні $y_1, y_2, \dots, y_k$ пронумеровані у порядку зменшення значень дисперсії $s^2(y_1) \geq s^2(y_1) \geq \dots \geq s^2(y_k)$.

Змінні $y_1, y_2, \dots, y_k$ ортогональні, оскільки не корелюють одна з одною.

Таким чином, отримано новий простір ознак КП $y_1, y_2, \dots, y_k$, розмірність якого збігається з розмірністю вихідного простору. Новий простір ортогональний, змінні якого упорядковано за значенням зменшення їх дисперсії.

4. Визначення кількості головних компонент.

На даному етапі здійснюється зменшення ознакового простору біометричної моделі за допомогою "відсікання" певної кількості найменш інформативних змінних з максимальними номерами. Решта m змінних простору $y_1, y_2, \dots, y_m (m \ll k)$ називаються головними компонентами. Так, в процесі визначення головних компонент система k рівнянь (7) зводиться до m рівнянь (8):

$$y_i = \sum_{j=1}^{k} a_{i,j} x_j, (i = 1, \dots, m). \tag{8}$$

Очевидно, що сума дисперсії головних компонент менша, ніж сума дисперсії вихідних змінних k, тому визначення кількості головних компонент доцільно здійснювати засобами критерію, заснованого на власних числах матриці кореляції. Суть даного підходу полягає в тому, щоб обмежити відбір головних компонент тими змінними y_i, яким відповідають власні значення $\lambda_i \geq 1$, тому що їх інформаційна значущість вища за інформаційну значущість відсічених змінних.

5. Синтез остаточного ознакового простору.

На даному етапі здійснюється отримання нового підпростору ознак КП S_{sub} шляхом інтерпретації максимальних за абсолютною величиною навантажень (коефіцієнтів лінійних перетворень $a_{i,j}$) із матриці навантажень у відповідності до кількості, значення якої визначено на попередньому етапі.

Матрицю навантажень на головні компоненти представлено таблицею 1.

Таблиця 1

Матриця навантажень на компоненти

Ознака	y_1	y_2	…	y_m	…	y_k
x_1	$a_{1,1}$	$a_{2,1}$	…	$a_{m,1}$	…	$a_{k,1}$
x_2	$a_{1,2}$	$a_{2,2}$	…	$a_{m,2}$	…	$a_{k,2}$
…	…	…	…	…	…	…
x_k	$a_{1,k}$	$a_{2,k}$	…	$a_{m,k}$	…	$a_{k,k}$

Таким чином, до ознакового простору біометричної моделі додається нечітка підмножина визначених головних компонент (9):

$$M_{u_i} = \{p, d, t_s, t_1^w, \dots, t_{10}^w\} \cup S_{sub} = \{y_1, \dots, y_m\} \rightarrow \{p, d, t_s, t_1^w, \dots, t_{10}^w, y_1, \dots, y_m\}. \quad (9)$$

Оцінка сепарабельності отриманого ознакового простору. Оскільки вирішення завдання регуляризації ознакового простору біометричної моделі КП M_{u_i} вирішує завдання її нелінійної сепарабельності, то оцінку отриманих результатів застосування методу доцільно здійснювати у рамках оцінки сепарабельності моделі до регуляризації її ознакового простору та після.

Оскільки, для n-вимірного ознакового простору множини векторів є лінійно-сепарабельні, якщо вони можуть бути відокремлені (n-1)-вимірною гіперплощиною [24], а також із врахуванням того, що M_{u_i}побудована на основі теорії нечіткої логіки (нечітких множин), то оцінку її сепарабельності доцільно здійснювати на основі міри подібності Жаккара (коефіцієнту флористичної спільноти) [25; 26]. Суть підходу полягає у вимірюванні подібності множин на основі значення співвідношення міри спільної частини і міри їх об'єднання (10).

$$J(A,B) = 1 - J(A,B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cap B|}. \quad (10)$$

Таким чином, міра подібності Жаккара дозволить отримати значення зміни ознакового простору до регуляризації та після (від 0 до 1), де 0 – множини не мають спільних елементів, 1 – множини ідентичні.

Висновки. У статті вирішується актуальне наукове завдання регуляризації ознакового простору біометричної моделі КП користувачів ІС військового призначення у рамках підвищення ефективності процедури автентифікації користувачів системами контролю і розмежування доступу. Обрано біометричну модель КП, особливістю якої є формалізація унікальності користувача ІС на основі виявлення властивих йому закономірностей КП нечіткими правилами.

Запропоновано удосконалений метод регуляризації ознакового простору біометричної моделі КП користувачів ІС військового призначення. Суть запропонованого методу, що

відрізняє його від існуючих, полягає у тому, що збільшення множини ознак біометричної моделі досягається шляхом додавання до неї виявлених прихованих фактів із множини власних ознак на основі факторного аналізу із найбільшим показником їх мінливості.

Застосування даного підходу дозволяє вирішити описані у статті недоліки аналізованих наукових досліджень:

визначати факт підміни уже авторизованого користувача за наявними у системі ідентифікаторами;

вирішити питання нелінійної сепарабельності спільного для усіх користувачів системи ознакового простору;

поєднати переваги імовірнісно-статистичних методів та методів машинного навчання для побудови біометричної моделі КП в умовах прийнятної обчислювальної складності.

Перспективним напрямком подальших наукових досліджень є розробка методики автентифікації користувачів інтелектуальними системами контролю та розмежування доступу ІС військового призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII: станом на 31 берез. 2023 р.

2. Фесьоха В. В. Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального призначення / В. В. Фесьоха, Н. О. Фесьоха, О. Д. Доброштан // Збірник наукових праць ВІТІ. 2020. № 3. С. 129–136.

3. Фесьоха В. В., Фесьоха Н. О. Модель нечіткої автентифікації користувачів інформаційних систем органів військового управління на основі поведінкової біометрі // Захист інформації. 2021. Т. 23, № 2. С. 116–123.

4. Фесьоха В. В., Кисиленко Д. Ю., Турчак О. Р. Перспективи удосконалення існуючих рішень виявлення шкідливого програмного забезпечення в інформаційних системах військового призначення // Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: матеріали ІІ Міжнар. наук.-практ. конф., м. Київ, 1 груд. 2022 р. Київ, ВІТІ ім. Героїв Крут, 2022. С. 216.

5. Zero-day polymorphic cyberattacks detection using fuzzy inference system / I. Y. Subach et al. // Austrian Journal of Technical and Natural Sciences. 2020. Vol. 5, 6. P. 8–13.

6. Алексеев В. А. Сравнительный анализ перспективных технологий аутентификации пользователей ПК по клавиатурному почерку / В. А. Алексеев, Д. В. Маслий, Д. Ю. Горелов // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2017. Вып. 189. С. 195–201.

7. Shklyar E., Vorobyev E., Savelyev M. Browser-based keystroke dynamics recognition. Saint Petersburg Electrotechnical University «LETI». No 5/2019. Pp. 58–63.

8. Young J. R. and Hammon R. W. Method and Apparatus for Verifying an Individual's Identity. Patent Number 4,805,222, U.S. Patent and Trademark Office, Washington, D.C., Feb., 1989.

9. Kim J., Kang P. Recurrent neural network-based user authentication for freely typed keystroke data // arXiv preprint arXiv: 1806.06190. 2018.

10. Continuous authentication by free-text keystroke based on CNN and RNN / X. Lu et al. // Computers & Security. 2020. Vol. 96. P. 101861. URL: https://doi.org/10.1016/j.cose.2020.101861 (date of access: 02.03.2023).

11. Yevetskyi V., Horniichuk I. Analysis of stability of the user's keyboard handwriting characteristics in the biometric authentication systems // Collection "Information technology and security". 2018. Vol. 6, no. 2. P. 19–28. URL: https://doi.org/10.20535/2411-1031.2018.6.2.153487 (date of access: 05.03.2023).

12. Krutohvostov D., Khitsenko V. Password Authentication and Continuous Authentication by Keystroke Dynamics Using Mathematical Statistics // Voprosy kiberbezopasnosti. 2017. № 5 (24). P. 91–99.

13. Чалая Л. Модель идентификации пользователей по клавиатурному почерку // Штучний інтелект. 2004. Т. 4. С. 811–817.

14. Heuristic Methods for Reservoir Monthly Inflow Forecasting: A Case Study of Xinfengjiang Reservoir in Pearl River, China / C.-T. Cheng et al // Water. 2015. Vol. 7, no. 12. P. 4477–4495.

15. Судова почеркознавча експертиза // Київський науково-дослідний інститут судових експертиз. URL: https://kndise.gov.ua/pocherkoznavcha/ (дата звернення: 15.03.2023).

16. L. Rosasco, T. Poggio, A Regularization Tour of Machine Learning, MIT-9.520 Lectures Notes (book draft), 2015.

17. Character recognition using the mahalanobis distance // Taguchi’s quality engineering handbook. Hoboken, NJ, USA. С. 1288–1292.

18. Krutohvostov D., Khitsenko V. Password Authentication and Continuous Authentication by Keystroke Dynamics Using Mathematical Statistics // Voprosy kiberbezopasnosti. 2017. № 5 (24). P. 91–99.

19. Фесьоха В., Фесьоха Н. Удосконалена процедура автентифікації користувачів інформаційних систем військового призначення на основі аналізу біометричного профілю клавіатурного почерку // InterConf: матеріали 8-ї Міжнар. науково-практ. конф. «Глоб. Та регіон. Аспекти сталого розвитку», м. Копенгаген, 26–28 берез. 2023 р. 2023. С. 505–506.

20. Nikitin V. V., Bobin D. V. Principal component analysis for weighted data in the procedure of multidimensional statistical forecasting // Statistics and economics. 2021. Т. 18, № 2. С. 4–11.

21. Халимов Г. Анализ методов гарсия и главных компонент биометрической идентификации личности // Системи обробки інформації. 2013. № 5. С. 106–110.

22. Jolliffe I. T. Principal component analysis. 2nd ed. New York: Springer, 2002. 487 p.

23. Principal manifolds for data visualization and dimension reduction / ed. By A. N. Gorban et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

24. Сайфуллин Р., Александров С. Этапы реализации метода главных компонент при обработке сигналов аналитических приборов // Вестник самарского государственного технического университета. Серия «технические науки». 2018. Т. 26, № 2. С. 60–66.

25. Gruzling N. Linear separability of the vertices of an n-dimensional hypercube. Northern British Columbia: The University of Northern British Columbia, 2006. 88 p.

26. Jaccard P. Distribution de la flore alpine dans le Bassin des Dranses et dans quelques regions voisines // Bull. Soc. Vaudoise sci. Natur. 1901. V. 37, Bd. 140. S. 241–272.

DOI: 10.58254/viti.3.2023.18.163

УДК: 623.368

Чередниченко О. Ю. ORCID: 0000-0002-0816-8321 (ВІТІ ім. Героїв Крут)
Паламарчук Н. А. ORCID: 0000-0001-8818-7794 (ВІТІ ім. Героїв Крут)
Шемендюк О. В. ORCID: 0000-0002-5594-2973 (ВІТІ ім. Героїв Крут)
Мартинюк В. В. ORCID: 0000-0003-0244-7861 (ВІТІ ім. Героїв Крут)

СИНТЕЗ СИСТЕМИ ВИЯВЛЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ НА БАЗІ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

У статті проведено аналіз вибухонебезпечних предметів різних типів та надана їхня характеристика. Демаскуючою їхньою ознакою є матеріал основної частини (корпусу), відмічено, що для фугасних мін характерне використання пластикового корпусу, для мін осколкової дії – металевого, найбільш складними для виявлення є міни з пластиковим корпусом. Розглянуто способи виявлення вибухонебезпечних предметів порівняно з тими, що застосовуються на цей час в Україні. На жаль, з огляду на масштаб замінованих територій вони є малоефективними, тому вочевидь необхідна розробка більш ефективних рішень для їх виявлення і знешкодження на основі сучасних досягнень технічного прогресу. Зарубіжні країни розробили та використовують сучасні мобільні робототехнічні комплекси для розмінування на базі безпілотних літальних апаратів зі встановленими на них датчиками різного типу.

