МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

ПРОБЛЕМИ СТВОРЕННЯ, ВИПРОБУВАННЯ, ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЇ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

27 (I)

Житомир
2024

Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : збірник наукових праць. Вип. 27 (І) / Житомирський військовий інститут імені С. П. Корольова. – Житомир : ЖВІ, 2024. – 140 с. – ISSN 2076-1546. https://doi.org/10.46972/2076-1546.2024.27

Наказами Міністерства освіти і науки України від 09.02.2021 № 157 та від 15.04.2021 № 420 збірник наукових праць включений у категорію «Б» Переліку наукових фахових видань України.

Науковий профіль видання:
122 – Комп'ютерні науки
125 – Кібербезпека
255 – Озброєння та військова техніка

Рекомендовано до друку рішенням вченої ради Житомирського військового інституту імені С. П. Корольова, протокол № 06 від 27.12.2024.

Головний редактор – ФРИЗ С. П., заслужений працівник освіти України, доктор технічних наук, професор (Житомирський військовий інститут імені С. П. Корольова, Україна).
Відповідальний секретар – СТАВІСЮК Р. Л., кандидат технічних наук, старший дослідник (Житомирський військовий інститут імені С. П. Корольова, Україна).
Члени редакційної колегії:
ВАСЮТА К. С., заслужений діяч науки і техніки України, доктор технічних наук, професор (Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна);
ГРИЩУК Р. В., заслужений діяч науки і техніки України, доктор технічних наук, професор (Військова академія (м. Одеса), Україна);
ЖУРАВСЬКИЙ Ю. В., доктор технічних наук, старший науковий співробітник (Житомирський військовий інститут імені С. П. Корольова, Україна);
КАНЕВСЬКИЙ Л. Б., кандидат технічних наук, доцент (Житомирський військовий інститут імені С. П. Корольова, Україна);
КОВБАСЮК С. В., лауреат державної премії України в галузі науки і техніки, доктор технічних наук, старший науковий співробітник (Державний університет «Житомирська політехніка», Україна);
МЕРЧИК Зигмунт, доктор технічних наук, професор (Військова технічна академія, Республіка Польща);
МОСОВ С. П., заслужений діяч науки і техніки України, лауреат державної премії України в галузі науки і техніки, доктор військових наук, професор (Інститут державного управління та наукових досліджень з цивільного захисту, Україна);
ПІЛЬКЕВИЧ І. А., заслужений працівник освіти України, доктор технічних наук, професор (Житомирський військовий інститут імені С. П. Корольова, Україна);
САМЧИШИН О. В., кандидат технічних наук, старший дослідник (Житомирський військовий інститут імені С. П. Корольова, Україна);
ФЕДОРЧУК Д. Л., кандидат технічних наук, старший дослідник (Житомирський військовий інститут імені С. П. Корольова, Україна).

ISSN 2076-1546

Наукові статті, включені до збірника наукових праць, пройшли рецензування.

Рішення Національної ради України з питань телебачення і радіомовлення про державну реєстрацію № 1181 від 11.04.2024 (ідентифікатор медіа – R30-03932).

© Житомирський військовий інститут імені С. П. Корольова, 2024

ЗМІСТ

Корченко О. Г., Грищук О. М. Метод криптографічного захисту мовної інформації на основі диференціальних перетворень ……..... 4

Пількевич І. А., Мірошніченко С. І., Заєць Ю. О., Лобода В. В. Автоматизована інформаційна система «Кадри» ……..…….... 20

Трутнєв С. Г. Аналіз імовірних витоків помилок в обчисленні математичних моделей бойових дій у комп'ютерних системах імітаційного моделювання ……... 31

Зімчук І. В., Шапар Т. М., Ковба М. В. Алгоритм фільтрації вимірювань акселерометричних датчиків у безплатформених інерціальних системах навігації безпілотних літальних апаратів ……..……..... 44

Охрімчук В. В., Охрімчук І. А. Аналіз засобів моделювання мереж щодо можливості їх використання для практичної підготовки фахівців із кібербезпеки …. 56

Пулеко І. А., Чумакевич В. О., Шестак І. М., Рикун В. Л., Свистунович І. В. Функція щільності розподілу цілей для планування застосування безпілотних літальних апаратів ……..…….…… 69

Ісмаілова Н. П., Мікрюков І. С., Бикова Л. Г. Технічне рішення для проєктування спряжених зубчастих зачеплень щодо визначення інтерференції в озброєнні та військовій техніці ……..... 82

Тимчук С. В., Тарасенко В. О. Аналіз методів розпізнавання зображень та їх класифікація ……. 93

Ахтирцева В. С., Весельська А. Р. Теоретичні виклики та практичні можливості оцінювання ефективності заходів психологічних операцій ……..…… 105

Гребенюк О. О. Математична модель сигналу із заданими поляризаційними параметрами в ортогональному поляризаційному базисі ……... 114

Бондаренко Ю. Л., Петрук М. Д., Ступак Д. Є., Іщенко І. А. Спосіб підвищення ефективності роботи трифазного генератора шляхом адаптивного перерозподілу потужності між однофазними споживачами …….……... 123

Автори випуску…..... 136

ISSN 2076-1546
УДК 004.056 DOI: 10.46972/2076-1546.2024.27.01

О. Г. Корченко, О. М. Грищук

МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ

Проблема безпеки інформації, яка циркулює в каналах зв'язку, постійно актуалізується. Особливо гостро вона стоїть для VoIP-телефонії військового призначення або подвійного використання. Це пов'язано й зі зростанням цінності конфіденційної інформації, яка становить інтерес для кіберзлочинців, і з нарощенням технологічної складності кібератак за одночасного збільшення продуктивності технічних засобів несанкціонованого отримання інформації. Серед відомих механізмів забезпечення кібербезпеки мовної інформації, яка циркулює в каналах зв'язку, одне з ключових місць займають криптографічні методи її захисту. Найчастіше для організації безпечного VoIP-трафіку використовують протоколи безпеки SRTP, які реалізують симетричний криптографічний алгоритм шифрування AES. Водночас потенційна компрометація найкращого симетричного криптографічного алгоритму AES-256 потребує пошуку нових нетривіальних підходів до удосконалення механізмів забезпечення кібербезпеки. Одним із них є підхід, який ґрунтується на використанні моделі криптосистеми Фредгольма. Згадана криптографічна система належить до класу симетричних криптографічних систем, але до сьогодні, через відсутність науково обґрунтованих криптографічних алгоритмів, вона ще й досі не набула практичного впровадження. Для вирішення цієї суперечності в дослідженні з урахуванням принципу О. Керкгоффса розроблено метод криптографічного захисту мовної інформації на основі диференціальних перетворень академіка НАН України Г. Пухова. Запропонований метод дозволяє отримати шифр у вигляді диференціального спектра, який стійкий до відомих методів криптоаналізу. У статті розроблено алгоритм реалізації цього методу. Наведено результати шифрування та розшифрування мовної інформації. Збіжність результатів моделювання з іншими відомими методами підтверджує роботоздатність розробленого методу.

Ключові слова: *симетричний криптографічний алгоритм; диференціальні перетворення; ключ шифрування; диференціальний спектр; шифр; дискрета; гарантована криптостійкість; обернена задача; інтегральне рівняння Фредгольма першого роду.*

Постановка проблеми в загальному вигляді. VoIP-телефонія, порівняно з традиційними технологіями організації комунікацій між абонентами інформаційного обміну, має низку ключових переваг, зокрема її дешевизна та висока якість зв'язку [1] і надалі сприятимуть інтенсивному впровадженню в епоху діджиталізації технологій VoIP-телефонії в усі сфери діяльності суспільства. Разом із тим, незважаючи на застосовувані механізми забезпечення кібербезпеки VoIP-трафіку, наприклад,

© О. Г. Корченко, О. М. Грищук, 2024

шифрування з використанням таких безпечних протоколів, як IPSec, SSH та SRTP [2], які забезпечують конфіденційність [3], [4] засобів автентифікації, VPN-тунелювання тощо, мовна інформація й надалі стає об'єктом перехоплення технічних засобів несанкціонованого отримання інформації [5]–[7] та кібератак різних типів. Такими кібератаками з боку недобросовісних конкурентів можуть бути MITM, NAT Attack [8], [9]. Саме тому проблема забезпечення кібербезпеки VoIP-телефонії є та залишатиметься актуальною. Особливо гостро вона стоїть для VoIP-телефонії військового призначення та подвійного використання, а також інших критичних систем [10].

Аналіз останніх досліджень і публікацій. У публікації [6] достатньо ґрунтовно розкрито проблеми захисту мовної інформації за технологією VoIP-телефонії, зокрема зазначено, що криптографічному захисту підлягає сигнальний трафік, під яким розуміється мовна інформація, а також способи генерування (розподілу) ключів для протоколів її захисту.

Із [8] та [11] відомо, що серед протоколів захисту сигнального трафіку найбільшого поширення отримали SIP (стандарт IETF RFC 3261) та SIPS (стандарт RFC 3261). Разом із тим на практиці застосовують й інші протоколи під час роботи із сигнальним трафіком, наприклад такі [6], [12]: H.323 (стандарти ITU-T); MGCP і Megaco (стандарти ITU-T і IETF); MiNET (стандарти Mitel) тощо.

Зважаючи на стрімкий розвиток інформаційних технологій, зокрема й на основі квантових комп'ютерів, нині в галузі криптографії розробляють й інші, відмінні від проаналізованих вище класичних підходів, методи криптографічного захисту інформації [13].

На сучасному етапі розвитку науки й техніки під час шифрування та розшифрування в асиметричних та симетричних криптографічних системах використовують такі математичні методи: арифметика залишків; методи заміни та перестановки; метод шифрування за допомогою матриць; методи шифрування на основі теорії множин, еліптичних кривих тощо. Вони є математичним підґрунтям для розроблення відповідних безпечних протоколів. Так, для захисту мовної інформації в [14]–[17] запропоновано інноваційну технологію криптографічного захисту на диференціальних перетвореннях як новий засіб забезпечення кібербезпеки VoIP-трафіку. Основу цієї технології становить класична симетрична криптографічна система [18]–[20]. Водночас її відмінністю від відомих є застосування як криптографічного алгоритму інтегрального рівняння Фредгольма першого роду та операційного методу диференціальних перетворень академіка НАН України Г. Пухова [21]. Також відмінною є процедура генерування ключа шифрування на основі відповідного алгоритму [22], [23]. Однак ні в [13], ні в інших наукових публікаціях ґрунтовно не розкрито процедури шифрування та розшифрування для такого перспективного підходу. Також жоден із відомих методів не дає змоги шифрувати й розшифровувати мовну інформацію в симетричній криптографічній системі Фредгольма [19], [20], що стримує подальше розроблення новітніх методів шифрування та безпечних протоколів на їхній основі.

Формулювання завдання дослідження. Метою статті є розроблення методу криптографічного захисту мовної інформації на основі диференціальних перетворень.

Виклад основного матеріалу. Для практичної реалізації запропонованої в [13] методології в [24] наведено результати аналізу відомих математичних моделей мовної інформації, а в [25] обґрунтовано вибір такої моделі у вигляді гармонічного сигналу

$$z(t) = A_c \cos(2\pi f_c t + \varphi_c(t) + \varphi_c), \quad (1)$$

де $z(t)$ – математична модель мовної інформації, що підлягає шифруванню;

A_c – амплітуда сигналу, В;

f_c – несуча частота, Гц;

t – час передачі голосового повідомлення, с;

$\varphi_c(t)$ – фазова функція, рад/с;

φ_c – початкова фаза, рад.

Через зростаючі в комунікаційних системах потоки мовної інформації (1), яка має підлягати криптографічному захисту, основною вимогою, крім гарантованої теоретичної та практичної криптостійкості алгоритмів шифрування, залишається вимога до її шифрування в реальному масштабі часу. Відомі чисельні методи [26] (Ньютона – Котеса, Гаусса, Чебишева), що ґрунтуються на використанні квадратурних формул, суттєво обмежені в застосуванні в криптографічних системах, адже потребують значного обсягу обчислень. Тому для шифрування мовної інформації в реальному масштабі часу в симетричній криптографічній системі Фредгольма у [18]–[20] запропоновано застосувати точний операційний метод диференціальних перетворень академіка НАН України Г. Пухова [21]. Цей метод уже використовують у багатьох галузях науки й техніки. Наприклад, його було застосовано в електротехніці, спектроскопії та інших галузях, у яких фізичні процеси описуються у вигляді інтегральних та диференціальних рівнянь. Уперше в галузі кібербезпеки цей метод було використано для моделювання процесів кібернападу на державні інформаційні ресурси [27].