Доцільним є створення універсальної системи виявлення, яка може бути розгорнута на будь-якому безпілотному літальному апараті вертолітного типу (квадрокоптер, мультикоптер), на якому встановлено декілька датчиків виявлення одночасно з метою ведення розвідки мінної обстановки, виявлення мін і дистанційного їх знищення. В статті запропоновано синтез системи виявлення вибухонебезпечних предметів на базі безпілотного літального апарата зі встановленим на ньому тепловізором, в поєднанні з металошукачем та маніпулятором із вибухівкою для дистанційного розмінування. Розглянуто параметри виявлення вибухонебезпечних предметів, тип сенсорних датчиків та основні функції системи. Запропоновано алгоритм дій оператора системи з виявлення вибухонебезпечних предметів.

Ключові слова: *вибухонебезпечні предмети, міни, протипіхотні міни, виявлення вибухонебезпечних предметів, розмінування, дистанційне розмінування, безпілотний літальний апарат, тепловізор, металошукач.*

O. Cherednychenko, N. Palamarchuk, O. Shemendiuk, V. Martynyuk Synthesis of the system for detection of explosive objects on the base of an unmanned aerial vehicle.

The article analyzes explosive objects of various types and provides their characteristics. Their unmasking feature is the material of the main part (casing), it is noted that high-explosive mines are characterized by the use of a plastic casing, for fragmentation mines – a metal casing, and the most difficult to detect are mines with a plastic casing. Methods of detecting explosive objects compared to those currently used in Ukraine are considered. Unfortunately, given the scale of mined areas, they are ineffective, so it is obviously necessary to develop more effective solutions for their detection and neutralization based on modern achievements of technical progress. Foreign countries have developed and use modern mobile robotic complexes for demining based on unmanned aerial vehicles with various types of sensors installed on them.

It is expedient to create a universal detection system that can be deployed on any helicopter-type unmanned aerial vehicle (quadcopter, multicopter), on which several detection sensors are installed at the same time for the purpose of reconnaissance of the mine situation, detection of mines and their remote destruction. The article proposes the synthesis of a system for detecting explosive objects based on an unmanned aerial vehicle with a thermal imager installed on it, in combination with a metal detector and a manipulator with explosives for remote demining. The parameters of detection of explosive objects, the type of sensor sensors and the main functions of the system are considered. The algorithm of actions of the operator of the system for detecting explosive objects is proposed.

Keywords: *explosive objects, mines, anti-personnel mines, detection of explosive objects, demining, remote demining, unmanned aerial vehicle, thermal imager, metal detector.*

Постановка завдання. Внаслідок повномасштабного вторгнення російської федерації в Україну майже 30 % її території виявилася забруднена або потенційно забруднена різними типами вибухонебезпечних предметів (далі – ВНП), що становить значну загрозу для життя і здоров’я цивільного населення та військових, які здійснюють виконання бойових завдань у зонах бойових дій та на деокупованих територіях. Процес розмінування та очищення місцевості від ВНП досить складний та довгий. Найнадійніший та безпечніший спосіб – це розмінування за допомогою механічного тралення, але, на жаль, в Україні відсутня необхідна кількість тралів, та специфіка місцевості не завжди дозволяє їх використовувати. Тому, доводиться застосовувати ручне розмінування, а це важка, виснажлива, довготривала та небезпечна праця саперів.

Застосування безпілотних літальних апаратів (далі – БпЛА) в сучасних війнах дозволяє вести розвідку вздовж всієї лінії фронту, виявляти сили та ворожу техніку, дистанційно коригувати артилерійський вогонь, здійснювати пошуково-рятувальні роботи та скидати вибухівку на ворожі об’єкти. Новою та важливою сферою застосування БпЛА є виявлення та знешкодження ВНП. На сьогодні зарубіжні країни розробили та використовують сучасні мобільні робототехнічні комплекси (далі – РТК) для розмінування, найбільш перспективні з них – це комплекси на базі БпЛА зі встановленими на них датчиками різного типу. Різні типи РТК використовуються для виявлення пластикових або металевих ВНП, але наразі не існує універсальної системи для виявлення ВНП різних типів одночасно. Тому, доцільним буде створення універсальної системи виявлення як пластикових, так і металевих ВНП.

Аналіз основних досліджень і публікацій. Вирішенням проблеми розмінування займаються вітчизняні фахівці, вчені, та залучаються закордонні неурядові організації в межах гуманітарного розмінування. Саме закордонні фахівці значно просунулися у сфері застосування різних типів датчиків на базі БпЛА [1]. Датчики активно застосовуються цивільними у гірничовидобувній сфері в пошуках корисних копалин [2–4] та військовими у сфері виявлення ВНП. Нині країни-члени НАТО активно використовують БпЛА для виявлення металевих [5] та пластикових [6] мін. Також існують певні комбіновані зразки для виявлення ВНП різних типів [7]. Але наразі не існує єдиної універсальної системи для виявлення та знешкодження ВНП одночасно. Тому виникає задача синтезу системи на базі БпЛА для виявлення різних типів ВНП та подальшого їх знешкодження. Такий підхід дає змогу швидко впроваджувати БпЛА з різними типами датчиків у спеціалізовані підрозділи, що значно підвищить ефективність розмінування.

Мета статті – визначення основних етапів синтезу системи виявлення ВНП на базі БпЛА.

Виклад основного матеріалу.

У зв’язку з повномасштабним російським вторгненням Україна стала найбільш замінованою країною у світі. Прийнято вважати, що рік війни – це 10 років на розмінування. Враховуючи, що військові дії почалися ще у 2014 році, завдання розмінування постраждалих територій стоїть давно та погіршується з кожним днем. Аналіз ВНП [8] показав, що найбільш розповсюдженими є протипіхотні фугасні міни, міни пастки, протитанкові міни фугасної дії, протипіхотні міни осколкової дії, протитанкові міни дистанційного мінування, їхні характеристики представлено в таблиці 1.

Таблиця 1

Характеристики ВНП

Класифікація ВНП	Назва ВНП	Матеріал корпусу	Вибухова речовина	Принцип дії
Протипіхотні фугасні міни	ПМН-4	Пластмаса	(ТГ-40 – тротил 40 %, гексоген 60 %) – 0,05 кг	Натискна
	ПМН	Пластмаса	(тротил) – 0,2 кг	Натискна
	ПФМ-1	Поліетилен	(ВС-6Д) – 0,04 кг	Натискна
	ПМН-2	Пластмаса	(ТГ-40 – тротил 40 %, гексоген 60 %) – 0,1 кг	Натискна
Міни-пастки	Міна-пастка МЛ-7	Пластмаса	(30гр – ВР-5, 10гр – тетрил) – 0,04 кг	Розвантажувальна
	Міна-сюрприз МС-3	Пластмаса	(тротил) – 0,2 кг	
Протитанкові міни фугасної дії	ТМ-62М	Сталь	(ВВО-32) – 8,2 кг	Натискна
	ТМ-62ПЗ	Поліетилен	(ВВО-32) – 8,2 кг	Натискна
Протипіхотні міни осколкової дії	ПОМ-2	Сталь	(ПВВ-4) – 0,14 кг	Натяжної, дистанційного мінування
	МОН-50	Пластмаса	(ПВВ-4) – 0,7 кг	Керована спрямованої дії
	ПОМЗ-2М	Чавун	(тротил) – 0,075 кг	Натяжної дії
	МОН-90	Пластмаса	(ПВВ-4) – 6,2 кг	Керована спрямованої дії
	МОН-100	Сталь	(тротил) – 2 кг	Керована спрямованої дії
	МОН-200	Сталь	(тротил) – 12 кг	Керована спрямованої дії
	ОЗМ-72	Чавун	(МС) – 0,66 кг	Кругове ураження, що вистрибує
Протитанкові міни дистанційного мінування	ПТМ-1	Поліетилен	(ПВВ-12С-1) – 1,1 кг	Натискна
	ПТМ-3	Сталь	(тротил, ТГА, МС) – 1,8 кг	Натискна

У таблиці описано принцип дії ВНП та матеріали, з якого виготовлена їх основна частина (корпус). Звідси бачимо, що для фугасних мін характерне використання пластмас, для мін осколкової дії – метал. Відповідно, матеріал виготовлення корпусу виступатиме демаскуючою ознакою ВНП. Згідно з таблицею бачимо, що в основному для корпусу характерний матеріал виготовлення пластмаса, яку виготовляють за технологією лиття під тиском, завдяки цьому ВНП має високу ступінь ударомiцності, стійкість до вологи та переносимість впливу високих температур. Таким чином, ВНП з пластиковим корпусом мають дуже малий вміст металу, що ускладнює їх виявлення металошукачами.

Аналіз найбільш поширених ВНП на території України дає підґрунтя для синтезу системи виявлення ВНП (далі – СВВ) (рис 1).

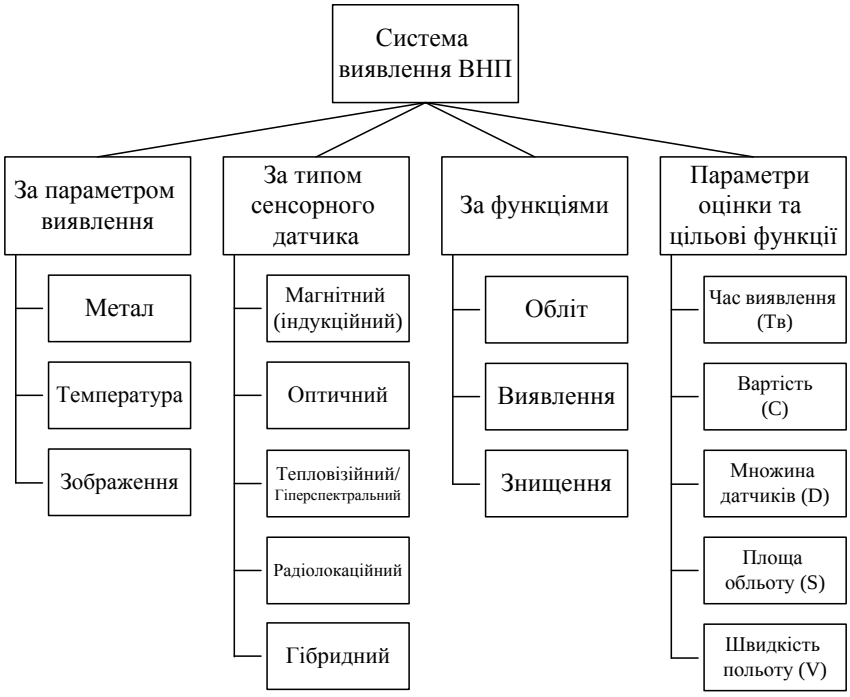


Рис. 1. Складові етапів синтезу СВВ

Розглянемо складові етапів синтезу СВВ.

За параметром виявлення. Виявлення ВНП здійснюється двома основними способами: пошук металевих (металовмісних) ВНП за допомогою металошукача (під землею або на поверхні землі); пошук пластикових ВНП за допомогою візуального або програмного аналізу зображення з тепловізійної та оптичної камери (ВНП, що знаходяться на поверхні землі). Зазначені способи є базовими при виявленні ВНП і являтимуть основу в запропонованому синтезі СВВ.

При пошуку та виявленні металовмісних ВНП важлива не стільки маса конкретного ВНП, скільки площа поверхні, пов'язана з його діаметром d. Для оцінки максимальної глибини h_{max} виявлення ВНП за допомогою звичайного металошукача в умовах сухого ґрунту (провідністю 10^4 Ом·м – 10^5 Ом·м) допустима інженерна формула (1) [9]:

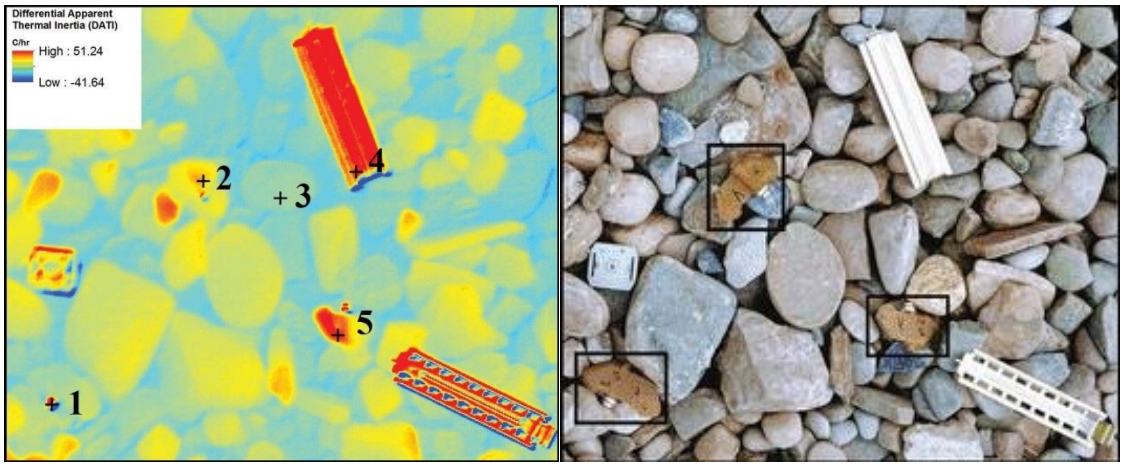
$$h^2_{max}=11d, \quad (1)$$

де d – діаметр (мінімальний габарит) ВНП.

Слід пам'ятати, що основною функцією металошукача є виявлення металу у міні, а оскільки багато років використовуються міни в неметалевих корпусах, то це значно ускладнює роботу з їх виявлення. Також уповільнює процес виявлення ВНП за допомогою металошукача наявність хибних сигналів від осколків снарядів та інших металів, якими перенасичений ґрунт внаслідок ведення бойових дій. За даними [10], отриманими під час перевірки ґрунтової дороги в Донецькій області, на кілометр дороги шириною до 9 м було зафіксовано близько 4700 хибних сигналів або 80900 хибних сигналів на одну виявлену міну. Це призводить до зниження темпів розмінування, швидкої стомлюваності саперів і зростання

небезпеки пропуску ВНП. Тому, використання одного способу буде недостатнім та малоефективним [9; 10].

Використання тепловізійної камери [6] дозволяє знайти пластикові міни на поверхні, а при певних умовах і на невеликій глибині. Використання тепловізору доцільніше при зростанні або зменшенні температури, оскільки всі матеріали відбивають, поглинають, передають і випромінюють теплове випромінювання з різною швидкістю. Через свій фізичний і хімічний склад пластиковому корпусу міни властиво швидко нагріватися та охолоджуватися, і цим він кардинально відрізняється від навколишнього середовища. Ці контрасти в швидкості нагрівання та охолодження потенційно найбільш виражені в ранкові та вечірні години після сходу і заходу сонця, коли відбувається висока зміна температури, тому оператору доцільно дотримуватися цих вимог при виявлення ВНП, що не містять метал. Наприклад, неглибоко закопані у пісок міни мають деякі затримки теплообміну, через що ділянки, де вони закопані, будуть повільніше нагріватися зранку та охолоджуватися ввечері. Для прикладу, результати сканування території за допомогою БПЛА з тепловізором представлені на рисунку 2.



а) б)

Рис. 2. Приклад відображення температури різних предметів в період з 06:50 до 07:10 ранку:
а: *1* – алюмінієвий детонатор протипіхотної фугасної міни ПФМ-1 (далі – ПФМ-1); *2* – корпус міни ПФМ-1; *3* – загальний фон; *4* – частина касети КСФ-1; *5* – крило ПФМ-1;
б: загальний фон, в чорних квадратах відображені міни ПФМ-1

Встановлення поряд з тепловізійною камерою оптичної камери з високою роздільною здатністю та встановлення на ній того ж ракурсу надає змогу оператору порівняти дані з датчиків (сенсорів) із зовнішнім виглядом місцевості і зробити висновки щодо вірного чи хибного їх спрацювання у випадках, коли ВНП знаходяться на поверхні землі.

Використання зазначеного обладнання у поєднанні із геоінформаційною системою дає змогу виявляти ВНП із дуже високою точністю, визначати їхні координати, тип, глибину залягання, створювати карту розташування ВНП у автоматичному режимі та в масштабі реального часу.

За типом сенсорного датчика. Для вирішення своїх функцій обладнання БпЛА може містити не тільки штатні оптичні відеокамери, а і додаткові датчики, перспективними з яких є:

гіперспектральна камера дистанційного зондування земної поверхні;

інфрачервона (тепловізійна) камера;

радіолокаційний підповерхневий локатор для пошуку ВНП (георадар);

мобільний металошукач;

магнітометр.

На основі аналізу параметрів виявлення ВНП пропонується використовувати систему для виявлення ВНП із декількома датчиками виявлення (гібридного типу), котрі інтегровані у систему БпЛА. Зазвичай існуючі системи виявлення ВНП використовують лише один із

типів датчиків (виявлення ВНП за одним із параметрів), що значно зменшує кількість об’єктів, які можуть бути виявлені. Тому, доцільним є створення універсальної системи, яка може бути використана будь-яким БпЛА, котрий відповідає певним тактико-технічним характеристикам, та використовує декілька способів (датчиків) виявлення одночасно.

За допомогою СВВ на БпЛА вирішується основна задача – обліт БпЛА території розмінування, пошук, виявлення ВНП (з визначенням їхніх координат), які відкрито розміщені на земній поверхні або на глибині, та передача цієї інформації оператору.

Запропонована узагальнена структура СВВ на БпЛА представлена на рисунку 3, до її складу входять різні датчики виявлення та система управління, яка містить наступні підсистеми: виявлення (розпізнавання) ВНП, управління польотом БпЛА, радіозв’язку та знищення ВНП.

Підсистема виявлення (розпізнавання) ВНП забезпечує збір даних з датчиків БпЛА при досягненні певних цільових функцій управління.

Підсистема управління польотом забезпечує політ БпЛА за розрахованою траєкторією, з певною швидкістю і висотою.

Підсистема радіозв’язку забезпечує обмін даними між СВВ на БпЛА і оператором.

Підсистема знищення ВНП забезпечує дистанційне знищення ВНП за допомогою вибухівки.

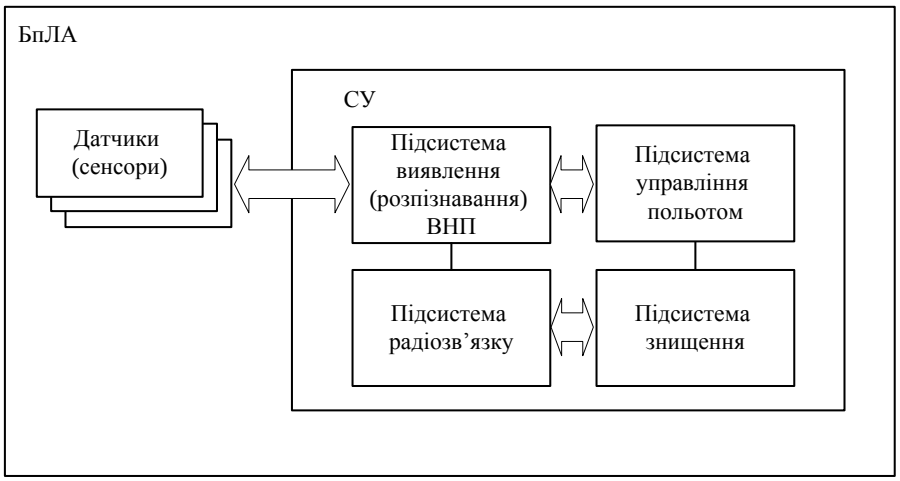
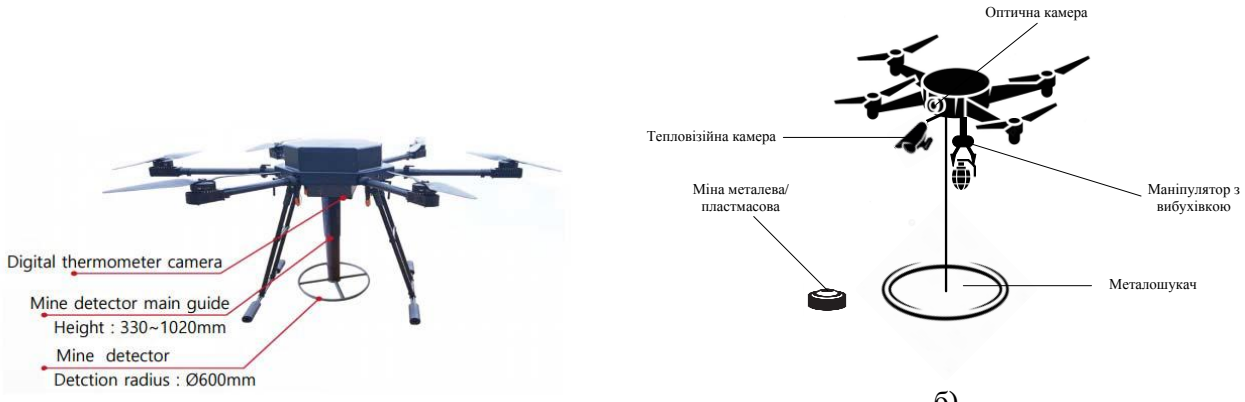


Рис. 3. Узагальнена структура СВВ на БпЛА

Варіант компоновки елементів СВВ на базі БпЛА представлений на рисунку 4. У системі пропонується використовувати наступні датчики: тепловізійна та оптична камери, металошукач [5; 9] та маніпулятор з вибухівкою для дистанційного розмінування.



а) б)

Рис. 4. Варіант компоновки СВВ:

а – існуюча комбінована система; *б* – перспективна система з маніпулятором для вибухівки

За функціями СВВ.

1. Робота оператора в СВВ починається з побудови маршруту розмінування та введення координат в налаштуваннях БпЛА. Типовий маршрут обльоту БпЛА замінованої місцевості представлений на рисунку 5.

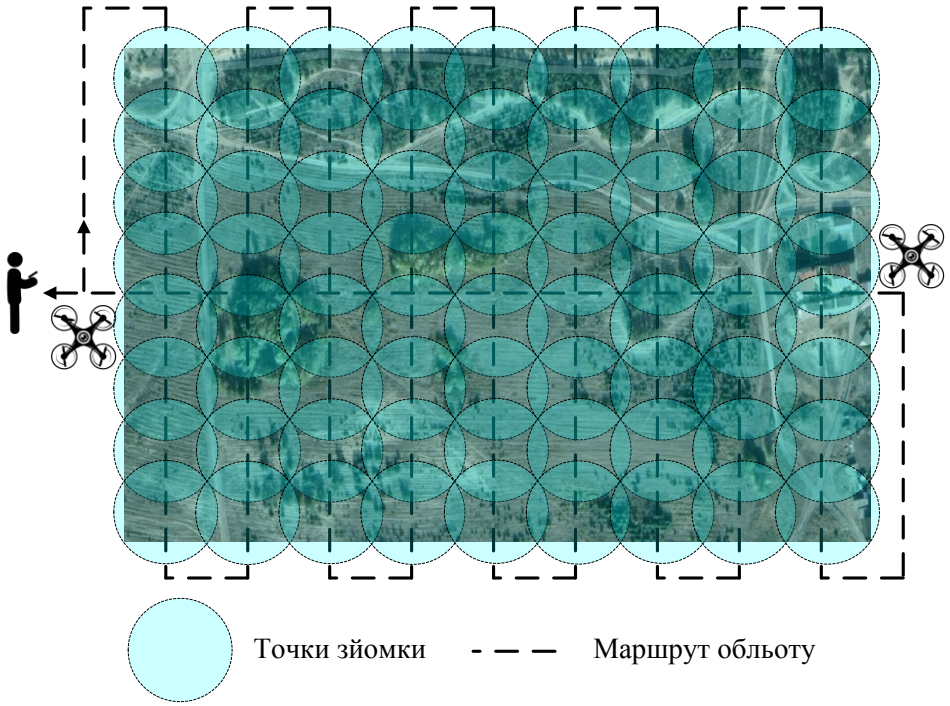


Рис. 5. Типовий маршрут обльоту БпЛА замінованої місцевості

2. Під час обльоту території оператором аналізується зображення з оптичної та тепловізійної камери [6] для пошуку ВНП, що знаходяться на поверхні. Зображення території на знімках оптичної камери з гарною розподільчою здатністю дозволяє провести поверхневий аналіз ґрунту за допомогою нейронних мереж або власноруч спеціалістом.