На відміну від відомих операційних методів інтегральних перетворень Лапласа та Фур'є, під час шифрування мовної інформації диференціальні перетворення ґрунтуються на переведенні оригіналів в область зображень за допомогою операції диференціювання [21]. У такому разі шифрування мовної інформації в області зображень для збереження точності вихідної математичної моделі мовної інформації без часового аргументу зводиться до виконання чотирьох арифметичних операцій в аналітичному або чисельному вигляді: множення, ділення, додавання та віднімання, – що практично реалізуються сучасними апаратними або програмними засобами криптографічного захисту. Крім того, ще однією перевагою методу диференціальних перетворень є значно простіша процедура розшифрування мовної інформації під час переходу з області зображень в область оригіналів.

Згідно з [21], [28] та [29] диференціальні перетворення передбачають подання вихідної математичної моделі степеневим рядом Тейлора із центром розкладання ряду в точці $t = 0$. Пряме і, відповідно, зворотне перетворення в загальному вигляді описують такими виразами [21]:

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \underline{\cdot} \; x(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \tag{2}$$

де $x(t)$ – оригінал, який є безперервною, що диференціюється нескінченну кількість разів, і обмеженою разом з усіма своїми похідними функцією дійсного аргументу *t*;

$X(k)$ і $\underline{x}(k)$ – рівноцінні позначення диференціального спектра за конкретних числових значень параметрів моделі.

Кількість дискрет диференціального спектра мовної інформації визначає точність розшифрування мовної інформації в області оригіналів і на практиці обмежується першими трьома-п'ятьма ненульовими дискретами.

Підвищення точності моделювання на основі диференціальних перетворень за потреби можна досягти двома шляхами. Перший – це збільшення кількості дискрет диференціального спектра досліджуваної моделі, але в цьому разі зростатиме аналітична складність моделі. І другий шлях – це застосування диференціальних перетворень нетейлорівського типу, але для цього потрібно мати апріорну інформацію про вигляд шуканої апроксимаційної функції.

Суть методу. Шифрування мовної інформації. Нехай у симетричній криптографічній системі захисту інформації [19], [20] шифруванню підлягає мовна інформація, яка від абонента *Alice* до абонента *Вов* передається протягом деякого фіксованого часу *T*, с. У загальному вигляді мовна інформація описується гармонічною математичною моделлю аналогового сигналу $z(t)$ (1) [25].

Шифрування мовної інформації $z(t)$ пропонуємо здійснювати на основі диференціальних перетворень (2) за криптографічним алгоритмом, що в загальному вигляді описується інтегральним рівнянням Фредгольма першого роду [17]:

$$\int_a^b K(\omega, t)\, z(t)\, dt = z(\omega), \; a \le \omega \le b, \; a \le t \le b. \tag{3}$$

У виразі (3) прийнято такі позначення: $K(\omega, t)$ – секретний ключ шифрування (ядро інтегрального рівняння Фредгольма першого роду), що підлягає генеруванню; $z(\omega)$ – зашифровані дані (шифрограма), які відкритим каналом від відправника *Alice* передаються до одержувача *Bob.*

Головною перевагою шифрування за криптографічним алгоритмом (3) є гарантована теоретична та практична криптостійкість, яка випливає з некоректності за Ж. Адамаром [30], [31], адже без знання ключа шифрування задача дешифрування є практично не розв’язуваною [17]. Безпека шифру $z(\omega)$ залежить від складності розв’язання оберненої некоректної задачі розшифрування [17], [30], [32], яка описується інтегральним рівнянням Фредгольма першого роду (3). Зазначені положення підтверджують гіпотезу Н. Фергюсона [33], що слугує науковим підґрунтям для подальших досліджень.

На основі згенерованого згідно з (2) відповідним алгоритмом [23] ключа шифрування $K(\omega,t)\cdot \bar{K}(\omega,k)$ здійснюється шифрування мовної інформації $z(t)$. Для цього застосовується метод диференціальних перетворень (2) до (1) та (3). У результаті отримуємо диференціальний спектр $Z^k(\omega)$, що є зашифрованою мовною інформацією $z(\omega)$ в області зображень.

Розшифрування мовної інформації. Нехай розшифруванню підлягає шифрограма, що описується диференціальним спектром вигляду $Z^k(\omega)$, яку отримав одержувач *Bob* відкритим каналом зв'язку. Одержувачу також відомий секретний ключ шифрування $K(\omega,k)$, переданий йому через закритий канал. Розшифрування шифрограми на стороні одержувача пропонуємо здійснювати на основі диференціальних перетворень (2) за криптографічним алгоритмом, що в загальному вигляді описується методом регуляризації академіка М. Тихонова [31] та Д. Філліпса [32]:

$$z(\omega)=\lim_{\alpha\to 0} z_{\alpha}(\omega), \tag{4}$$

де $z_a(\omega)$ – розшифрована мовна інформація з точністю до параметра регуляризації a, при цьому $a>0,\ a\to 0$.

У результаті застосування методу регуляризації (4) та зворотного диференціального перетворення (2) розшифруванню підлягає мовна інформація, яка передавалася (1). На цьому метод завершує свою роботу.

Блок-схему методу криптографічного захисту мовної інформації на основі диференціальних перетворень наведено на рис. 1.

Алгоритм методу має певні кроки (див. рис. 1).

У ході шифрування мовної інформації алгоритм методу складається з восьми кроків.

Крок 1. Генерування мовної інформації $z(t)=A_c\cos(\omega_c t)$, де $\omega_c=2\pi f_c$ – циклічна частота, рад/с; $\varphi_c(t)=0$ рад/с; $\varphi_c=0$ рад.

Крок 2. Формування моделі диференціального спектра мовної інформації $Z(k)$ на основі диференціальних перетворень (2): $Z(k)=A_c\dfrac{(\omega_c H)^k}{k!}\cos\dfrac{\pi k}{2}$.

Крок 3. Розрахунок нульової дискрети для *k*:= 0: $Z(0)=A_c$.

Крок 4. Розрахунок першої дискрети для *k*:= 1: $Z(1)=A_c\dfrac{(\omega_c H)}{1!}\cos\dfrac{\pi}{2}=0$.

Крок 5. Розрахунок *n*-ї дискрети для *k*:= *n*: $Z(n)=A_c\dfrac{(\omega_c H)^n}{n!}\cos\dfrac{\pi n}{2}$.

Крок 6. Побудова диференціального спектра мовної інформації:

$$S(k)=\sum_{k=0}^{k=n} Z(k)=Z(0)+Z(1)+\ldots+Z(n)=A_c-A_c\frac{(\omega_c H)^2}{2}+\ldots+A_c\frac{(\omega_c H)^n}{n!}\cos\frac{\pi n}{2}.$$

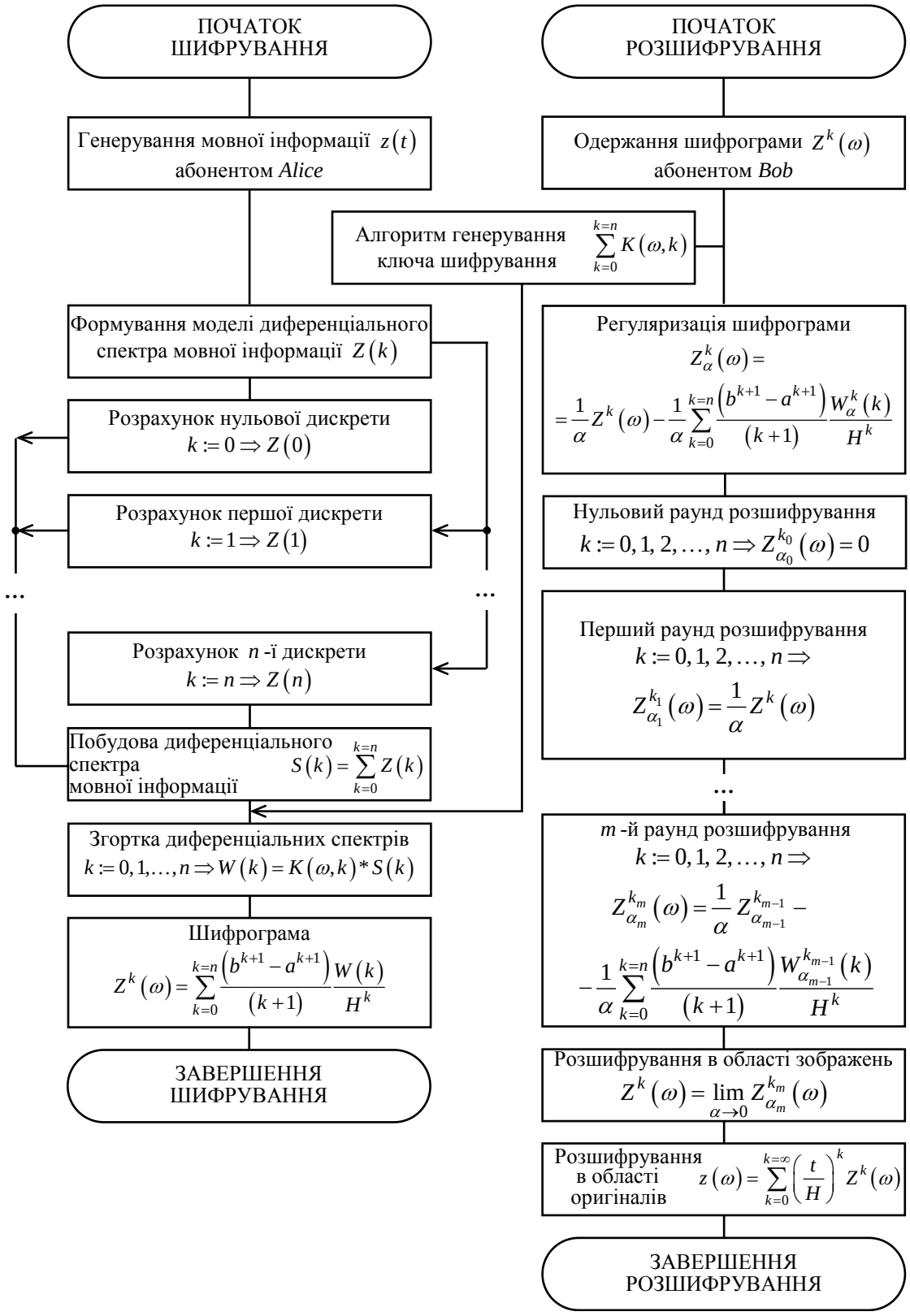


Рис. 1. Алгоритм методу шифрування мовної інформації на основі диференціальних перетворень

Крок 7. Розрахунок згортки диференціальних спектрів для k:= 0, 1,…, n:

$$W(k) = K(\omega,k) * S(k) = \sum_{l=0}^{l=k} (\omega,k-l) S(l),$$

де $K(\omega,k)$ – ключ шифрування в області зображень [23].

Крок 8. Отримання шифрограми для *k*:= 0, 1,…, *n*: $Z^k(\omega) = \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W(k)}{H^k}$.

Під час розшифрування мовної інформації алгоритм методу складається із семи кроків.

Крок 1. На приймальній стороні одержується шифрограма такого вигляду: $Z^k(\omega) = \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W(k)}{H^k}$.

Крок 2. Здійснюється регуляризація шифрограми:

$$Z_a^k(\omega) = \frac{1}{a} Z^k(\omega) - \frac{1}{a} \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W_a^k(k)}{H^k},$$

де *a* – параметр регуляризації, $a > 0,\ a \to 0$.

Крок 3. Проводиться нульовий раунд розшифрування для k_0 при *k*:= 0, 1, 2,…, *n*: $Z_{a_0}^{k_0}(\omega) = 0$.

Крок 4. Проводиться перший раунд розшифрування для k_1 при *k*:= 0, 1, 2,…, *n*: $Z_{a_1}^{k_1}(\omega) = \frac{1}{a} Z^k(\omega)$.

Крок 5. Проводиться *m*-й раунд розшифрування для k_m при *k*:= 0, 1, 2,…, *n*:

$$Z_{a_m}^{k_m}(\omega) = \frac{1}{a} Z_{a_{m-1}}^{k_{m-1}}(\omega) - \frac{1}{a} \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W_{a_{m-1}}^{k_{m-1}}(k)}{H^k}.$$

Крок 6. Здійснюється розшифрування мовної інформації в області зображень k_m при *k*:= 0, 1, 2,…, *n*:

$$Z^k(\omega) = \lim_{\alpha \to 0} Z_{\alpha_m}^{k_m}(\omega).$$

Крок 7. Розшифрування мовної інформації в області оригіналів:

$$z(\omega) = \sum_{k=0}^{k=\infty} \left(\frac{t}{H}\right)^k Z^k(\omega) = A_c \cos(\omega_c t).$$

Перевірку достовірності розробленого методу здійснимо шляхом порівняння з відомими рішеннями, наприклад, викладеними в [34] та [35].