3. Одночасно за допомогою металошукача здійснюється пошук металовмісних предметів на поверхні землі та під землею. Особливістю використання металошукача (який є звичайною котушкою) на базі БпЛА є необхідність розміщення її на відстані не менш ніж 30 см від БпЛА, для уникнення перешкод при передачі даних із системи БпЛА до оператора. Також при пошуку критичною є відстань між поверхнею землі та металошукачем [5; 7; 9], яка не повинна бути більш ніж 20 см, інакше металошукач ігнорує об’єкти, котрі знаходяться під землею (оператор повинен постійно контролювати цю відстань).

4. На завершальному етапі, якщо оператор підтверджує виявлення ВНП, за допомогою маніпулятора буде здійснюватися закладення вибухівки на місця виявлення ВНП і проводитися дистанційний підрив, завчасно відвівши БпЛА на безпечну відстань. Для наглядності приведемо алгоритм дій оператора з виявлення ВНП (рис. 6).

Завдяки отриманню даних в режимі онлайн оператор може приймати рішення щодо виявлення ВНП в режимі реального часу або вести запис цих даних у зручній для нього формі та повертатися до відмічених ділянок пізніше. Наприклад, якщо оператор має сумніви щодо виявлення ВНП, він може поставити маркер на карті і повернутися до нього повторно, або власноруч зробити перевірку підозрілого предмету на місцевості. Доцільним рішенням можна вважати створення карти із відображенням отриманих та оброблених даних у певних ділянках пройденого шляху, це дозволить зберігати усі отримані дані та відображати їх, наприклад, у вигляді зображень. Для створення таких карт система має отримувати не тільки дані про наявність або відсутність ВНП, а й про переміщення БпЛА у просторі. Запропонований варіант СВВ ВНП буде достатнім для виявлення більшості ВНП, що знаходяться на поверхні.

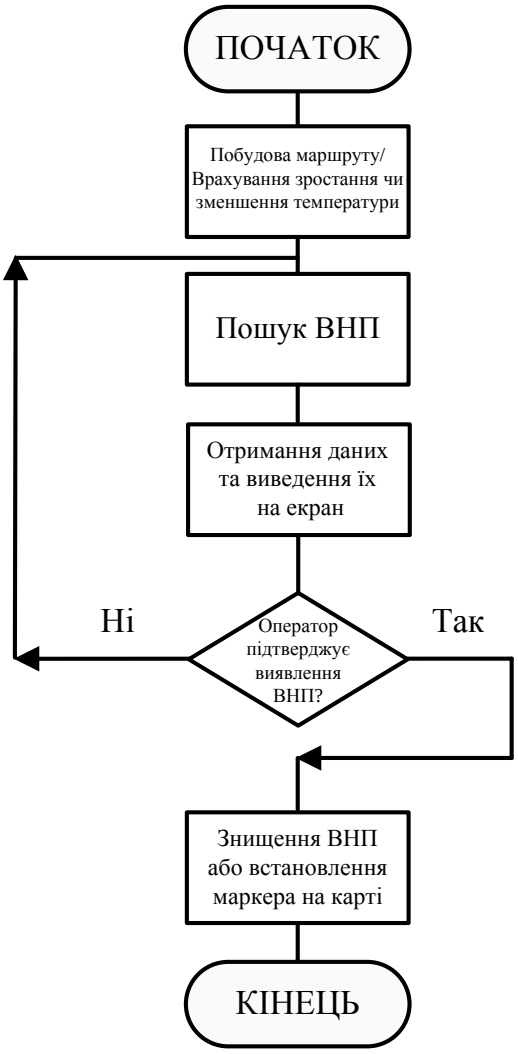


Рис. 6. Алгоритм дій оператора з виявлення ВНП

Параметри оцінки та цільові функції. Ефективність використання СВВ на базі БпЛА залежить від комплексу засобів пошуку, що використовуються для вирішення поставлених завдань, лише комплексне поєднання та використання сучасних засобів і способів розвідки й розмінування дозволить ефективно вирішувати завдання з виявлення ВНП [11].

Параметри оцінки ефективності функціонування СВВ залежать від наступних вихідних даних:

множина датчиків $D = \{d_1, d_2, \ldots, d_i, \ldots, d_n\}$, $i = 1 \ldots n$;

площа обльоту замінованої території $S = [S_{min}, S_{max}]$;

швидкість польоту з врахуванням заданої ймовірності виявлення ВНП на одиницю площі $V = [V_{min}, V_{max}]$.

Оцінка ефективності пошуку ВНП здійснюється за критерієм:

мінімум ***часу виявлення*** $T_в$ ВНП – за мінімальний (обмежений) час польоту (один раунд обльоту) з забезпеченням заданої ймовірності виявлення з отриманими даними від всіх датчиків становить:

$$T_в \rightarrow \min \text{ або } T_в \leq T_{взад},$$

де $T_{взад}$ – заданий час виявлення ВНП.

Час виявлення ВНП залежить від характеристик БпЛА (тривалість, швидкість і висота польоту, радіообладнання й ін.), характеристик датчиків, вимог щодо ймовірності виявлення ВНП, параметрів довжини маршруту тощо. Довжина маршруту залежить від кількості точок збору інформації, їх розміщення. Зі збільшенням висоти польоту БпЛА збільшується зона покриття, однак гранична висота обмежена відстанню котушки металошукача до землі, тому будемо вважати, що $h \leq 20$ см.

Зменшення ***вартості*** СВВ C становить:

$$C \rightarrow \min,\ C = C_E + C_P + C_O ,$$

де C_E – вартість експлуатації; C_P – вартість розробки; C_O – вартість обладнання.

Висновки. У статті проаналізовано вихідні дані найбільш розповсюджених ВНП на території України. На основі аналізу ВНП сформовані вимоги до створення СВВ. Визначені складові етапів синтезу СВВ: параметри виявлення, типи датчиків, функції, параметри оцінки та цільові функції.

Подальшим напрямком наукових досліджень може бути інтегрування бази сигнатур ВНП за допомогою нейронних мереж в процес функціонування СВВ із врахуванням міжнародних стандартів з питань протимінної діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Balestrieri E., Daponte P., De Vito L., Picariello F., Tudosa I. Sensors and Measurements for UAV Safety: An Overview. Sensors 2021, 21, 8253.

2. Shahmoradi J., Talebi E., Roghanchi P., Hassanalian M. A Comprehensive Review of Applications of Drone Technology in the Mining Industry. Drones 2020, 4, 34.

3. Ren H., Zhao Y., Xiao W., Hu Z. A review of UAV monitoring in mining areas: current status and future perspectives. Int J Coal Sci Technol (2019), 6(3): 320–333.

4. He X., Yang X., Luo Z., Guan T. Application of unmanned aerial vehicle (UAV) thermal infrared remote sensing to identify coal fres in the Huojitu coal mine in Shenmu city, China.

5. Ackerman E. Metal-Detecting Drone Could Autonomously Find Land Mines.

6. Drones with cameras learned to find dangerous mines-butterfly.

7. Kovács Z., Ember I. Landmine detection with drones. Land Forces Academy Review Vol. XXVII, No. 1 (105), 2022.

8. Наука про цивільний захист як шлях становлення молодих вчених / Матеріали Всеукраїнської науково-практичної конференції курсантів, студентів, ад'юнктів (аспірантів). Черкаси: Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, 2022. 305 с.

9. Молочко С. М., Башинський В. Г., Каламурза О. Г., Журахов В. А. Аналіз сучасного стану, характеристик та перспектив розвитку датчиків виявлення вибухонебезпечних предметів, встановлених на БпАК, збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2021. № 8 (2). С. 80–90.

10. Колос Р. Л., Фтемов Ю. О. Організація виконання робіт з розмінування місцевості від вибухонебезпечних предметів, військово-технічний збірник. 2017. № 17. С. 53–60.

11. Романюк В. А., Лисенко О. І., Романюк А. В., Новіков В. І., Гуйда О. Г. Метод збору інформації з вузлів безпроводової сенсорної мережі з використанням інтелектуальних адаптивних літаючих інформаційно-телекомунікаційних роботів, вчені записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71). № 2. С. 25–35.

DOI: 10.58254/viti.3.2023.19.171

УДК 519.718.2

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)

МЕТОДИЧНИЙ ПІДХІД ДО ВІДНОВЛЕННЯ ПРАВИЛЬНОГО ФУНКЦІОНУВАННЯ ВБУДОВАНИХ СИСТЕМ НА РІВНІ ПРОГРАМОВАНОЇ ЕЛЕМЕНТНОЇ БАЗИ

У статті запропоновано методичний підхід до відновлення правильного функціонування спеціалізованих мікропроцесорних систем управління на рівні програмованої елементної бази. Цей підхід включає два етапи.

На першому етапі вирішується основна задача технічної діагностики, а саме розпізнавання стану спеціалізованої мікропроцесорної системи, яка включає в себе: оцінку технічного стану, прогнозування, виявлення та локалізацію несправностей. Дана задача вирішується шляхом виявленням помилок в роботі спеціалізованої мікропроцесорної системи управління, які спричинені відмовою та збоєм цифрових пристроїв, помилками в програмному забезпеченні, або іншими причинами, застосовуючи існуючі методи контролю, а також локалізацією несправностей спеціалізованої мікропроцесорної системи управління, застосовуючи методи тестового та функціонального діагностування цифрових пристроїв, які є складовою системи, яка розглядається.

На другому етапі здійснюється відновлення правильного функціонування спеціалізованої мікропроцесорної системи управління шляхом реконфігурації її внутрішньої структури на рівні логічних елементів. При цьому в основу реконфігурації внутрішньої структури покладене положення прескриптивної теорії, яка розглядає питання цілеспрямованого управління об’єктами різної природи, які перебувають у стані «конфлікту» з іншими об’єктами.

Реалізація запропонованого підходу в подальшому може бути основою для проектування активних відмовостійких систем, які будуть здатні протидіяти відмовам та збоям апаратного та програмного характеру в наслідок внутрішніх або зовнішніх несприятливих впливів.

Ключові слова: *прескриптивна теорія, реконфігурація, спеціалізована мікропроцесорна система управління, вбудована система, контроль і діагностування цифрових пристроїв, відновлення правильного функціонування.*

S. Shtanenko, Y. Samokhvalov. S. Toliupa Methodological approach to recovery correct functioning of embedded systems at the level of programmable element base.

The article proposes a methodical approach to restoring the proper functioning of specialized microprocessor control systems at the level of the programmable element base. This approach includes two stages.

At the first stage, the main task of technical diagnostics is solved, namely the recognition of the state of a specialized microprocessor system, which includes: assessment of the technical state, forecasting, detection and localization of malfunctions. This task is solved by detecting errors in the operation of a specialized microprocessor control system, which are caused by the failure and failure of digital devices, errors in software, or other reasons, using existing control methods, as well as localization of malfunctions of a specialized microprocessor control system, using methods of test and functional diagnostics digital devices that are part of the system under consideration.

At the second stage, the correct functioning of the specialized microprocessor control system is restored by reconfiguring its internal structure at the level of logical elements. At the same time, the reconfiguration of the internal structure is based on the position of the prescriptive theory, which considers the issue of purposeful management of objects of various nature, which are in a state of "conflict" with other objects.

The implementation of the proposed approach in the future can be the basis for the design of active fault-tolerant systems that will be able to counteract failures a hardware and software nature as a result of internal or external adverse actions.

Keywords: *prescriptive theory, reconfiguration, specialized microprocessor control system, embedded system, control and diagnostics of digital devices, restoration of proper functioning.*

Постановка завдання. Вбудовані системи (Embedded Systems) являють собою спеціалізовані мікропроцесорні системи управління, концепція розробки яких ґрунтується на тому, що такі системи взаємодіють з об’єктом управління або контролю, будучи вбудованими безпосередньо у пристрій, яким вони управляють [1; 2].

На сьогоднішній день вбудовані системи широко використовуються в різних галузях діяльності, таких як: машинобудування та верстатобудування, авіація, автомобілебудування, атомна енергетика, банківська сфера, військово-промисловий комплекс, а також

застосовуються як основа побудови автоматизованих систем управління, засобів автоматичного регулювання та управління технологічними процесами.

Слід зазначити, що перші вбудовані системи розроблялися як спеціалізовані цифрові пристрої на базі інтегральних схем малого та середнього ступеня інтеграції. Однак, з появою мікроконтролерної та мікропроцесорної техніки, а пізніше інтегральних схем із програмованою структурою, поняття вбудованої системи сильно трансформувалося. Так, якщо перші вбудовані системи являли собою спеціалізовану структуру, яка мала у своєму складі центральний процесор, окремі інтегральні схеми контролерів периферійного обладнання, цифрових запам'ятовуючих пристроїв, то сучасні вбудовані системи реалізують вже технологію System-on-Chip (SoC) – система на кристалі [3; 4].

Під системою на кристалі (System on Chip – SoC) мають на увазі обчислювальну систему, реалізовану в інтегральному виконанні, до складу якої входить високопродуктивний процесор або кілька процесорів, математичний процесор обробки даних та цифрової обробки сигналів, додаткові модулі пам'яті, набори периферійних пристроїв (контролерів) тощо. Така організація обчислювальної системи набула широкого поширення за допомогою своєї універсальності, малого енергоспоживання і навіть можливості реконфігурації її алгоритмічної структури. Зазначимо, що на сьогодні системи на кристалі витісняють громіздкі обчислювальні структури, реалізовані за допомогою набору інтегральних схем, замінюючи їх сучасними мікроконтролерами (PIC, AVR, MSP430, STM32, Cortex-M, TSP32 тощо), програмованими логічними інтегральними схемами (ПЛІС – CPLD, FPGA, FLEX) та одноплатними комп'ютерами типу Raspberry Pi [5].

Крім цього, слід врахувати, що створення сучасних систем, які використовують технологію System-on-Chip, засноване на застосуванні високотехнологічних САПР функціональних цифрових пристроїв, що вимагає від розробників глибоких знань не тільки цифрової схемотехніки та архітектури обчислювальних систем, але і знання методів синтезу спеціалізованих пристроїв з мікропрограмним управлінням, знання мов опису апаратури та розробки програмного коду, а також методів контролепридатного синтезу. Таким чином, враховуючи вищесказане, актуальною науковою задачею є визначення технічного стану вбудованої системи реалізованої відповідно до концепції System on Chip та відновлення її правильного функціонування з припущенням, що в якості елементної бази використовуються програмовані логічні інтегральні схеми.

Аналіз останніх публікацій. На сьогодні питанням проєктування та функціонування вбудованих систем присвячено велику кількість наукових праць. Так, у роботі [6] розглянуто задачу підвищення якості функціонування мікропроцесорів, що використовуються в системах контролю та управління доступом. Виділено вимоги, а також запропоновано варіант складу команд, які необхідні для якісної побудови мікропроцесорів, що працюють на основі системи залишкових класів, для контролю та управління доступом. У [7] наведено огляд засобів проєктування вбудованих мікропроцесорних систем, що реалізуються на основі програмованих логічних інтегральних мікросхем та розглянуті інструменти налагодження програмного забезпечення мікропроцесорних систем на основі ядер сімейства Pico Blaze, Micro Blaze та Power PC. У [8] розглянуто задачу організації апаратної частини вбудованих мікропроцесорних систем, а також синтез елементів вбудованих систем на програмованій логіці на основі моделі програмно-керуючого автомата. У роботі [9] розглянуто модельно-орієнтоване проєктування за допомогою програмних продуктів Math Works, що дозволяють автоматизувати процес розробки, налагодження та верифікації програмного забезпечення для систем управління. Крім цього у роботі [10] представлений спосіб відбору інтегральних схем по стійкості до електрорушійної сили з використанням критичної напруги живлення. У роботі [11] розглядається технологія застосування методу власного випромінювання для відзначення несправного радіоелектронного компонента в складі цифрового блока сучасного радіоелектронного обладнання за допомогою автономної автоматизованої системи діагностування.

Однак проведений аналіз показує, що на сьогодні не в повному обсязі висвітлені питання, які пов'язані з виявленням та локалізацією відмов спеціалізованих мікропроцесорних систем управління, а також оперативного автоматичного відновлення правильного їх функціонування. Крім цього необхідно враховувати, що існуючі методи контролю та діагностування, як правило, розробляються для конкретного типу інтегральних схем, що не є завжди прийнятним для застосування щодо конкретного екземпляра.

Таким чином, **метою статті** є розробка методичного підходу до відновлення правильного функціонування спеціалізованої мікропроцесорної системи управління на рівні програмованої елементної бази за результатами самодіагностування.

Виклад основного матеріалу.

Контроль та діагностування мікропроцесорних систем. Під контролем мікропроцесорних (обчислювальних) систем розуміється процес отримання інформації, що дозволяє визначити технічний стан обчислювальної системи, застосувавши апаратні, програмні та комбіновані методи та засоби контролю, встановити її відповідність вимогам, що висуваються до даного типу систем [12].

При цьому для оцінки ефективності методів контролю можна використовувати коефіцієнт якості обчислювальної системи з контролем, який визначається як ймовірність видачі безпомилкового результату перетворення інформації

$$K(t) = 1 - P_{\text{пом}},$$

де $P_{\text{пом}}$ – ймовірність пропуску помилок системою контролю при видачі результату перетворення інформації в обчислювальній системі.

На рисунку 1 представлені основні види контролю обчислювальних систем.

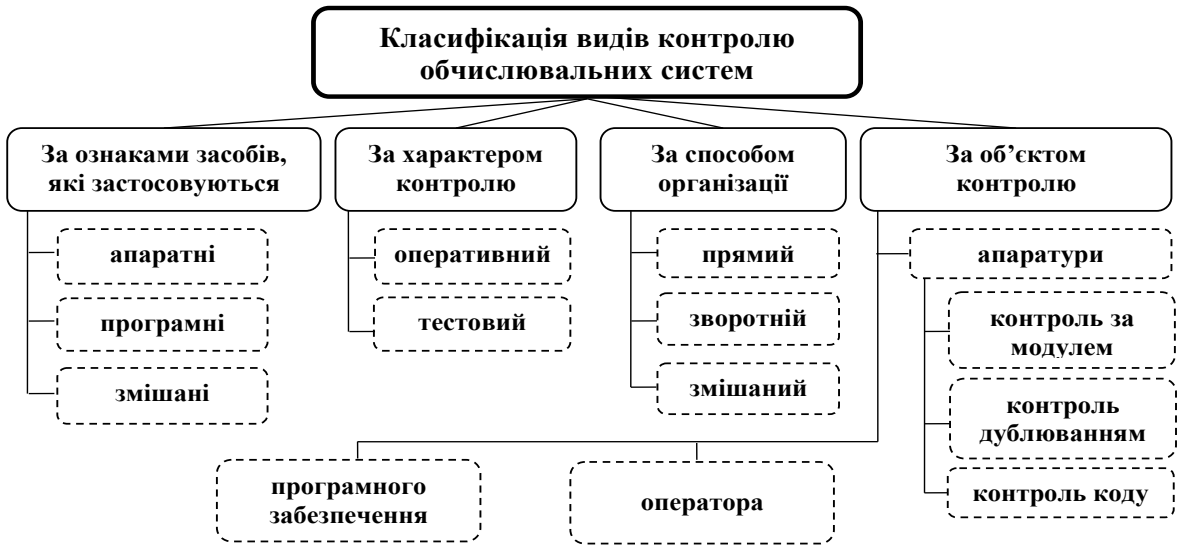


Рис. 1. Класифікація видів контролю обчислювальних систем

Однак слід враховувати, що представлені види контролю зазвичай застосовуються в універсальних обчислювальних системах. Разом з тим у спеціалізованих обчислювальних системах, зокрема, у вбудованих системах, що виконують обмежену кількість функціональних програм, широко застосовується контроль правильності виконання програм, який називається програмно-логічним контролем, до якого входять: контроль тривалості виконання, послідовності виконання, метод контрольних функцій і контроль гладкості [13]. Розглянемо її більш детальніше.

1. Контроль тривалості виконання програми заснований на тому, що для кожної програми заздалегідь відома максимальна тривалість виконання та будь-яке її перевищення означає, що програма зациклилася, зупинилася або виконана неправильно. Перевищення тривалості виконання необов'язково пов'язане з помилками у програмі, часто причиною може бути спотворення адресної інформації збоями. Можливі навіть випадки, коли почне

виконуватися одна програма, а потім результат збою виконання переходить помилково до іншої програми. Тому іноді застосовують контроль послідовності виконання підпрограм, порівнюючи номери фактично виконаних підпрограм з потрібними значеннями.

2. Метод контрольних функцій полягає в тому, що результати роботи програми повинні відповідати певним функціональним співвідношенням. Наприклад, рішення системи диференціальних рівнянь можуть бути перевірені за критерієм задоволення контрольного рівняння, утвореного у вигляді рівнянь вихідної системи.

3. Контроль гладкості заснований на тому, що якщо ряд результатів обчислень є більш-менш гладкою функцією, то будь-які різкі відхилення результату від екстрапольованого значення свідчать про помилку.

Перераховані види контролю правильності виконання програм здійснюються переважно програмними засобами. Вони дозволяють виявляти помилки в роботі обчислювальних систем із затримкою, порівнянною з часом виконання програми або підпрограми. Спільно з апаратними програмні види контролю допомагають виявити помилки, які не були виявлені апаратними засобами. Якщо ж за цільовим призначенням обчислювальної системи не потрібно швидке виявлення помилок, достатньо обмежитися програмними засобами контролю.

Далі, під діагностуванням мається на увазі процедура локалізації несправності об’єкта, тобто встановлення того, яка частина об’єкта, що діагностується, несправна. При діагностуванні проводиться встановлення несправності об’єкта на більш нижчому ієрархічному рівні, ніж під час контролю. У деяких випадках контроль обчислювальних систем сприймається як окремий випадок діагностування. Продовжуючи спускатися ієрархічною структурою об’єкта діагностування, можна доходити до будь-якого бажаного рівня ієрархії, до окремих контактних з’єднань, логічних елементів або навіть частин їх конструкції. Мірою проникнення ієрархією об’єкта є глибина діагностування. При цьому глибина діагностування вирішується, виходячи з організації процесу відновлення. З метою швидкого відновлення системи доцільно обмежитися спочатку встановленням пристрою, що відмовив. Це завдання вирішується здебільшого засобами апаратного контролю, без залучення програмних методів тестування. При цьому процедуру контролю можна розглядати як процедуру діагностування за найменшої глибини. Розглянемо найпоширеніші методи діагностування обчислювальних систем.

На сьогодні за характером взаємодії між об’єктом та засобом діагностування розрізняють тестове та функціональне діагностування. При тестовому діагностуванні на об’єкт подають спеціально підготовлені тестові дії та порівнюють реакції об’єкта на ці дії з еталонними відповідями. Цей вид діагностування застосовується тоді, коли необхідно перевірити справність функціонування або виявити несправність (дефект), що впливають на працездатність об’єкта, що перевіряється. При тестовому діагностуванні реалізуються спеціальні алгоритми, які складаються з елементарних етапів контролю. Остаточний діагноз ставиться за результатами елементарного контролю обчислювальної системи. При цьому використовуються евристичні підходи, діагностичні моделі аналітичних описів або графо-аналітичних уявлень основних властивостей об’єкта та розроблені на їхній основі алгоритми діагностування у вигляді сукупності послідовних операцій. Слід зазначити, що методи тестового діагностування містять дуже громіздкі та дорогі підготовчі операції з розробки детермінованих тестів та еталонних реакцій. При цьому виділяються три типи тестування [14]:

статистичне, коли зміна тестових наборів на виході та зняття реакцій значно нижча за частоту при роботі обчислювальної системи в реальних умовах;

динамічне, коли тестові набори подаються, а вихідні реакції аналізуються на граничних частотах роботи обчислювальної системи;

параметричне, коли перевіряються параметри обчислювальної системи, а саме: статичні – напруга, струм, опір, коефіцієнт передачі; динамічні – зміна напруги, струму,

провідності, коефіцієнта передачі, тимчасові затримки тощо. Основні методи тестового діагностування обчислювальних систем представлені на рисунку 2.