Шифрування мовної інформації

Крок 1. Генерування мовної інформації.

Нехай шифруванню підлягає мовна інформація, яка описується гармонічною моделлю загального вигляду $z(t)=cos(t)$, де A_c =1 В, ω_c =1 рад/с; $\varphi_c(t)=0$ рад/с; $\varphi_c=0$ рад [34] та [35].

Крок 2. Формування моделі диференціального спектра мовної інформації $Z(k)$ [25] на основі диференціальних перетворень (2):

$$Z(k)=\frac{H^k}{k!}cos\frac{\pi k}{2}. \tag{5}$$

Крок 3. Розрахунок нульової дискрети для *k*:= 0:

$$Z(0)=1. \tag{6}$$

Крок 4. Розрахунок першої дискрети для *k*:= 1:

$$Z(1)=0. \tag{7}$$

Крок 5. Розрахунок *n*-ї дискрети мовної інформації для *k*:= 2, 3,…, *n*, де *n* = 8, маємо:

$$\left[\begin{array}{ll}
для\ k:=2 & Z(2)=-\frac{1}{2}H^2;\\
для\ k:=3 & Z(3)=0;\\
для\ k:=4 & Z(4)=\frac{1}{24}H^4;\\
для\ k:=5 & Z(5)=0;\\
для\ k:=6 & Z(6)=-\frac{1}{720}H^6;\\
для\ k:=7 & Z(7)=0;\\
для\ k:=8 & Z(8)=\frac{1}{40320}H^8.
\end{array}\right. \tag{8}$$

Крок 6. Побудова диференціального спектра мовної інформації (5) з урахуванням (6)–(8):

$$S(k)=\sum_{k=0}^{k=8}Z(k)=1-\frac{1}{2}H^2+\frac{1}{24}H^4-\frac{1}{720}H^6+\frac{1}{40320}H^8. \tag{9}$$

Крок 7. Розрахунок згортки диференціальних спектрів $W(k)$ (9). При цьому диференціальний спектр ключа шифрування $K(\omega,k)$ для *k*:= 0, 1,…, *n* для обраного прикладу згідно з [35] в області оригіналів описується виразом $K(\omega,t)=cos(\omega-t)$.

Відповідно до алгоритму генерування ключа шифрування на основі диференціальних перетворень [22], [23], дискрети диференціального спектра для *k*:= 0, 1,…, *n*, де *n* = 8, дорівнюватимуть

$$\begin{cases} для\ k := 0 \quad K(\omega,0) = \cos(\omega); \\ для\ k := 1 \quad K(\omega,1) = \sin(\omega) H; \\ для\ k := 2 \quad K(\omega,2) = -\frac{1}{2}\cos(\omega) H^2; \\ для\ k := 3 \quad K(\omega,3) = -\frac{1}{6}\sin(\omega) H^3; \\ для\ k := 4 \quad K(\omega,4) = \frac{1}{24}\cos(\omega) H^4; \\ для\ k := 5 \quad K(\omega,5) = \frac{1}{120}\sin(\omega) H^5; \\ для\ k := 6 \quad K(\omega,6) = -\frac{1}{720}\cos(\omega) H^6; \\ для\ k := 7 \quad K(\omega,7) = -\frac{1}{5040}\sin(\omega) H^7; \\ для\ k := 8 \quad K(\omega,8) = \frac{1}{40320}\cos(\omega) H^8. \end{cases} \tag{10}$$

З урахуванням дискрет диференціального спектра ключа шифрування (10) та дискрет мовної інформації (9) згортка їхніх диференціальних спектрів $W(k)$ визначатиметься як

$$W(k) = \sum_{l=0}^{l=k} K(\omega, k-l) S(l) = K(\omega,8) S(0) + K(x,7) S(1) + \\ + K(\omega,6) S(2) + \ldots K(\omega,0) S(8) = \frac{1}{315}\cos(\omega) H^8. \tag{11}$$

Крок 8. Отримання шифрограми для *k*:= 0, 1,…, 8:

$$Z^{k_8}(\omega) = \sum_{k=0}^{k=8} \frac{\pi^{k+1}}{H^k} \frac{W(k)}{(k+1)} = \frac{\pi^9}{2835}\cos(\omega). \tag{12}$$

Розшифрування мовної інформації

Крок 1. На приймальній стороні одержано шифрограму у вигляді (19).

Крок 2. Регуляризація шифрограми:

$$Z_\alpha^k(\omega) = \frac{1}{\alpha} Z^k(\omega) - \frac{1}{\alpha} \sum_{k=0}^{k=n} \frac{\left(b^{k+1} - a^{k+1}\right)}{(k+1)} \frac{W_\alpha^k(k)}{H^k}. \tag{13}$$

Крок 3. Нульовий раунд розшифрування для k_0 при *k*:= 0, 1, 2,…, 8:

$$Z_{a_0}^{k_0}(\omega) = 0. \tag{14}$$

Крок 4. Перший раунд розшифрування для k_1 при *k*:= 0, 1, 2,…, 8:

$$Z_{a_1}^{k_1}(\omega)=\frac{1}{a}Z^{k}(\omega)=\frac{\pi^9}{2835a}cos(\omega). \tag{15}$$

Крок 5.m-й раунд розшифрування для k_m при *k*:= 0, 1, 2,…, 8:

$$Z_{\alpha_8}^{k_8}(\omega)=\frac{\pi^9}{2835\,\alpha}\cos(\omega)-\frac{1}{\alpha}\sum_{k=0}^{k=8}\frac{\pi^{k+1}}{k!}\frac{W_{\alpha_1}^{k_1}(k)}{(k+1)}=\frac{\pi^9}{2835\,\alpha}\cos(\omega)-\frac{\pi^9}{2835\,\alpha^2}\times$$
$$\times\left(\pi-\frac{1}{3!}\pi^3+\frac{1}{5!}\pi^5-\frac{1}{7!}\pi^7+\frac{1}{9!}\pi^9\right), \tag{16}$$

де $b=\pi$, $a=0$ [35].

Крок 6. Здійснюється розшифрування мовної інформації в області зображень при *k*:= 0, 1, 2,…, 8.

З урахуванням (16) розшифрована мовна інформація в області зображень із точністю до параметра регуляризації *a* визначається за таким виразом:

$$Z_{a}^{k}(\omega)=\frac{\pi^9}{2835a}cos(\omega)ъ(k), \tag{17}$$

де $\pi-\frac{1}{3!}\pi^3+\frac{1}{5!}\pi^5-\frac{1}{7!}\pi^7+\frac{1}{9!}\pi^9\approx sin(\pi)=0$;

$ъ(k)$ – теда, $ъ(k)=\begin{cases}1,\ k=0;\\ 0,\ k\geq 1.\end{cases}$

У разі обрання параметра регуляризації *a* рівним 10,46, маємо *a* = 10,46, тоді для окремого прикладу (17) в області зображень отримаємо

$$Z_{a_8}^{k_8}(\omega)\approx cos(\omega)ъ(k). \tag{18}$$

Крок 7. Розшифрування мовної інформації в області оригіналів при *k*:= 0, 1, 2,…, 8:

$$z(\omega)=\frac{H^k}{k!}\left[\frac{d^kZ_{a_8}^{k_8}(\omega)}{dt^k}\right]_{t=0}=cos(\omega). \tag{19}$$

Висновки. Розроблений у статті метод криптографічного захисту мовної інформації на основі диференціальних перетворень дає змогу в реальному масштабі часу шифрувати та розшифровувати мовну інформацію, подану моделями гармонічних сигналів. Гарантована теоретична криптостійкість визначається кількістю дискрет диференціального спектра ключа шифрування. Практична криптостійкість є величиною обернено пропорційною до параметра регуляризації. Вона забезпечується практичною

нерозв'язуваністю задачі розшифрування на основі оберненої некоректної задачі на базі інтегрального рівняння Фредгольма першого роду. Збіжність результатів шифрування й розшифрування на основі розробленого методу й інших відомих рішень підтвердили його роботоздатність. Напрямом подальших досліджень є розроблення протоколу шифрування мовної інформації на основі запропонованого методу.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Claxson N. Securing VoIP: Encrypting Today's Digital Telephony Systems // Network Security. 2018. № 11. P. 11–13.
2. Bilash D. A., Tkachov V. M. Security Mechanisms of VoIP-telephony // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : матеріали 11-ї Міжнар. наук.-техн. конф. Т. 2. Баку : ВА ЗС АР; Харків : НТУ «ХПІ», 2021. С. 78.
3. How to Know if VoIP is the Right Solution for Your Business // Weave Communications. 2020. URL: https://www.getweave.com/en-ca/how-to-know-if-voip-is-the-right-solution-for-your-business (last accessed: 21.08.2024).
4. Kumar V., Roy Om Prakash. Security and Challenges in Voice over Internet Protocols: A Survey // IOP Conf. Series: Materials Science and Engineering. 2021. 012020. https://doi.org/10.1088/1757-899x/1020/1/012020
5. Chan Y. Y., Al-Marzouqi S. M. Practical Implementations for Securing VoIP Enabled Mobile Devices // Network and System Security : Third International Conference. Australia, Gold Coast, QLD, Oct. 19–21, 2009. P. 409–415. https://doi.org/10.1109/nss.2009.24
6. Popescu E.-E. VoIP Security Threats // International Journal of Information Security and Cybercrime. 2024. Vol. 13, Iss. 1. P. 66–70. https://doi.org/10.19107/ijisc.2024.01.06
7. Sadiwala R. Analysis of Security Threats of VoIP Systems // SHODH SANGAM – A RKDF University Journal of Science and Engineering. No. 2581–5806, Vol. 01, Iss. 02. P. 34–46.
8. Kumar V., Roy Om Prakash. Reliability and Security Analysis of VoIP Communication Systems // Rising Threats in Expert Applications Solutions. Advances in Intelligent Systems and Computing. 2020. Vol. 1187. P. 687–694. https://doi.org/10.1007/978-981-15-6014-9_84
9. Arafat M. Y., Ahmed F., Sobhan M. A. SIP Security in IP Telephony // International conference. Elastix World. Mexico, October, 2013. P. 1–11.
10. Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури : монографія / С. П. Євсеєв, О. Ю. Заковоротний, О. В. Мілов та ін. Харків : Вид-во «Новий Світ-2000», 2024. 300 с.
11. Alvaonos D., Limniotis K., Stavrou S. On the Cryptographic Features of a VoIP Service // Cryptography. 2018. № 2, Vol. 1. P. 1–12. https://doi.org/10.3390/cryptography2010003
12. Мажаренко В. В. Дослідження особливостей впровадження сервісів IP-телефонії в інтернет-ресурси : магістерська дис. 171 – Електроніка. Київ : КПІ ім. Ігоря Сікорського, 2020. 110 с.
13. Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г. К. Бронштак, И. А. Громыко, С. И. Доценко, Е. Л. Перчик // Прикладная электроника. 2014. Т. 13, № 3. С. 337–349.
14. Грищук О. М., Жилін А. В. Новітня технологія криптографічного захисту мовної інформації // Актуальні питання застосування спеціальних інформаційно-комунікаційних

систем : тези доп. VII наук.-практ. конф. (Київ, 12 червня 2024). Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2024. С. 376.
15. Грищук О. М. Сучасні інформаційні технології криптографічного захисту інформації у секторі безпеки і оборони // Графічні технології моделювання об'єктів, процесів та явищ : тези доп. Міжнар. наук.-практ. конф. (Одеса, 23–24 квітня 2020). Одеса : Військова академія, 2020. С. 87.
16. Грищук О. М. Інновації в криптографії // Воєнні інновації в сучасних війнах : зб. тез Міжнар. академіч. форуму. Київ : ЦНДІ ЗС України, 2024. С. 192.
17. Грищук О. М. Симетрична криптосистема на диференціальних перетвореннях як новий засіб забезпечення кібербезпеки VoIP-трафіку // Всеукр. наук.-практ. інтернет-конф. ["Стратегії кіберстійкості: управління та безперервність бізнесу"] (25 лютого 2021). Київ : ДУТ, 2021. С. 51–52.
18. Грищук О. М. Математичний опис криптосистеми Фредгольма // Міжнар. наук.-практ. конф. ["Інформаційна безпека та інформаційні технології"] (24–25 квітня 2019). Харків : ХНЕУ ім. Семена Кузнеця, 2019. С. 4.
19. Грищук О. М., Грищук Р. В. Узагальнена модель криптосистеми Фредгольма // Кібербезпека: освіта, наука, техніка. 2019. № 1 (4). С. 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423
20. Hryshchuk O. Mathematical Model of a Symmetrical Cryptographic System for the Protection of Speech Information Based on Differential Transformations // Кібербезпека: освіта, наука, техніка. 2024. № 1 (25). С. 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409
21. Пухов Г. Е. Дифференциальные преобразования и математическое моделирование физических процессов : монография. Київ : Наук. думка, 1986. 158 с.
22. Грищук О. М. Особливості вибору ключа шифрування для криптосистеми Фредгольма // Комп'ютерна інженерія і кібербезпека: досягнення та інновації : тези доп. ІІ Всеукр. наук.-практ. конф. (25–27 листопада 2020). Кропивницький, 2020. С. 109–110.
23. Hryshchuk O. Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations / International security and practical conference ["Information security and information technologies"]. (September, 13–19, 2021). Kharkiv; Odesa, 2021. P. 229–233.
24. Корченко О. Г., Грищук О. М. Порівняльний аналіз математичних моделей мовної інформації // Безпека інформації. 2022. № 2 (28). С. 48–56. https://doi.org/10.18372/2225-5036.28.16949
25. Грищук О. М. Диференціальний спектр мовної інформації // Захист інформації. 2022. № 3 (24). С. 120–128. https://doi.org/10.18372/2410-7840.24.17189
26. Крилик Л. В., Богач І. В., Лісовенко А. І. Чисельне інтегрування функцій. Вінниця : ВНТУ, 2019. 74 с.
27. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія. Житомир : Рута, 2010. 280 с.
28. Пухов Г. Е. Дифференциальные преобразования функций и уравнений : монография. Київ : Наукова думка, 1980. 420 с.
29. Пухов Г. Е. Дифференциальные спектры и модели : монография. Київ : Наукова думка, 1990. 184 с.