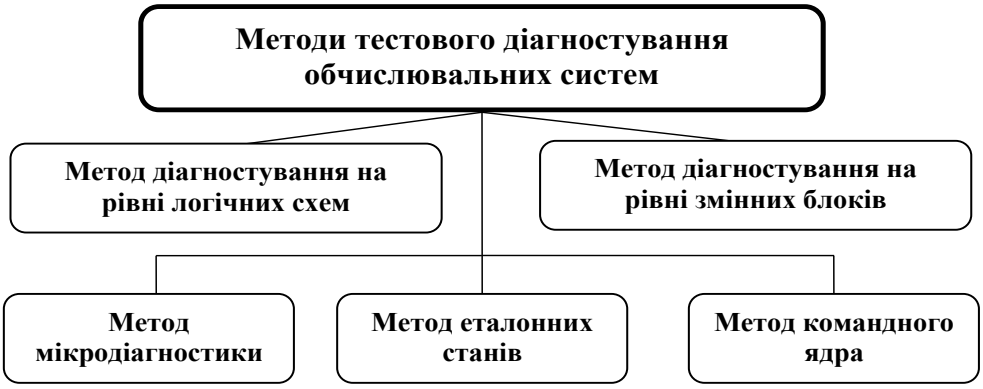


Рис. 2. Методи тестового діагностування обчислювальних систем

Другий – ймовірнісну (стохастичну) модель, яка полягає у подачі на вхід обчислювальної системи шумоподібних (випадкових та псевдовипадкових) впливів, що генеруються вбудованими генераторами, та аналіз вихідних реакцій. Основні методи функціонального діагностування обчислювальних систем представлені на рисунку 3.

Рис. 3. Методи функціонального діагностування обчислювальних систем

Окремо слід виділити компактне тестування (сигнатурний аналіз), який відноситься як до ймовірнісних методів контролю, так і методів тестового діагностування. Суть даного методу полягає у порівнянні результатів тестування з еталоном (стиснутою довгою бітовою послідовністю з високою точністю в короткі коди – сигнатури). Це здійснюється за допомогою сигнатурних регістрів, що реалізують поліном згортки бітових послідовностей з високою точністю. Отримані сигнатури порівнюються з еталонними, занесеними до словника сигнатур, реалізованих у вигляді дерева пошуку дефекту. А також слід виділити конкуруючий з методом сигнатурного аналізу – метод спектрограм, який дає можливість використовувати в якості діагностичних ознак розподіл відносних частот появи окремих комбінацій, утворених вихідними символами в послідовні моменти часу. Такі розподіли називають спектрограмами обчислювального пристрою, що діагностується. При цьому спектрограма може бути отримана аналітично або шляхом моделювання роботи пристрою на фіксованій вхідній послідовності [15].

Отже, розглянуті методи контролю та діагностування технічних засобів є загальною методологічною та технічною основою для прогнозування та діагностування відмов, а це у свою чергу дозволяє забезпечити необхідні показники надійності та ефективності обчислювальних систем при найменших витратах сил та засобів.

Підхід до усунення відмов шляхом реконфігурації спеціалізованої мікропроцесорної системи управління із самодіагностуванням. Мікропроцесорна система як об'єкт

діагностування є складною функціональною структурою, яка містить велику кількість електронних елементів і безліч розгалужених зв'язків. Крім цього велика різноманітність мікропроцесорів відрізняються між собою набором та порядком виконання команд, часовою організацією роботи, мають різну продуктивність, тактову частоту, розрядність, обсяг кеш-пам'яті та мікро- та макроархітектуру. Виходячи з цього, згідно з [16] при організації контролю, а також тестового та функціонального діагностування мікропроцесорних систем використовується декомпозиційний підхід, при якому в якості об'єкта контролю та діагностування виступають окремі функціональні пристрої: арифметико-логічний прилад, процесор, оперативно-запам'ятовуючий пристрій, постійно запам'ятовуючий пристрій, пристрої введення-виведення тощо. При цьому необхідно враховувати і труднощі, що виникають у процесі контролю та діагностування мікропроцесорних систем, які пов'язані з високим ступенем інтеграції ВІС/НВІС, розгалуженими зв'язками між елементами, відсутністю повної інформації про внутрішню структуру мікропроцесорної системи, а також відсутністю апаратних засобів контролю самого процесора. А враховуючи той факт, що одним з найбільш перспективних напрямків при проєктуванні мікропроцесорних систем є технологія System-on-Chip, в якості елементної база якої використовуються мікроконтролери, інтегральні схеми з програмованою структурою та одноплатні комп'ютери типу Raspberry Pi, то проблема контролю та діагностування набуває абсолютно нового характеру.

Так, у роботах [16; 17] для визначення технічного стану мікропроцесорних систем, реалізованих на ПЛІС, запропоновано використовувати засоби самодіагностування цифрових пристроїв, при цьому реалізувавши принцип взаємодії (тестування) мікропроцесорів між собою шляхом введення до складу багатопроцесорної системи сервісного процесора. Основною функцією такого процесора є контроль та діагностування багатопроцесорної системи, а також оперативне автоматичне відновлення шляхом реконфігурації системи. При цьому реалізація запропонованого принципу взаємодії та використання засобів самодіагностування наділить мікропроцесорну систему властивістю адаптації, тобто можливістю зміни параметрів, структури, управляючого впливу з метою досягнення оптимального функціонування системи при початковій невизначеності і в умовах роботи, що змінюються [18; 19]. Розглянемо детальніше принцип взаємного тестування процесорів.

Нехай система S складається з n пристроїв, причому кожен пристрій тестується підмножиною інших пристроїв. Така система може бути описана через граф $G(V, E)$, де V – множина вершин графа, що відповідають окремим пристроям, а E – множина дуг графа, направлених від пристрою, який тестує, до пристрою, який тестується, які зображують проведення тестів. Нехай ваги дуг означають: 1 – відмова пристрою, який тестується, виявлена; 0 – відмова пристрою, який тестується, не виявлена. Система S називається

t_0-діагностованою, якщо вона при заданому $G(V, E)$ забезпечує виявлення пристроїв, що відмовили, за наявності не більше ніж t_0 пристроїв, що відмовили.

Твердження. Система S є t_0-діагностованою, якщо: 1) кількість вхідних дуг у кожної вершини графа $G(V, E)$ не менше t_0, 2) для будь-якого цілого p за умови $0 \le p < t_0$ і кожного $V' \subset V$ при числі вершин $|V'| = n - 2t_0 + p$, числі вершин $|\Gamma V'|$ підмножини вершин $\Gamma V'$, куди входять вихідні V' з дуги графа, більше p. При цьому $|V'|$ означає число вершин, що входять до підмножини V'.

Зазначимо, що оскільки з твердження випливає, що $n > 2t_0 + |V'| - |\Gamma V'|$, а завжди знаходиться V', яке задовольняє умові $|V'| = |\Gamma V'|$, то $n \ge 2t_0 + 1$ – умова необхідна, але не достатня.

В якості прикладу розглянемо граф, де $t_0 = 2$ (рис. 4). Тоді $p \in \{0,1\}$ і $|V'| = 6 - 4 + \{0,1\} = \{2,3\}$. З рисунка. 4 видно, що для кожного V' при $|V'| = 2$ величина $|\Gamma V'| = 2 > 0$ і для кожного $|V'| = 3$ величина $|\Gamma V'| = 2 > 1$. Легко переконатися, що при $t_0 = 3$ ці умови не задовольняються. Отже, система на рисунку 4 є t_0 -діагностованою при $t_0 = 2$.

Визначення. Система, зображувана графом $G(V, E)$ при $t_0 \le ent\,(n-1)/2$, де ent –ціла частина, є $D(n, t_0, X)$-системою при $\vartheta_i, \vartheta_j \in E$ тоді й лише тоді, коли $(i-j) \bmod n \in X$, де $X = (x_1, x_2, ..., x_{t_0})$ – деяка множина цілих чисел, таких як $1 \le x_i \le ent\,(n-1)/2$ для всіх $1 \le i \le t_0$, а $x_i < x_{i+1}$. Символ $(\vartheta_i, \vartheta_j)$ тут означає дугу графа G, яка виходить з вершини ϑ_i і входить в вершину ϑ_j .

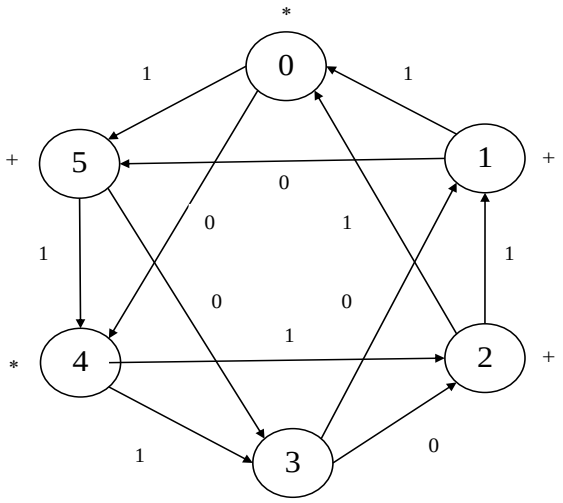


Рис. 4. Граф багатопроцесорної системи із взаємним діагностуванням

Іншими словами, $D(n, t_0, X)$-система – це t_0- діагностована n-процесорна кільцева система з діагональними зв'язками, що визначаються X.

Система на рисунку 4 є $D(6, 2, \{1, 2\})$-системою. Далі представлений алгоритм для діагностування $D(n, t_0, X)$ системи. Передбачається, що заданий граф системи з вагами дуг і потрібно визначити вершини, що відмовили і не відмовили. Алгоритм складається з наступних етапів.

Етап 1. Встановити $i = n-1$ та побудувати підграф $G^i(V^i E^i) \subset G$, де $V_i = \{\vartheta_i\} \cup V_a \cup V_b$ і $E^i = \{(\vartheta, \vartheta_i)\}$ для всіх $\vartheta \in \{V_a\} \cup \{(\vartheta_{i+x_j+x_{t_0}}, \vartheta_{i+x_j})\}$ для всіх $i \in [1, t_0]$. В останньому вираженні індекси у ϑ додаються за $\bmod n$.

Нехай $V^{\alpha_1\alpha_2} = \{\vartheta_a \in V_a | \omega(\vartheta_b, \vartheta_a) = \alpha_1, \omega(\vartheta_a, \vartheta_i) = \alpha_2, \vartheta_b \in V_b\}$. Тоді, якщо $|V_a^{00}| \ge |V_a^{01}|$ робиться висновок про те, що вершина ϑ_i не відмовила і позначається через (+), інакше переходити до виконання етапу 3, вважаючи, що вершина ϑ_i відмовила (позначається $*$). При цьому $\omega(\vartheta_b, \vartheta_a)$ означає вагу дуги, з вершини ϑ_b до вершини ϑ_a. Операція встановлення працездатності вузла ϑ_i, яка записана вище в короткій символічній формі, означає, що спочатку встановлюється підмножина V_a вершин, перевіряючих вершину ϑ_i, а потім – підмножина V_b різних вершин, перевіряючих кожен по одній вершині з V_a. Вершина ϑ_i вважається працездатною тоді і лише тоді, коли кількість ланцюгів з елементів V_b через елементи V_a в ϑ_i з вагами (0, 0) більше або дорівнює, ніж кількість ланцюгів з вагами (0, 1), тобто кількість ланцюгів, де працездатність вершини ϑ_i підтверджується працездатною вершиною, більше чи дорівнює кількості ланцюгів, де непрацездатність вершини ϑ_i підтверджується вершиною з підтвердженою працездатністю.

Етап 2. Позначити кожну вершину $\vartheta \in \Gamma_{\vartheta i}$ знаком +, якщо $\omega(\vartheta_i, \vartheta) = 0$, знаком $*$, якщо $\omega(\vartheta_i, \vartheta) = 1$. При цьому $\Gamma_{\vartheta i}$ – підмножина вершин, до яких відносяться дуги графа, які виходять із ϑ_i.

Етап 3. Підставити $i := i - 1$. Якщо $i < 0$, то виконувати етап 4, якщо ϑ_i позначений +, то здійснити перехід до етапу 2, інакше до етапу 1.

Етап 4. Якщо кількість позначених $*$ вершин більше t_0, то система не діагностується, інакше підмножина вершин, позначених $*$, – підмножина вершин, що відмовили.

Етап 5. Кінець.

Далі представлений метод реконфігурації структури цифрових пристроїв (складових мікропроцесорної системи), який полягає в зміні внутрішніх зв'язків між логічними елементами з появою відповідного сигналу від засобів самодіагностування. Даний метод розглядає цифрові пристрої, які є складовими мікропроцесорної системи в якості динамічних управляючих систем, що функціонують в умовах несприятливих впливів. Для компенсації дій зовнішніх впливів на правильне функціонування таких систем використовується положення прескриптивної теорії, яка розглядає питання цілеспрямованого управління об'єктами різної природи, що перебувають у стані «конфлікту» з іншими об'єктами [20].

Суть даного методу полягає у відшукуванні такої надмірності структури B_i, яка при підключенні до входу модуля A (при відключеному несправному вузлі A_j) призводить до відновлення правильного функціонування модуля A (рис. 5).

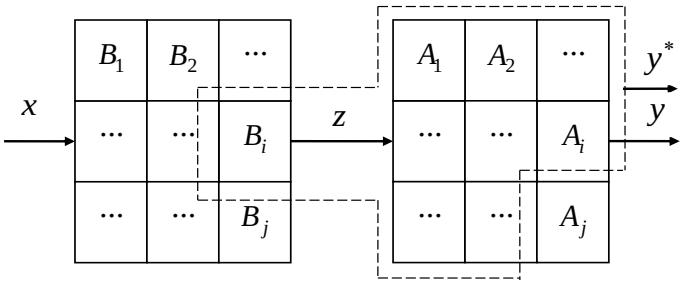


Рис. 5. Структура відновленого модуля

Модуль A, що розглядається, являє собою сукупність логічних елементів a_i, або IP-блоків (Intellectual Property – інтелектуальна власність) для ПЛІС, який реалізує функцію

$$Y_{n-1} = \varphi_0(X_n, Y_n),$$

де $X(x_1, x_2, ..., x_n)$ – вхідне слово, $Y(y_1, y_2, ..., y_n)$ – вихідне слово, n – часові такти.

Потрібно синтезувати деяку систему $S \supseteq A$, що також реалізує задану функцію $\varphi_0(X_n, Y_n)$, за умови виходу з ладу будь-якої з підсистем A_j системи $A(a_i \in A)$ заданої складності розбиття C_j. Систему A можна подати у вигляді матриці M_A будь-якої з її підсистем A_j. Вилучення з матриці M_A будь-якої з її підсистем призводить до утворення матриці спотворень $M\{A_{0j}\}, A_{0j} = (A_0 \setminus A_i)$, що результує сукупність нових функцій $M\{\varphi_{0j}(X_n, Y_n)\}$.

Для відновлення правильного функціонування системи (реалізації функції Y) необхідно утворити матрицю $\{M_{B_j}\}$, що відновлюється. При цьому кожна підсистема B_j матриці $\{M_{B_j}\}$ підключається на вхід підсистеми A_{0j} матриці спотворень $M\{\varphi_{0j}(X_n, Y_n)\}$. У загальному випадку для всіх B_i, як правило, існує перетин структур

$$\bigcap_i B_i = B_1 B_2 \ldots B_j \ ,$$

що володіє функціональними властивостями, загальними для всіх $B_1, B_2 ..., B_j$ або більшості з них. Але можуть існувати й окремі структури, які не містять перетинів. У цьому випадку для кожної несправності та підсистеми A_j, що відключається, формування надлишкової

структури B_i на основі узагальненого модуля $\bigcap_i B_i$ утворюється відповідним підключенням вхідних $\{X\}$ і вихідних $\{Z\}$ сигналів цього модуля (рис. 6).

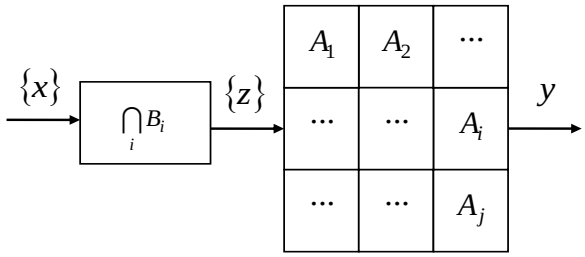


Рис. 6. Механізм відновлення модуля

Змістом функціонально-надійного синтезу системи A_0 є визначення правил Ψ опису підсистеми B_j матриці $M\{B_j\}$ при вилученні будь-якої підсистеми A_j матриці M_A. При цьому зауважимо, що правило Ψ повинно індукувати як підсистеми B_j, що відновлюються, за A_{0j}: $B_j = \Psi A_{0j}$, так і матрицю $M\{B_j\}$, яка відновлюється, підматриці спотворень:

$$M\{B_j\} = \Psi\{M_{Aj}\}.$$

Таким чином, розглянутий метод реконфігурації цифрових пристроїв дозволяє визначити структуру надмірних підсистем B_j залежно від відключених несправних підсистем A_j даного пристрою A_0. При цьому розрахована структура B_j й частина, яка залишилася справною, $A_{0j} = A_0 \setminus A_j$ реалізує задану функцію Y_{n+1}.

Зазначимо, що при реконфігурації цифрових пристроїв обов'язковим є контролюючий (діагностуючий) пристрій. А враховуючи той факт, що його структура і функціональні завдання, які він виконує, досить складні, то доцільно розробити самодіагностуючий пристрій. Принцип побудови таких пристроїв може бути заснований на методі реконфігурації надмірних цифрових пристроїв. В цьому випадку цифровий пристрій A також поділяється на вузли $A_1, A_2, ..., A_j$ і залежно від цього поділу будується структура надмірного пристрою B, що складається з схем $B_1, B_2, ..., B_j$. Пристрій із самодіагностуванням і самовідновленням, зображений на рисунку 7, містить реконфігуратор R, що забезпечує відповідну реконфігурацію пристроїв A і B, та два контрольні регістри запису результатів розрахунків P_1 і P_2.

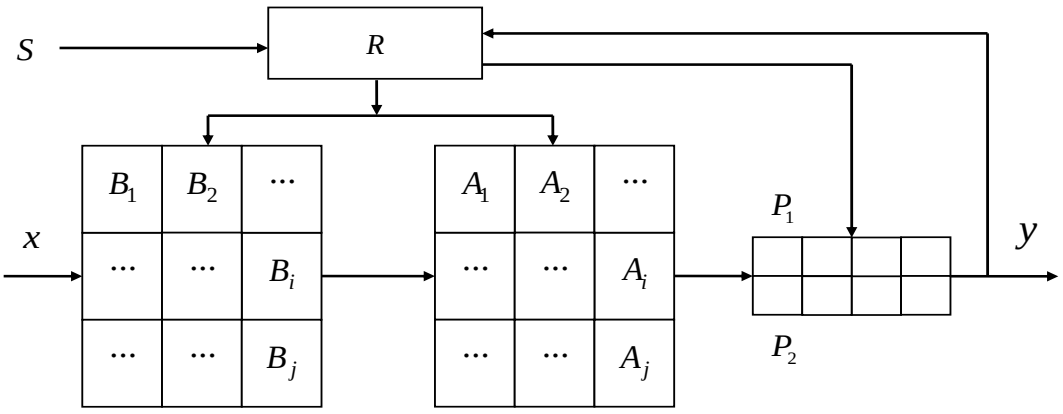


Рис. 7. Структура надмірного цифрового пристрою із самодіагностуванням

Принцип роботи полягає в тому, що цифровий пристрій A, що складається з вузлів $A_1, A_2, ..., A_j$, може бути розділений на три укрупнені блоки A_I, A_{II}, A_{III} (рис. 8, *а*). Далі, за відсутності несправностей функціонує весь пристрій A. Після певного кроку обчислень в реконфігуратор R подається сигнал S самоконтролю. У цьому випадку в пристрій вводиться тестова програма і в перший регістр P_1 записується проміжний результат обчислень (перший крок). Перед другим кроком обчислень реконфігуратор R відключає частину пристроїв, наприклад A_I, і підключає до нього відповідно пристрій B, наприклад B_I. На вхід пристрою, що утворився, $B_I - A_{II} - A_{III}$ подається таж тестова програма, що і на першому кроці обчислень, а результат обчислень записується в другий регістр P_2 (другий крок). Реконфігурація пристроїв цього типу представлена на рисунку 8, *б*.

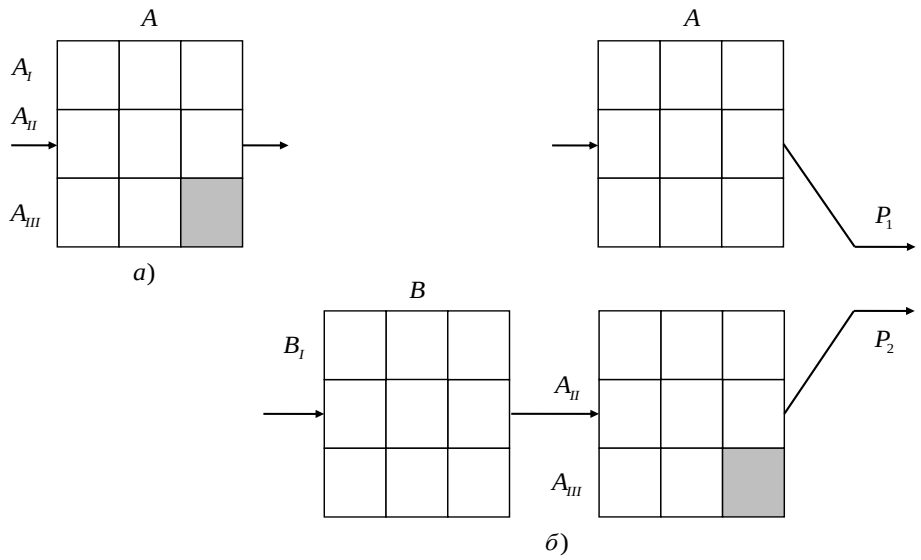


Рис. 8. Принцип реконфігурації цифрового пристрою із самодіагностуванням:
а – укрупнений цифровий пристрій А; *б* – цифровий пристрій А з надмірною структурою В

Якщо вміст регістрів P_1 і P_2 збігаються, то пристрій A продовжує функціонувати. Якщо ж результати обчислень P_1 і P_2 різні, то це означає, що несправний один з блоків пристрою A. Зазначимо, що в якості сигналу S може бути використаний один з методів тестового діагностування, представлених на рисунку 2.

Отже, розглянутий метод реконфігурації із самодіагностуванням дає можливість не тільки визначати технічний стан цифрового пристрою, але й відновлювати правильне його функціонування шляхом перебудови внутрішньої структури.

Висновки. Запропоновано методичний підхід відновлення правильного функціонування цифрових пристроїв, які є основою побудови спеціалізованої мікропроцесорної системи управління, реалізованої за технологією «система на кристалі». В основі цього підходу лежать методи контролю та діагностування спеціалізованих мікропроцесорних систем, а також метод реконфігурації цифрових надлишкових структур із засобами самодіагностування на рівні булевих рівнянь. Реалізація даного підходу при проєктуванні спеціалізованих мікропроцесорних систем управління на сучасній елементній базі надасть змогу підвищити надійність не лише системи, яка розглядається, а й усієї системи управління складними об'єктами та технологічними процесами в загалом.

Напрямами подальшої роботи є проєктування адаптивної мікропроцесорної системи управління з вбудованою інтелектуальною системою розпізнавання технічного стану та системою оперативного автоматичного відновлення правильного функціонування, здатної протидіяти несприятливим впливам, як навмисного так і ненавмисного характеру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Crespo, P. Albertos, J. Simó, Embedded control systems: from design to implementation, Ifac Proceedings Volumes, Volume 40, Issue 1, 2007, Pages 25–32, ISSN 1474-6670, ISBN 9783902661210. DOI: 10.3182/20070213-3-CU-2913.00006.