30. Тихонов А. М., Арсенин В. Я. Методы решения некорректных задач. Москва, 1979. 285 с.
31. Охріменко М. Г., Жуковська О. А., Купка О. О. Методи розв'язування некоректно поставлених задач. Київ : Центр учбової літератури, 2022. 166 с.
32. Phillips D. L. A Technique for the Numerical Solution of Certain Integral Equations of the First Kind // J. Ass. Comput. 1962. P. 84–97. https://doi.org/10.1145/321105.321114
33. Ferguson N., Schroeppel R., Whiting D. A Simple Algebraic Representation of Rijndael // Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2001. P. 103–111. https://doi.org/10.1007/3-540-45537-X_8
34. Wazwaz A. M. The Regularization Method for Fredholm Integral Equations of the First Kind // Computer Methods in Applied Mechanics and Engineering. 2011. № 61. P. 2981–2986. https://doi.org/10.1016/j.camwa.2011.03.083
35. Wazwaz A. M. The Regularization-Homotopy Method for the Linear and Non-Linear Fredholm Integral Equations of the First Kind // Communications In Numerical Analysis. 2011. Vol. 2011. P. 1–11. https://doi.org/10.5899/2011/cna-00105

Стаття надійшла до редакції 05.11.2024.

REFERENCES

1. Claxson, N. (2018). Securing VoIP: Encrypting Today's Digital Telephony Systems. *Network Security, 11,* 11–13.
2. Bilash, D. A., & Tkachov, V. M. (2021). Security Mechanisms of VoIP-telephony. In *Suchasni napriamy rozvytku informatsiino-komunikatsiinykh tekhnolohii ta zasobiv upravlinnia: materialy 11-i Mizhnar. nauk.-tekhn. konf. [Modern Directions of Development of Information and Communication Technologies and Management Tools: Materials of the 11th International Scientific and Technical Conference]*. Vol. 2. (p. 78). Baku; Kharkiv [in Ukrainian].
3. How to Know if VoIP is the Right Solution for Your Business (2020). *Weave Communications.* Retrieved from https://www.getweave.com/en-ca/how-to-know-if-voip-is-the-right-solution-for-your-business
4. Kumar, V., & Roy Om Prakash. (2021). Security and Challenges in Voice over Internet Protocols: A Survey. In *IOP Conf. Series: Materials Science and Engineering*, 012020. https://doi.org/10.1088/1757-899x/1020/1/012020
5. Chan, Y. Y., & Al-Marzouqi, S. M. (2009). Practical Implementations for Securing VoIP Enabled Mobile Devices. In *Network and System Security: Third International Conference*. Australia, Gold Coast, QLD, Oct. 19–21, 2009. (pp. 409–415). https://doi.org/10.1109/nss.2009.24
6. Popescu, E.-E. (2024). VoIP Security Threats. *International Journal of Information Security and Cybercrime, 13,* Iss. 1, 66–70. https://doi.org/10.19107/ijisc.2024.01.06
7. Sadiwala, R. (n. d.). Analysis of Security Threats of VoIP Systems. *SHODH SANGAM – A RKDF University Journal of Science and Engineering. No. 2581–5806,* Vol. 01, Iss. 02, 34–46.
8. Kumar, V., & Roy Om Prakash. (2020). Reliability and Security Analysis of VoIP Communication Systems. *Rising Threats in Expert Applications Solutions. Advances in Intelligent Systems and Computing, 1187,* 687–694. https://doi.org/10.1007/978-981-15-6014-9_84
9. Arafat, M. Y., Ahmed, F., & Sobhan, M. A. (2013). SIP Security in IP Telephony. In

International conference. Elastix World. Mexico, October, 2013. (pp. 1–11).
10. Yevseiev, S. P., Zakovorotnyi, O. Yu., & Milov, O. V. et al. (2024). *Metodolohiia syntezu modelei intelektualnykh system upravlinnia ta bezpeky ob'iektiv krytychnoi infrastruktury : monohrafiia [Methodology for the Synthesis of Models of Intelligent Control and Security Systems for Critical Infrastructure Facilities: Monograph]*. Kharkiv [in Ukrainian].
11. Alvaonos, D., Limniotis, K., & Stavrou, S. (2018). On the Cryptographic Features of a VoIP Service. *Cryptography, № 2*, Vol. 1, 1–12. https://doi.org/10.3390/cryptography2010003
12. Mazharenko, V. V. (2020). *Doslidzhennia osoblyvostei vprovadzhennia servisiv IP-telefonii v internet-resursy : mahisterska dys. 171 – Elektronika [Research on the Features of Implementing IP Telephony Services in Internet Resources: Master's thesis. 171 – Electronics]*. Kyiv [in Ukrainian].
13. Bronshpak, G. K., Gromyko, I. A., Dotsenko, S. I., & Perchik, E. L. (2014). Kriptografiia novogo pokoleniia: Integral'nye uravneniia kak al'ternativa algebraicheskoi metodologii [New Generation Cryptography: Integral Equations as an Alternative to Algebraic Methodology]. *Prikladnaia elektronika [Applied Electronics], Vol. 13,* № 3, 337–349 [in Russian].
14. Hryshchuk, O. M., & Zhylin, A. V. (2024). Novitnia tekhnolohiia kryptohrafichnoho zakhystu movnoi informatsii [The Latest Technology of Cryptographic Protection of Speech Information]. In *Aktualni pytannia zastosuvannia spetsialnykh informatsiino-komunikatsiinykh system : tezy dop. VII nauk.-prakt. konf. [Current Issues of the Application of Special Information and Communication Systems: Theses of the VII Scientific-Practical Conference]*. Kyiv, June 12, 2024. (p. 376). Kyiv [in Ukrainian].
15. Hryshchuk, O. M. (2020). Suchasni informatsiini tekhnolohii kryptohrafichnoho zakhystu informatsii u sektori bezpeky i oborony [Modern Information Technologies of Cryptographic Protection of Information in the Security and Defense Sector]. In *Hrafichni tekhnolohii modeliuvannia ob'iektiv, protsesiv ta yavyshch : tezy dop. Mizhnar. nauk.-prakt. konf. [Graphical Technologies for Modeling Objects, Processes and Phenomena: Theses of the International Scientific-Practical Conference]*. Odesa, April 23–24, 2020. (p. 87). Odesa: Military Academy [in Ukrainian].
16. Hryshchuk, O. M. (2024). Innovatsii v kryptohrafii [Innovations in Cryptography]. In *Voienni innovatsii v suchasnykh viinakh: zb. tez Mizhnar. akademich. forumu. [Military Innovations in Modern Wars: Collection of Theses of the International Academic Forum]*. (p. 192). Kyiv [in Ukrainian].
17. Hryshchuk, O. M. (2021). Symetrychna kryptosystema na dyferentsialnykh peretvorenniakh yak novyi zasib zabezpechennia kiberbezpeky VoIP-trafiku [Symmetric Cryptosystem on Differential Transformations as a New Means of Ensuring Cybersecurity of VoIP Traffic]. In *Vseukr. nauk.-prakt. internet-konf. ("Stratehii kiberstiikosti: upravlinnia ta bezperervnist biznesu") [All-Ukrainian Scientific and Practical Internet Conference ("Cyber Resilience Strategies: Management and Business Continuity")]*. Kyiv, February 25, 2021. (pp. 51–52). Kyiv: SUT [in Ukrainian].
18. Hryshchuk, O. M. (2019). Matematychnyi opys kryptosystemy Fredholma [Mathematical Description of the Fredholm Cryptosystem]. In *Mizhnar. nauk.-prakt. konf. ("Informatsiina bezpeka ta informatsiini tekhnolohii") [International scientific and practical conference ("Information Security and Information Technologies")]*. Kharkiv, April 24–25, 2019. (p. 4). Kharkiv: KhNEU [in Ukrainian].

19. Hryshchuk, O. M., & Hryshchuk, R. V. (2019). Uzahalnena model kryptosystemy Fredholma [Generalized Model of Fredholm Cryptosystem]. *Kiberbezpeka: osvita, nauka, tekhnika [Cybersecurity: Education, Science, Technology]*, *1* (4), 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423 [in Ukrainian].
20. Hryshchuk, O. (2024). Mathematical Model of a Symmetrical Cryptographic System for the Protection of Speech Information Based on Differential Transformations. *Kiberbezpeka: osvita, nauka, tekhnika [Cybersecurity: Education, Science, Technology]*, *1* (25), 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409
21. Pukhov, G. E. (1986). *Differentsial'nye preobrazovaniia i matematicheskoe modelirovanie fizicheskikh protsessov : monografiia [Differential Transformations and Mathematical Modeling of Physical Processes: Monograph]*. Kyiv [in Russian].
22. Hryshchuk, O. M. (2020). Osoblyvosti vyboru kliucha shyfruvannia dlia kryptosystemy Fredholma [Features of Choosing an Encryption Key for the Fredholm Cryptosystem]. In *Komp'iuterna inzheneriia i kiberbezpeka: dosiahnennia ta innovatsii : tezy dop. II Vseukr. nauk.-prakt. konf. [Computer Engineering and Cybersecurity: Achievements and Innovations: Theses of the II All-Ukrainian Scientific and Practical Conference]*. Kropyvnytskyi, November 25–27, 2020. (pp. 109–110). Kropyvnytskyi [in Ukrainian].
23. Hryshchuk, O. (2021). Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations. In *International security and practical conference ("Information security and information technologies").* Kharkiv, Odesa, September 13–19, 2021. (pp. 229–233).
24. Korchenko, O. H., & Hryshchuk, O. M. (2022). Porivnialnyi analiz matematychnykh modelei movnoi informatsii [Comparative Analysis of Mathematical Models of Speech Information]. *Bezpeka informatsii [Information Security]*, *2* (28), 48–56. https://doi.org/10.18372/2225-5036.28.16949 [in Ukrainian].
25. Hryshchuk, O. M. (2022). Dyferentsialnyi spektr movnoi informatsii [Differential Spectrum of Speech Information]. *Zakhyst informatsii [Information Security]*, *3* (24), 120–128. https://doi.org/10.18372/2410-7840.24.17189 [in Ukrainian].
26. Krylyk, L. V., Bohach, I. V., & Lisovenko, A. I. (2019). *Chyselne intehruvannia funktsii [Numerical Integration of Functions]*. Vinnytsia [in Ukrainian].
27. Hryshchuk, R. V. (2010). *Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren : monohrafiia [Theoretical Foundations of Modeling Information Attack Processes Using Methods of Differential Game Theories and Differential Transformations: Monograph]*. Zhytomyr [in Ukrainian].
28. Pukhov, G. E. (1980). *Differentsial'nye preobrazovaniia funktsii i uravnenii : monografiia [Differential Transformations of Functions and Equations: Monograph]*. Kyiv [in Russian].
29. Pukhov, G. E. (1990). *Differentsial'nye spektry i modeli : monografiia [Differential Spectra and Models: Monograph]*. Kyiv [in Russian].
30. Tikhonov, A. M., & Arsenin, V. Ia. (1979). *Metody resheniia nekorrektnykh zadach [Methods for Solving Ill-posed Problems]*. Moscow [in Russian].
31. Okhrimenko, M. H., Zhukovska, O. A., & Kupka, O. O. (2022). *Metody rozv'iazuvannia nekorektno postavlenykh zadach [Methods of Solving Incorrectly Posed Problems]*. Kyiv [in Ukrainian].