2. Smit, Wim & Hendriksen, Wim. (2004). Embedded systems: Smart and intelligent tools in an increasingly interconnected globalised world. International Journal of Technology Policy and Management. Vol. 4. pp. 309–323. DOI:10.1504/IJTPM.2004.006614.

3. H. De Man, System-on-Chip design: impact on education and research, in *IEEE Design & Test of Computers*, vol. 16, no. 3, pp. 11–19, July – Sept. 1999. DOI: 10.1109/54.785820.

4. Иванюк А. А. Проектирование встраиваемых цифровых устройств и систем: монография / А. А. Иванюк. Минск: Бестпринт, 2012. 337 с. ISBN 978-985-6873-47-1.

5. Штаненко С. С. Технологія System-on-Chip як основа підвищення живучості складних технічних систем / С. С. Штаненко, Ю. Я. Самохвалов // Сучасна спеціальна техніка: ДНДІ МВС України. Київ. 2021. № 3(66). С. 31–43. ISSN: 2411-3816.

6. Магомедов Ш. Г. Проектирование микропроцессорных устройств, разработанных для систем контроля и управления / Ш. Г. Магомедов. Cloud of Science. 2019. Т. 6. № 4. С. 752–761. UBL: http://cloudofscience.ru.

7. Зотов В. Ю. Средства проектирования встраиваемых микропроцессорных систем, реализуемых на основе ПЛИС фирмы Xilinx. М.: Современная электроника, № 9. 2006. С. 64–70.

8. M. N. Granieri and F. J. Levy, "Embedded diagnostic system design using an automated diagnostic tool set," *AUTOTESTCON 93*, San Antonio, TX, USA, 1993, pp. 645–649. DOI: 10.1109/AUTEST.1993.396294.

9. Топораш Г. К. Модельно-ориентированное проектирование программного обеспечения для встраиваемых систем в среде Matlab/Simulink / Г. К. Топораш, А. В. Мазур, Д. А. Ковальчук, А. А. Пушкин // Автоматизація технологічних і бізнес-процесів. 2014. № 17. С. 26–29. DOI: 10.15673/АТБП2312-3125.17/2014.26326.

10. Горлов М. И. Диагностический контроль интегральных схем по измерению критического напряжения питания / М. И. Горлов, А. В. Строгонов, А. В. Арсентьев, А. А. Винокуров // Энергия. Воронеж: ЗАО «Орбита», 2017. С. 29–46.

11. Кузавков В. В. Методика локалізації несправного радіоелектронного компоненту / В. В. Кузавков, О. Г. Янковський // Збірник наукових праць Одеської державної академії технічного регулювання та якості, 2015. Вип. 1. С. 36–41.

12. Гуляев В. А. Техническая диагностика управляющих систем. Киев: Наукова думка, 1983. 208 с.

13. Jäger, Reinhold. (1991). Computer diagnostics – a survey: Practical applications of computerized assessment: Theoretical principles and perspectives. European Review of Applied Psychology / Revue Européenne de Psychologie Appliquée. 41. 247–268.

14. Иыуду К. А. Надежность, контроль и диагностика вычислительных машин и систем. М.: Высшая школа, 1989. 216 с.

15. Ручко В. В. Контроль цифровых схем с помощью спектрограмм / В. В. Ручко, Ю. Г. Савченко, А. В. Хмелевая // Управляющие системы и машины. Киев: УСиМ. 1984. № 3 (71). С. 28–31.

16. Штаненко С. С. Мікропроцесорні системи на програмованих логічних інтегральних схемах як об’єкт діагностики / С. С. Штаненко, Ю. Я. Самохвалов, О. Ю. Іохов, В. Г. Малюк // Сучасні інформаційні системи = Advanced Information Systems. 2022. Т. 6. № 1. С. 81–87. DOI: 10.20998/ 2522-9052.2022.1.14.

17. Погребинский С. Б. Проектирование и надежность многопроцессорных ЭВМ / С. Б. Погребинский, В. П. Стрельников. М.: Радио и связь, 1988. 168 с.

18. Герасимов Б. М. Інтелектуальні системи підтримки прийняття рішень / Б. М. Герасимов, В. М. Локазюк, О. Г. Оксіюк, О. В. Поморова. К: Вид-во Європ. ун-ту, 2007. 335 с.

19. Штаненко С. С. Адаптація мікропроцесорних систем управління до несприятливих впливів / С. С. Штаненко, Ю. Я. Самохвалов // Сучасна спеціальна техніка: ДНДІ МВС України. Київ. 2022. № 3 (70). С. 89–100. ISSN: 2411-3816.

20. Обухов В. Е. Синтез избыточных дискретных устройств с реконфигурацией структуры / В. Е. Обухов, В. В. Павлов. К.: Наукова думка, 1979. 156 с.

АВТОРИ НОМЕРА

1. ***Балан Дмитро Дмитрович*** – викладач кафедри автоматизованих систем управління Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

2. ***Бараннік Володимир Вікторович*** – доктор технічних наук, професор, професор кафедри Харківського національного університету ім. В. Н. Каразіна, м. Харків, Україна.

3. ***Бєляков Роберт Олегович*** – кандидат технічних наук, доцент, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

4. ***Бондаренко Леонід Олександрович*** – старший науковий співробітник науково-дослідного відділу (розвитку транспортних мереж) науково-дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

5. ***Борисов Олег Володимирович*** – кандидат технічних наук, старший викладач кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

6. ***Гаврилов Дмитро Сергійович*** – аспірант кафедри інформаційно-мережевої інженерії Харківського національного університету радіоелектроніки, м. Харків, Україна.

7. ***Горбачов Костянтин Миколайович*** – доктор філософії (військові науки), доцент кафедри Національного університету оборони України ім. Івана Черняховського, м. Київ, Україна.

8. ***Гримуд Андрій Геннадійович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

9. ***Гуржій Павло Миколайович*** – кандидат технічних наук, начальник кафедри телекомунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

10. ***Дикий Олександр Вікторович*** – начальник 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.

11. ***Драглюк Олексій Вікторович*** – начальник науково-дослідного управління (перспектив розвитку інформаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

12. ***Дроль Олександр Юрійович*** – старший викладач Харківського національного університету Повітряних Сил ім. Івана Кожедуба, м. Харків, Україна.

13. ***Єлісов Юрій Миколайович*** – кандидат технічних наук, науковий співробітник Науково-дослідного інституту воєнної розвідки.

14. ***Ільїнов Михайло Дмитрович*** – кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

15. ***Іляш Юрій Юрійович*** – кандидат технічних наук, завідувач кафедри комп'ютерних наук та інформаційних систем Прикарпатського національного університету ім. Василя Стефаника, м. Івано-Франківськ, Україна.

16. ***Кисиленко Дар'я Юріївна*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

17. ***Коваленко Ілля Григорович*** – кандидат технічних наук, старший науковий співробітник науково-дослідного відділу (інформаційного, лінгвістичного та ергономічного забезпечення) науково-дослідного управління (перспектив розвитку інформаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

18. ***Колесник Віталій Олександрович*** – науковий співробітник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, м. Чернігів, Україна.

19. ***Кондрусь Андрій Володимирович*** – старший викладач кафедри автоматизованих систем управління Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

20. ***Кузавков Василь Вікторович*** – доктор технічних наук, професор, начальник кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

21. ***Куценко Володимир Валерійович*** – кандидат технічних наук, начальник науково-дослідного відділу Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, м. Чернігів, Україна.

22. ***Лазута Роман Романович*** – начальник науково-дослідного відділу (розвитку мереж доступу та електромагнітної сумісності) науково-дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

23. ***Макарчук Василь Іванович*** – старший науковий співробітник науково-дослідного відділу (розвитку мереж доступу та електромагнітної сумісності) науково-дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

24. ***Мартинюк Віталій Валерійович*** – провідний науковий співробітник науково-дослідної лабораторії (спеціальних досліджень) науково-дослідного управління (проблем захисту інформації) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

25. ***Масесов Микола Олександрович*** – кандидат технічних наук, старший науковий співробітник, начальник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

26. ***Мацаєнко Андрій Миколайович*** – старший викладач кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

27. ***Михайлюк Сергій Станіславович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

28. ***Мороз Микола Вікторович*** – науковий співробітник Науково-дослідного інституту воєнної розвідки.

29. ***Нестеренко Ігор Костянтинович*** – кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

30. ***Нестеров Олександр Миколайович*** – заступник начальника кафедри бойового застосування підрозділів зв’язку Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

31. ***Олексенко Віталій Петрович*** – заступник начальника Головного управління зв’язку та кібербезпеки ГШ ЗС України, м. Київ, Україна.

32. ***Остапчук Віктор Миколайович*** – начальник Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

33. ***Паламарчук Наталія Анатоліївна*** – начальник науково-дослідної лабораторії (спеціальних досліджень) науково-дослідного управління (проблем захисту інформації) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

34. ***Погребняк Сергій Васильович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

35. ***Поляк Ілля Євгенійович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

36. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, професор, заступник начальника Військового інституту телекомунікацій та інформатизації ім. Героїв Крут з наукової роботи, м. Київ, Україна.

37. ***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.

38. ***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.

39. ***Руденко Володимир Іванович*** – старший науковий співробітник науково-дослідного відділу (розвитку транспортних мереж) науково-дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

40. ***Сакович Лев Миколайович*** – кандидат технічних наук, доцент, доцент кафедри теоретичних основ експлуатації засобів спеціальних інформаційно-телекомунікаційних систем Інституту спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ, Україна.

41. ***Самохвалов Юрій Яковлевич*** – доктор технічних наук, професор, професор кафедри інтелектуальних технологій Київського національного університету ім. Тараса Шевченка, м. Київ, Україна.

42. ***Симоненко Олександр Анатолійович*** – кандидат технічних наук, доцент, доцент кафедри автоматизованих систем управління Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

43. ***Слюсар Петро Петрович*** – науковий співробітник Науково-дослідного інституту воєнної розвідки.

44. ***Слюсарчук Олександр Олександрович*** – кандидат військових наук, старший дослідник, заступник начальника управління – начальник відділу Науково-дослідного інституту воєнної розвідки.

45. ***Телюков Сергій Миколайович*** – кандидат технічних наук, доцент кафедри Харківського національного університету Повітряних Сил ім. Івана Кожедуба, м. Харків, Україна.

46. ***Терещенко Тетяна Павлівна*** – старший науковий співробітник науково-дослідного відділу (кібернетичної безпеки в інформаційно-телекомунікаційних системах) науково-дослідного управління (проблем захисту інформації) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

47. ***Ткаченко Андрій Леонідович*** – кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного управління (розвитку військ зв’язку) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

48. ***Толюпа Сергій Васильович*** – доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченка, м. Київ, Україна.

49. ***Фесенко Олексій Дмитрович*** – викладач кафедри технічного та метрологічного забезпечення Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

50. ***Фесьоха Віталій Вікторович*** – доктор філософії (інформаційні технології), доцент кафедри комп’ютерних інформаційних технологій Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

51. ***Фесьоха Надія Олександрівна*** – старший викладач кафедри комп’ютерних інформаційних технологій Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

52. ***Хоменко Павло Володимирович*** – старший викладач кафедри телекомунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

53. ***Цімура Юрій Васильович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

54. ***Чередниченко Олексій Юрійович*** – старший науковий співробітник науково-дослідної лабораторії (спеціальних досліджень) науково-дослідного управління (проблем захисту інформації) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

55. ***Шаповал Віталій Михайлович*** – начальник науково-дослідного відділу (математичного та програмного забезпечення) – заступник начальника науково-дослідного управління (перспектив розвитку інформаційних систем) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

56. ***Шемендюк Олександр Віталійович*** – начальник науково-дослідного відділу (комплексних систем захисту інформації в інформаційно-телекомунікаційних системах) науково-дослідного управління (проблем захисту інформації) Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

57. ***Штаненко Сергій Станіславович*** – кандидат технічних наук, доцент, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

58. ***Янковський Олег Георгійович*** – кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж 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 – **А4 (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** з 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, 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 вичитки 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.