32. Phillips, D. L. (1962). A Technique for the Numerical Solution of Certain Integral Equations of the First Kind. *J. Ass. Comput*., 84–97. https://doi.org/10.1145/321105.321114
33. Ferguson, N., Schroeppel, R., Whiting, D. (2001). A Simple Algebraic Representation of Rijndael. *Selected Areas in Cryptography,* 103–111. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45537-X_8
34. Wazwaz, A. M. (2011). The Regularization Method for Fredholm Integral Equations of the First Kind. *Computer Methods in Applied Mechanics and Engineering, 61,* 2981–2986. https://doi.org/10.1016/j.camwa.2011.03.083
35. Wazwaz, A. M. (2011). The Regularization-Homotopy Method for the Linear and Non-Linear Fredholm Integral Equations of the First Kind. *Communications In Numerical Analysis, Vol. 2011,* 1–11. https://doi.org/10.5899/2011/cna-00105

O. G. Korchenko, O. M. Hryshchuk

SPEECH INFORMATION CRYPTOGRAPHIC PROTECTION METHOD BASED ON DIFFERENTIAL TRANSFORMATIONS

The problem of information security that circulates in communication channels is constantly being updated. It is especially acute for military VoIP telephony or dual use. This relates to the growth of the value of confidential information, which is of interest to cybercriminals, and with the increase in the technological complexity of cyberattacks at the same time as the productivity of technical means of obtaining unauthorized information increases. Cryptographic methods of information protection occupy one of the key places among the well-known mechanisms for ensuring the cyber security of speech information circulating in communication channels. SRTP security protocols, which implement the symmetric cryptographic encryption algorithm AES, are most often used to organize secure VoIP traffic. At the same time, the potential compromise of the best symmetric cryptographic algorithm AES-256 requires the search for new non-trivial approaches to improving cyber security mechanisms. One of these approaches developed in the article is an approach based on the use of the Fredholm cryptosystem model. The mentioned cryptographic system belongs to the class of symmetric cryptographic systems, but to date, due to the lack of scientifically based cryptographic algorithms, it has not yet gained practical implementation. To resolve this contradiction, the article, based on the principle of O. Kerckhoffs, developed a method of cryptographic protection of speech information based on differential transformations developed by Academician of the National Academy of Sciences of Ukraine H. Pukhov. The developed method makes it possible to obtain a cipher in the form of a differential spectrum, which is resistant to known methods of cryptanalysis. The article developed an algorithm for implementing the method. The results of encryption and decryption of speech information are given. The convergence of simulation results with other known methods confirms the workability of the developed method.

Keywords: *symmetric cryptographic algorithm; differential transformations; encryption key; differential spectrum; cipher; discrete; guaranteed cryptographic strength; inverse problem; Fredholm integral equation of the first kind.*

ISSN 2076-1546
УДК 004.9:378.112 DOI: 10.46972/2076-1546.2024.27.02

І. А. Пількевич, С. І. Мірошніченко, Ю. О. Заєць, В. В. Лобода

АВТОМАТИЗОВАНА ІНФОРМАЦІЙНА СИСТЕМА «КАДРИ»

Інтенсивний розвиток інформаційних систем створює умови для розробки та впровадження сучасних інформаційних засобів, що дозволяють автоматизувати систему управління кадровим потенціалом. Технології, які забезпечують можливість переходу до нових умов застосування інформаційних систем, впроваджуються поступово.

Перехід до стадії автоматизації здійснюється з початком трансферу даних. Користувачі активно використовують зв'язок систем і баз даних усіх типів, що створюються як централізовано, так й індивідуально ними. Основною складовою розробки всіх авторизованих систем управління є особовий склад, тому початок будь-якої розробки системи автоматизації виробництва або вищого навчального закладу потрібно починати з модуля автоматизованої системи управління «Кадри», до якого потім поступово можна долучати інші частини. Тобто модуль «Кадри» є першочерговим у розробці будь-якої автоматизованої системи управління. При цьому базовими принципами її побудови є ті, які ґрунтуються на сучасних загальноприйнятих ідеях проєктування відкритих автоматизованих систем і мереж, досвіді створення й експлуатації подібних систем у провідних вищих навчальних закладах.

У статті наведено приклад базової технічної структури автоматизованої системи управління вищого навчального закладу, а також проаналізовано структури інформаційних потоків інформаційної системи «Кадри».

За результатами проведеного аналізу побудована функціональна схема роботи системи ведення обліку кадрів. Розроблено алгоритм роботи інформаційної системи ведення обліку персоналу, який складається з дев'яти блоків, а також визначено систему управління базами даних та умови програмування.

Запропоновано можливі варіанти побудови модулів інформаційної системи «Кадри» та сформульовано вимоги до її апаратного й програмного забезпечення.

Локальне тестування розробленої інформаційної системи ведення обліку кадрів дозволило зробити висновок про те, що вона працездатна й функціонує правильно.

Ключові слова: *автоматизація; інформаційна система; відділ кадрів; обмін даними; моделювання.*

Постановка проблеми в загальному вигляді. Ефективність функціонування системи управління персоналом значною мірою залежить від інформаційної бази, яка є сукупністю даних про стан керованої системи та тенденції її розвитку. Основною проблемою функціонування таких систем є обмін даними між інформаційно-керувальними підсистемами. Інформація допомагає реалізації всіх функцій управління.

Вагомий внесок у створення автоматизованої інформаційної системи (ІС) управління персоналом належить науковим школам українських і закордонних вчених: Латишева І. Л., Алімарина Е. А., Журавльова І. В., Маренкова Н. Л., Пономаренко В. С., Романішина В. О.,

© І. А. Пількевич, С. І. Мірошніченко, Ю. О. Заєць, В. В. Лобода, 2024

Юрченко В. В. тощо. Проте, незважаючи на досягнуті результати, технологія автоматизації процесу управління персоналом нині достатньо ще не вивчена [1]. З урахуванням викладеного актуальним є розроблення автоматизованої ІС «Кадри» як складової автоматизованої системи управління (АСУ) вищого навчального закладу (ВНЗ).

Аналіз останніх досліджень і публікацій. У [2, 3] описано результати розроблення ІС для роботи відділу кадрів та підтримки електронної комерції, побудовано їх функціональні моделі, запропоновано блок-схеми та програмну реалізацію Логічним продовженням цих досліджень є [4, 5], де розглянуто питання створення АСУ персоналом з елементами штучного інтелекту, досліджено основні джерела інформації, сформульовано критерії оцінювання її якості, а також запропоновано АСУ кадрами за допомогою вбудованого в ІС інтерфейсного модуля. Варто зазначити, що багато джерел звертають увагу на перспективу розвитку автоматизованих ІС для роботи відділу кадрів, зокрема й у військовій сфері. Деякі з них зазначають, що такі технології мають велику перспективу в захисті ІС із закритим доступом [6].

Формулювання завдання дослідження. Основною метою роботи є розробка ІС ведення обліку кадрів ВНЗ, яка пришвидшує роботу системи та заощаджує час користувача, є базовою для створення інших модулів АСУ. Відомо [7], що використання комп'ютерних облікових програм дозволяє підвищити оперативність ведення обліку, збільшити рівень його деталізації, посилити контроль за достовірністю та правильністю облікової інформації на всіх етапах її оброблення. Саме тому завданням статті є розробка автоматизованої ІС «Кадри» як складової АСУ ВНЗ.

Виклад основного матеріалу. Згідно з принципом єдиної технічної політики побудови АСУ у ВНЗ повинні бути оновлені засоби обчислювальної техніки та зв'язку, які відповідають його актуальним вимогам. Завдання АСУ для конкретного закладу можуть відрізнятися, але загальні вимоги до неї є базовими. Приклад узагальненої базової технічної структури інтегрованої інформаційно-обчислювальної системи наведено на рис. 1.

Рис. 1. Варіант базової технічної структури АСУ ВНЗ

У ході аналізу структури АСУ ВНЗ можемо побачити, що головним елементом, на який замикається практично кожний модуль системи, є модуль «Кадри», саме тому розроблення практично будь-якої АСУ потрібно починати з його створення.

Для порівняння різних популярних баз даних слід враховувати, чи зручна для користувача конкретна система управління базами даних (СУБД), чи буде вона добре інтегруватися з іншими продуктами, які вже використовуються. Крім того, під час вибору СУБД слід взяти до уваги вартість системи й підтримки, що надається розробником.

Аналіз структури інформаційних потоків ІС «Кадри». Графічна модель – це засіб відображення структури компонентів програмних систем у процесах аналізу та проєктування ІС. На діаграмах DFD (Data Flow Diagram) відображаються потоки даних, процеси їх перетворення із вхідних на вихідні, а також сховища, джерела та споживачі інформації, зовнішні щодо системи. Кожний із процесів може бути поданий діаграмою нижчого рівня.

Блоки на DFD-діаграмі системи, що проєктується, розміщуються за ступінчастою схемою відповідно до їх домінування – впливу, який один блок здійснює на інші (рис. 2).

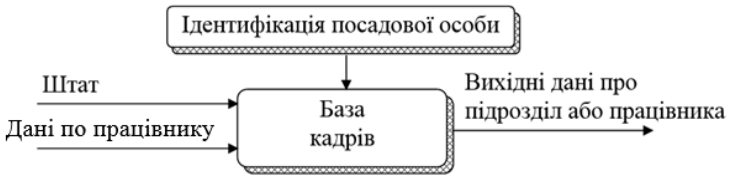


Рис. 2. Контекстна DFD-діаграма

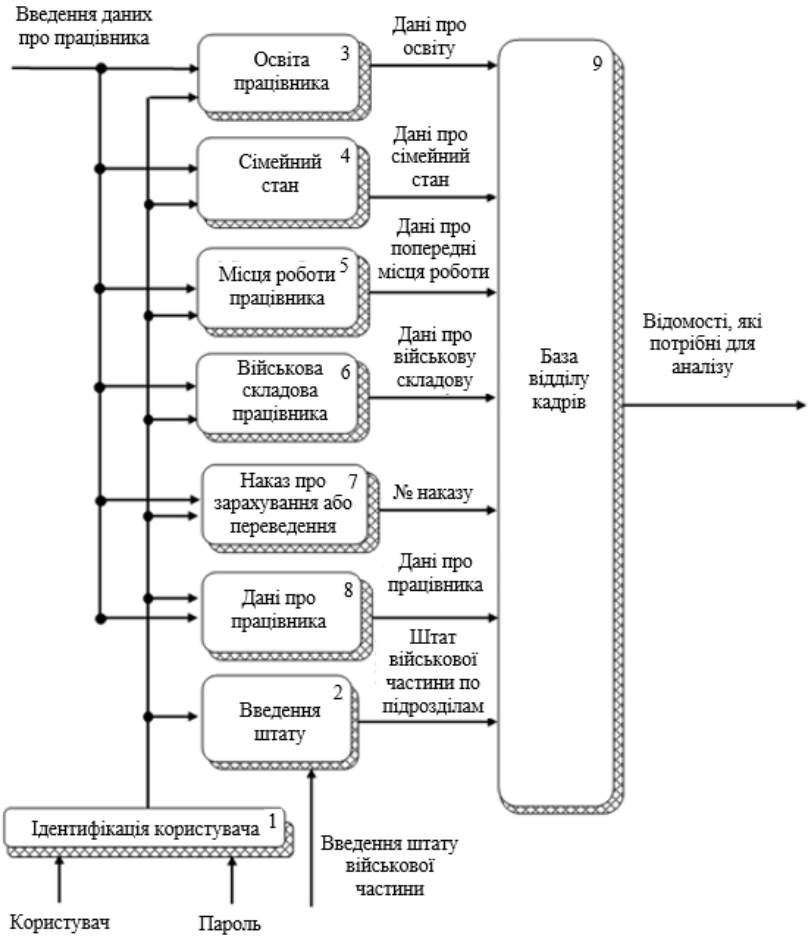


Рис. 3. Декомпозиційна DFD-діаграма

На рис. 3 наведено декомпозицію контекстної діаграми та функціональні складові ІС «Кадри». Виходячи з неї, можна побудувати варіант схеми роботи ІС ведення обліку кадрів ВНЗ, який складатиметься з блоків (рис. 4). Правильне функціонування всіх елементів схеми забезпечує швидку роботу системи та заощаджує час користувача.

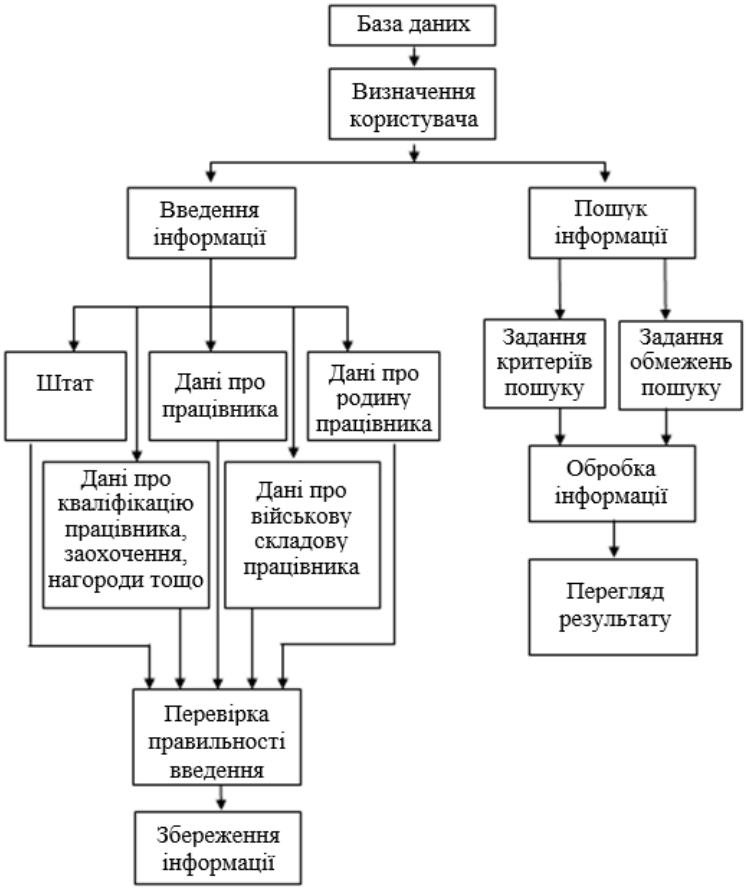


Рис. 4. Функціональна схема роботи системи ведення обліку кадрів

Процес розв’язування будь-якої задачі на ЕОМ є обробкою даних за заданим алгоритмом. **Алгоритм роботи** ІС ведення обліку кадрів складається з дев’яти блоків (рис. 5).

Перший блок призначений для визначення користувача, який працює в системі (введення імені та пароля користувача, надання йому можливості доступу до визначених функцій роботи в системі).

У другому блоці визначаються критерії роботи користувача. Якщо він не є адміністратором мережі (для нашого випадку – працівник відділу особового складу), то переходить до восьмого блоку, в іншому разі – до третього.

У третьому блоці вводиться штат ВНЗ (військової частини). Якщо користувач є адміністратором системи, то в нього є можливість заносити посади штату в базу даних ІС.

У четвертому блоці визначається вакантна посада в штаті військової частини. Якщо її немає, то керівництво встановлює, на яку посаду можливо призначити працівника, та заносить відповідні відомості про нього до бази даних. Це реалізується в п’ятому блоці з поверненням до четвертого.

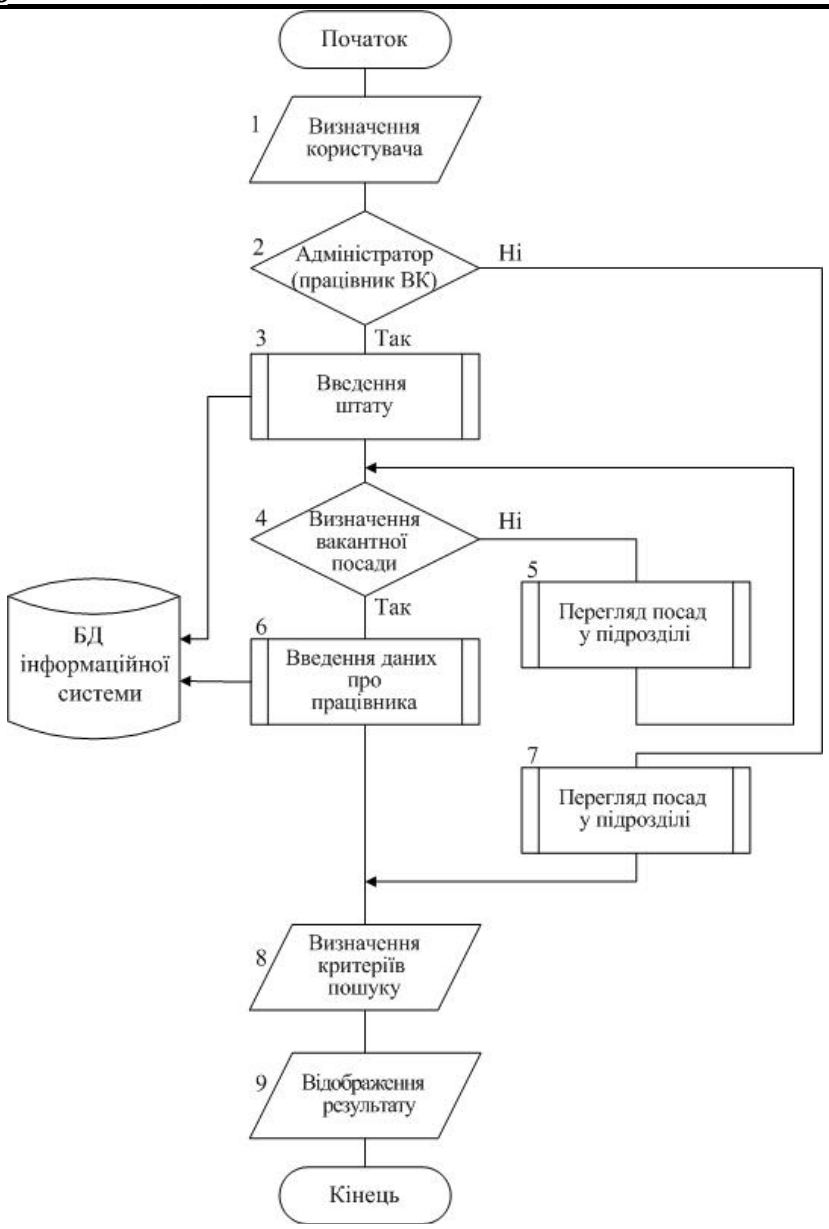


Рис. 5. Блок-схема алгоритму роботи ІС ведення кадрів

Якщо є вакантна посада, то працівник відділу кадрів у шостому блоці вносить особисті дані про працівника до бази даних ІС (освіта, попередні місця служби або роботи, сімейний стан, категорія, нагороди тощо).

Якщо користувач не є адміністратором системи, але є представником відділу кадрів, то йому можуть бути надати обмежені права для роботи з інформацією. У сьомому блоці показана можливість користувача переглядати інформацію, яка була визначена адміністратором системи.

У восьмому блоці можливий пошук документа за потрібними категоріями (якщо вони визначені), а в дев'ятому відображається інформація для її відпрацювання.

Визначення СУБД та мови програмування. Інформаційні вебсистеми мають свої переваги та недоліки. *Перевагами* є те, що ІС не вимагає встановлення на ПЕОМ об'ємного програмного забезпечення. Для повноцінної роботи потрібен браузер та доступ до Інтернету. Розробка не передбачає спеціального налаштування та адміністрування.

Необхідна лише мінімальна апаратна платформа, тому ІС можна використовувати всюди, де є доступ до глобальної мережі. Оновлення вебдодатків здійснюється автоматично адміністратором СУБД. *Недоліками* є те, що збій сервера або проміжного обладнання, яке забезпечує доступ до системи, може призвести до того, що всі дані, які зберігаються в ній, не будуть доступними. Крім того, є обмеження в інтернет-покритті деяких регіонів.

Проаналізувавши матеріал, для можливого створення ІС «Кадри» обираємо локальну систему з мовою розмітки сторінок HTML, мовою програмування PHP, сервером MySQL.

Можливий варіант побудови модуля ІС «Кадри». Варіант головного екрана ІС із введенням ідентифікації користувача показано на рис. 6. Для реєстрації необхідні ім’я (логін) та пароль.

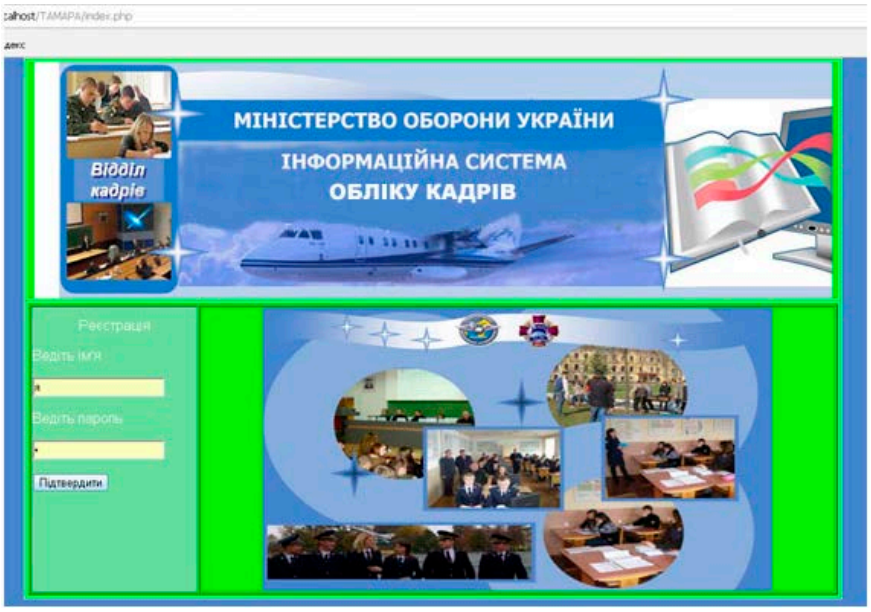


Рис. 6. Головна сторінка ІС

Новий користувач реєструється через адміністратора мережі (для нашої системи – працівника відділу кадрів, тому що саме цей підрозділ за наказом керівника закладу визначає необхідність доступу). Якщо логін або пароль неправильний, то нічого не відбувається. У разі введення правильних даних, відкривається сторінка адміністратора ІС (рис. 7).

Рис. 7. Форма адміністратора ІС

На сторінці доступна кнопка «Штатний розклад», натискаючи на яку, адміністратор потрапляє у форму введення штату, зовнішній вигляд якої наведено на рис. 8.

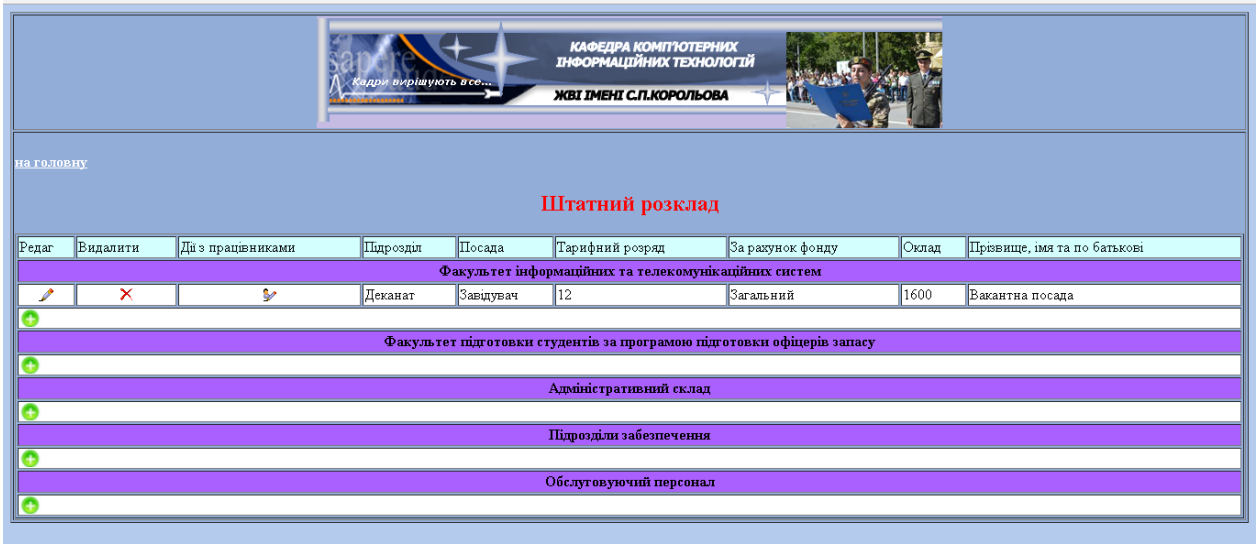


Рис. 8. Форма введення штатного розпису ІС

Штатні посади додаються натисканням на знак «+» або кнопок «Додавання», «Додати посаду» зі сторінки адміністратора ІС у формі введення нових посад (рис. 9).

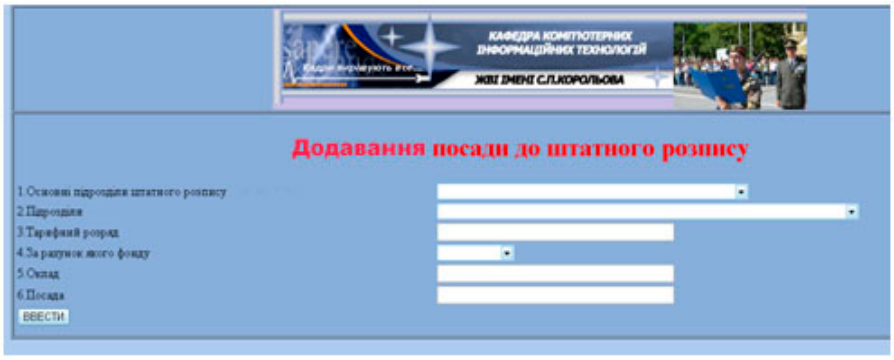


Рис. 9. Додавання посад до штатного розпису ІС

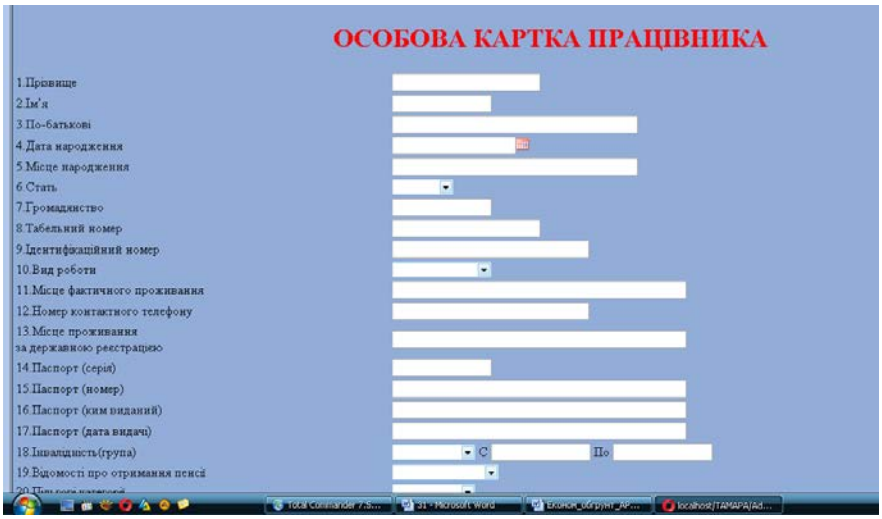


Рис. 10. Додавання особистих даних працівників до ІС

Особову картку працівника закладу наведено на рис. 10. Крім того, на сторінці введення штатного розпису є можливість видаляти непотрібні посади. У формі «Додавання» також доступне оновлення особистих даних.

Корегування та внесення додаткової інформації про працівника здійснюються під час виходу за допомогою кнопки «Пошук» із введенням початкової літери його прізвища у формі, наведеній на рис. 11.

Рис. 11. Вибір працівників для корегування в ІС

Для деталізації відкриваємо форми табельного номера працівника (рис. 12).

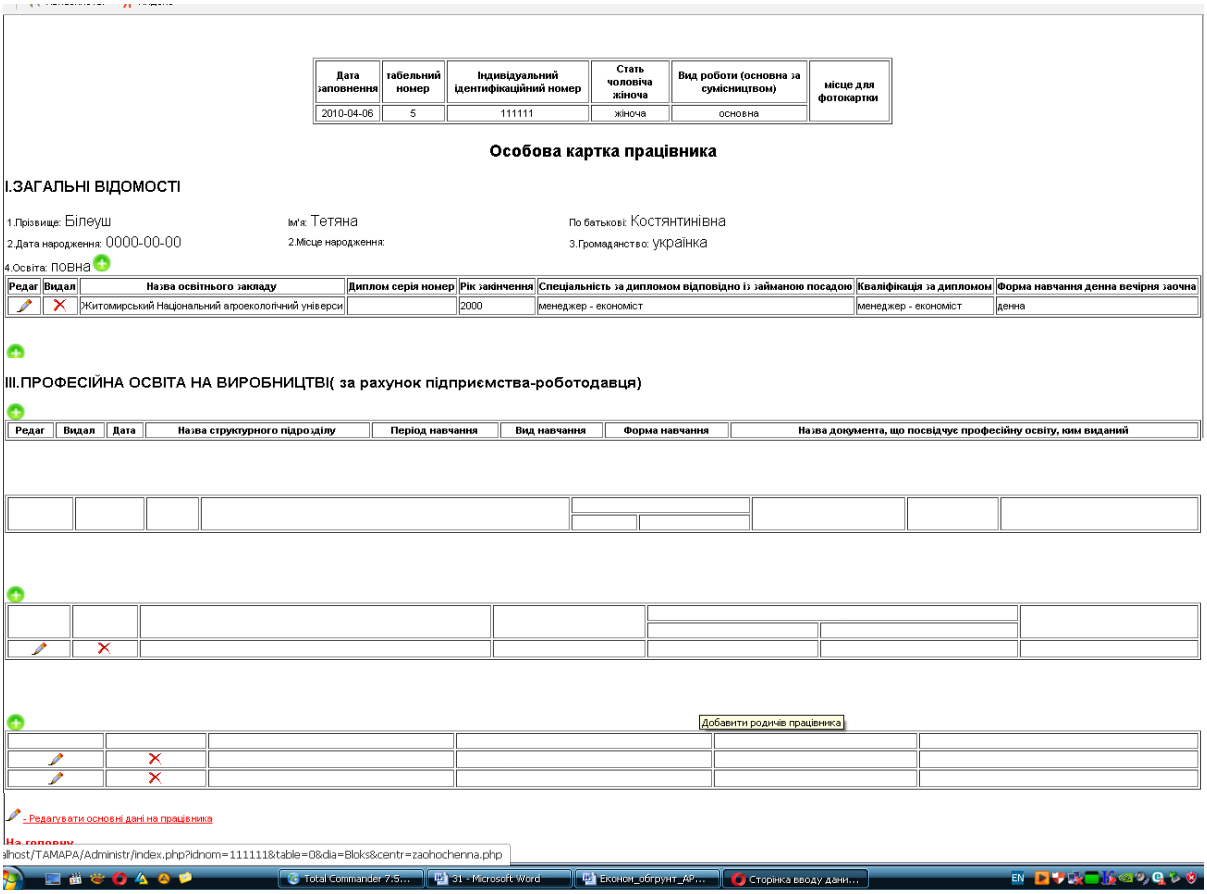


Рис. 12. Заповнення додаткових даних про працівників в ІС

У формі нагадування можна відстежити загальну інформацію про працівника закладу. Відповідну сторінку наведено на рис. 13.

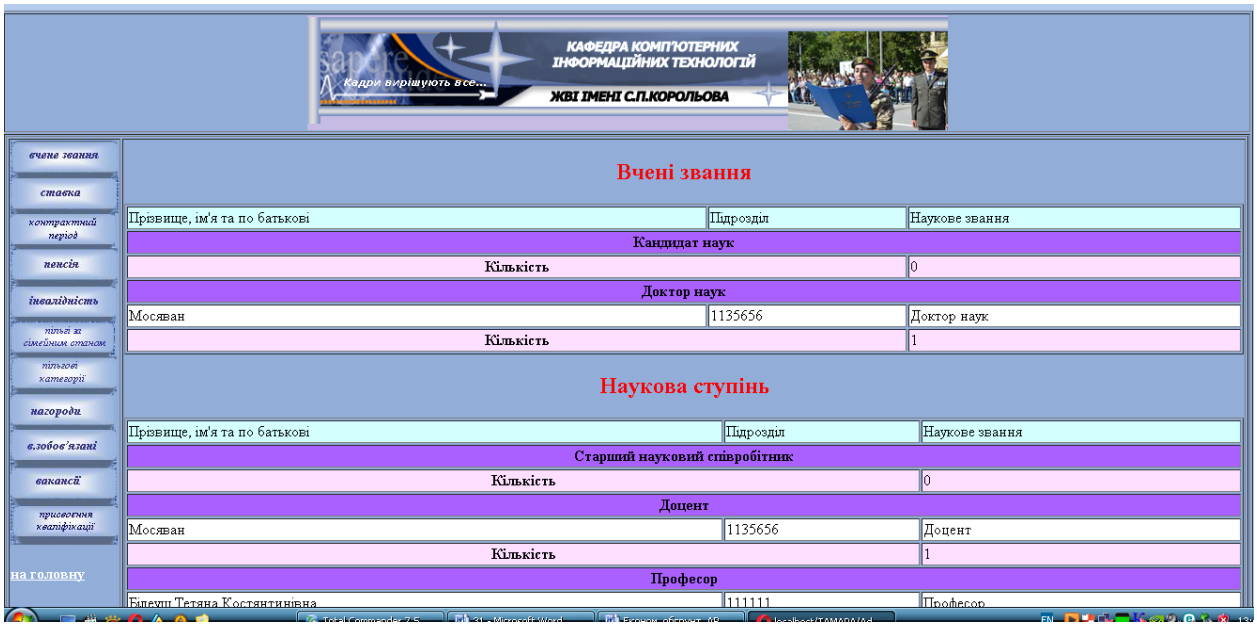


Рис. 13. Заповнення додаткових даних про працівників в ІС

Вимоги до апаратного та програмного забезпечення. Перевагою ІС є те, що вимоги до апаратного забезпечення досить невеликі. Головне, щоб була можливість завантажити браузер для відображення ІС та на жорсткому диску було достатньо місця для зберігання інформації про особовий склад. Якщо ПЕОМ буде використовуватися як сервер баз даних, то більше уваги приділяється швидкодії ліній, які з'єднують ПЕОМ користувачів у ВНЗ. Але сервер повинен бути потужним, тому що на ньому зберігається багато службових документів, крім того, оперативний запам'ятовуючий пристрій має бути також достатньо потужним для прискорення доступу для скачування або перегляду документа.

З боку користувача системні вимоги повинні дозволяти мати будь-яку операційну систему та інтернет-браузер (Internet Explorer, Mozilla, Flock, Opera) для перегляду сторінок. Апаратна конфігурація для ПЕОМ окремих користувачів може бути не дуже потужною.

Висновок. Розроблена ІС ведення обліку кадрів дозволяє представникам відділів кадрів закладу аналізувати інформацію про особовий склад та надавати необхідні відомості керівництву. Єдиною суттєвою вимогою є постійно включений сервер, де зберігається необхідна інформація.

Економічна доцільність розробки програмного забезпечення автоматизованого робочого місця оператора ведення обліку кадрів ВНЗ підтверджується тим фактом, що, навіть у разі його розроблення лише для власних потреб, воно має меншу вартість серед подібних на ринку програмних продуктів, а це дає можливість закладу зекономити матеріальні засоби. Крім того, цей модуль є основним в АСУ ВНЗ, тому за потреби необхідно додати поля до визначених таблиць для його зв'язку з іншими модулями АСУ.

Проведене локальне тестування ІС ведення обліку кадрів дозволяє зробити висновок, що система роботоздатна та працює правильно.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Про внесення змін до наказу Державної судової адміністрації України від 03.09.2015 № 163 «Про запровадження інформаційно-аналітичної системи "Кадри-WEB"» : наказ ДСА України від 06.04.2021 № 106. URL: https://zakon.rada.gov.ua/rada/show/v0106750-21#Text (дата звернення: 05.11.2024).
2. Бурлаков О. С. Інформаційні технології управління кадровим потенціалом // Modern Economics. 2019. № 14. С. 39–43. https://doi.org/10.31521/modecon
3. Гадецька З. М. Розробка та реалізація моделі інформаційної системи підтримки електронної комерції // Економіка і суспільство. 2018. Вип. 14. С. 1000–1004. URL: https://economyandsociety.in.ua/journals/14_ukr/142.pdf (дата звернення: 06.10.2024).
4. Дмитренко Т. А., Деркач Т. М., Рак Б. В. Побудова інформаційної системи відділу кадрів з елементами штучного інтелекту // Новітні інформаційні системи та технології. Полтава : ПНТУ, 2015. Т. 3. URL: https://journals.nupp.edu.ua/mist/article/view/512 (дата звернення: 15.09.2024).
5. Гафіяк А. М. Проблеми створення автоматизованої інформаційної системи управління персоналом // Економіка і суспільство. 2017. № 13. С. 1483–1487. URL: https://economyandsociety.in.ua/journals/13_ukr/244.pdf (дата звернення: 05.11.2024).
6. Левченко А. О., Трутнєв С. Г., Ісмаілова Н. П., Шарипова І. В. Програмна реалізація підсистем обміну даними експертів у розподілених комплексах імітаційного моделювання бойових дій // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2022. Вип. 22. С. 4–13. https://doi.org/10.46972/2076-1546.2022.22.01
7. Сусіденко В. Т. Інформаційні системи і технології в обліку : навч. посіб. Київ, 2016. 224 с.

Стаття надійшла до редакції 08.11.2024.

REFERENCES

1. Pro vnesennia zmin do nakazu Derzhavnoi sudovoi administratsii Ukrainy vid 03.09.2015 № 163 «Pro zaprovadzhennia informatsiino-analitychnoi systemy "Kadry-WEB"» : nakaz DSA Ukrainy vid 06.04.2021 № 106 [On Amendments to the Order of the State Judicial Administration of Ukraine from 03.09.2015 № 163 “On the Introduction of the Information and Analytical System "Kadry-WEB"”: Order of the State Judicial Administration of Ukraine from 06.04.2021 № 106.]. Retrieved from https://zakon.rada.gov.ua/rada/show/v0106750-21#Text [in Ukrainian].
2. Burlakov, O. S. (2019). Informatsiini tekhnolohii upravlinnia kadrovym potentsialom [Information Technologies for Human Resource Management]. *Modern Economics, 14*, 39–43. https://doi.org/10.31521/modecon [in Ukrainian].
3. Hadetska, Z. M. (2018). Rozrobka ta realizatsiia modeli informatsiinoi systemy pidtrymky elektronnoi komertsii [Development and Implementation of a Model of an Information System for Supporting Electronic Commerce]. *Ekonomika i suspilstvo [Economics and Society], 14*, 1000–1004. Retrieved from https://economyandsociety.in.ua/journals/14_ukr/142.pdf [in Ukrainian].
4. Dmytrenko, T. A., Derkach, T. M., & Rak, B. V. (2015). Pobudova informatsiinoi systemy viddilu kadriv z elementamy shtuchnoho intelektu [Building an Information System of the Personnel Department with Elements of Artificial Intelligence]. *Novitni informatsiini systemy ta*

tekhnolohii [New information systems and technologies], Vol. 3. Retrieved from https://journals.nupp.edu.ua/mist/article/view/512 [in Ukrainian].
5. Hafiiak, A. M. (2017). Problemy stvorennia avtomatyzovanoi informatsiinoi systemy upravlinnia personalom [Problems of Creating an Automated Information System of Personnel Management]. *Ekonomika i suspilstvo [Economy and Society], 13,* 1483–1487. Retrieved from https://economyandsociety.in.ua/journals/13_ukr/244.pdf [in Ukrainian].
6. Levchenko, A. O., Trutniev, S. H., Ismailova, N. P., & Sharypova, I. V. (2022). Prohramna realizatsiia pidsystem obminu danymy ekspertiv u rozpodilenykh kompleksakh imitatsiinoho modeliuvannia boiovykh dii [Software Implementation of Expert Data Exchange Sub-Systems in Distributed Complexes for Simulation of Combat Actions]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system : zb. nauk. prats [Problems of Construction, Testing, Application and Operation of Complex Information Systems: Scientific Journal of Korolov Zhytomyr Military Institute], 22,* 4–13. Zhytomyr: ZhMI https://doi.org/10.46972/2076-1546.2022.22.01 [in Ukrainian].
7. Susidenko, V. T. (2016). *Informatsiini systemy i tekhnolohii v obliku [Information Systems and Technologies in Accounting]*. Kyiv [in Ukrainian].

I. A. Pilkevych, S. I. Miroshnichenko, Yu. O. Zayets, V. V. Loboda

AUTOMATED INFORMATION SYSTEM “KADRY”

Intensive development of information systems creates conditions for development and implementation of modern information tools that allow automating human resources management. Technologies that enable transition to new conditions for using information systems are being introduced gradually.

Transition to automation begins with a start of data transfer. Users actively use connections between systems and databases all types, created both centrally and individually. Personnel is the main component development of all authorized management systems, so beginning any development of a production automation system or a higher education institution should start with a module of automated management system “Kadry”, to which other parts can be gradually added. In other words, “Kadry” module is a priority in developing any automated management system. At the same time, basic principles of its construction are those based on modern, generally accepted ideas of designing open automated systems and networks, and experience in creating and operating similar systems in leading higher education institutions. In this paper, we present an example a basic technical structure for an automated management system at a higher education institution and analyse information flow structures of the information system “Kadry”.

Based on results of analysis, a functional diagram of personnel records management system is built. Algorithm of the information system for personnel accounting, consisting in nine blocks, has been developed, and database management system and programming conditions have been defined.

Possible options for building modules of the information system “Kadry” are proposed and requirements for its hardware and software are formulated.

Local testing a developed information system for keeping records on personnel allowed to conclude that it is efficient and functions correctly.

Keywords: *automation; information system; human resources department; data exchange; modelling.*

УДК 004.4:003.26:681.326.3 DOI: 10.46972/2076-1546.2024.27.03

С. Г. Трутнєв

АНАЛІЗ ІМОВІРНИХ ВИТОКІВ ПОМИЛОК В ОБЧИСЛЕННІ МАТЕМАТИЧНИХ МОДЕЛЕЙ БОЙОВИХ ДІЙ У КОМП'ЮТЕРНИХ СИСТЕМАХ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

На сьогодні є безліч ситуацій, коли практично провести науковий дослід або відтворити певні обставини для прийняття виваженого рішення є неможливим чи потребує значних фінансових витрат. У такому разі завжди приходять на допомогу комп'ютерні системи імітаційного моделювання, які вже тривалий час використовуються для прийняття рішень, що впливають на людські життя, планування бойових дій, напрямки розвитку видів Збройних Сил та галузей промисловості й навіть перспективи державотворення. Але фахівці у відповідних сферах, ґрунтуючись на підсумках комп'ютерних розрахунків із поданням чисел у двійковому коді з плаваючою комою, не враховують особливостей точності цих розрахунків із двійковими числами та впливу двійкової арифметики на результати імітаційного моделювання. Як правило, математичні результати комп'ютерних розрахунків прийнято вважати достовірними, хоча вони можуть містити похибку, яка залежить від апаратного забезпечення електронно-обчислювальної машини, а саме від розрядності шини процесора. Це зумовлено технічним стандартом IEEE 754 для арифметики з плаваючою комою.

У статті проаналізовано математичні моделі, які використовуються в системах імітаційного моделювання бойових дій, та підходи до їх розв'язання. Проведено деталізацію подання бінарних чисел із плаваючою комою в комп'ютерних системах різної розрядності та визначено можливі витоки помилок у разі подання чисел у двійковому коді, а також проведено математичні розрахунки. Такий підхід дозволяє враховувати можливі межі похибок на етапі введення даних у комп'ютерні системи для обчислення та безпосередньо в ході проведення математичних розрахунків в електронно-обчислювальних системах.

Ключові слова: *подання чисел із плаваючою комою; математична модель; система моделювання бойових дій; архітектура комп'ютера; помилки моделювання; помилки округлення; діапазон точності чисел; стандарт IEEE 754.*

Постановка проблеми в загальному вигляді щодо витоку помилок у системах імітаційного моделювання бойових дій полягає в такому.

Незважаючи на бурхливий розвиток систем імітаційного моделювання бойових дій (СІМБД) та їх широке застосування для підготовки військ [1], питання забезпечення їх надійності та достовірності результатів моделювання залишається відкритим.

Сучасні методи верифікації та валідації СІМБД не в повній мірі вирішують проблеми, пов'язані із суб'єктивністю експертних оцінок, неповнотою вихідних даних та складністю порівняння з реальними даними.

© С. Г. Трутнєв, 2024

Отже, актуальною науковою проблемою є розроблення нових підходів до визначення помилок у системах імітаційного моделювання, які дозволять зменшити або врахувати похибку результатів моделювання.

Аналіз останніх досліджень і публікацій, у яких висвітлено проблеми виявлення та виправлення помилок у СІМБД, показує, що це питання залишається актуальним.

У роботі [2] досліджено традиційні підходи до верифікації та валідації СІМБД за допомогою оцінювання роботи моделі через числові експерименти, налаштування її параметрів на основі реальних даних для забезпечення точності моделювання, документування всіх процесів верифікації та валідації для зберігання прозорості й відслідковуваності.

Автори [3] спрямовують свою увагу на здійснення моніторингу та аналізу стохастичних випробувань. Результатом цього дослідження є порівняння отриманих результатів моделювання з реальною моделлю. Як джерело витоку похибок розглядається некоректний опис імітаційної моделі за допомогою програмного коду.

У [4] запропоновано підхід до впровадження технологій 3D цифрової симуляції для підвищення точності моделювання, покращення візуалізації, ідентифікації проблеми на ранніх етапах та зниження людського фактора. Ідентифікація й усунення помилок зводиться до виявлення візуальних аномалій під час тестування та виправлення програмного коду програмістом. У цілому впровадження 3D цифрових технологій симуляції дозволяє зробити процес виявлення й усунення помилок у системах імітаційного моделювання більш ефективним і точним. Це покращує якість систем, знижує витрати на виправлення помилок та підвищує надійність кінцевих продуктів.

У дисертаційній роботі [5] розглядаються протоколи та стандарти для симуляції й ко-симуляції, які застосовуються в складних морських операціях. Основні аспекти дослідження включають розробку протоколів (створення та впровадження протоколів, які забезпечують ефективну взаємодію між різними симуляційними системами), стандартизацію (визначення стандартів, які дозволяють уніфікувати процеси ко-симуляції, що є критично важливим для забезпечення сумісності різних систем). Основними джерелами витоку помилок автор визначає складність опису й реалізації розробленої моделі та технічні обмеження обчислювальних ресурсів.

У статті [6] запропоновано використовувати методи тестування програмного забезпечення, зокрема White Box та Black Box. White Box Testing підходить для ситуацій, коли необхідно перевірити внутрішню логіку та структуру коду. Black Box Testing дозволяє сфокусуватися на функціональних вимогах і спрощує процес тестування, не потребуючи знань коду.

Слід зазначити, що найефективніший підхід до тестування програмного забезпечення включає використання обох методів у комбінації для забезпечення повного покриття тестами та виявлення якомога більшої кількості потенційних проблем. Це дозволяє поєднувати глибоку внутрішню перевірку коду з перевіркою функціональної відповідності вимогам, частково автоматизувати процес тестування СІМБД та підвищити його ефективність. Проте потрібні значні обчислювальні ресурси, а для складних систем усе одно непросто забезпечити повне тестове покриття.

Деякі дослідники [7, 8] пропонують використовувати методи машинного навчання для автоматизованого виявлення аномалій та помилок у даних, отриманих у результаті моделювання. Ці підходи є перспективними, проте потребують подальшого вивчення.

Використання згаданих підходів лише допомагає розробникам переконатися, що системи імітаційного моделювання є точними, надійними й відповідними реальним умовам, проте не дозволяють виявляти шляхи витоку похибок, особливо в складних системах моделювання.

Отже, на цей час немає універсальних методів гарантованого виявлення всіх можливих помилок у СІМБД, тому потрібні подальші дослідження в цьому напрямку.

Формулювання завдання дослідження. На основі проведеного аналізу останніх досліджень бачимо, що основна тенденція щодо зменшення помилок у системах імітаційного моделювання спрямована на розробку методики верифікації [2, 3], а саме:

відповідності розробленої моделі поставленій меті та завданням дослідження. Перевіряється, чи дозволяє вона вирішувати необхідні практичні завдання;

коректності реалізації використаних математичних методів та алгоритмів. Виключаються можливі логічні та обчислювальні помилки;

адекватності зроблених спрощень і припущень. Оцінюється їх вплив на результати моделювання;

точності та стійкості обчислювальних методів. Перевіряється відсутність значних похибок моделювання.

Згадані підходи визначення помилок базуються на поєднанні традиційних шляхів (експертні оцінки, порівняння з реальними даними) та сучасних методів тестування програмного забезпечення й машинного навчання для автоматизації процесів верифікації та валідації без урахування точності розрахунків бінарних чисел із плаваючою комою в комп'ютерних системах імітаційного моделювання.

Отже, завдання цієї наукової роботи полягає в огляді та розв'язанні математичних моделей, які використовуються в СІМБД, а також визначенні можливих меж похибок результатів обчислення для подання чисел у комп'ютерних системах у двійковому коді із плаваючою комою.

Виклад основного матеріалу. Математичні моделі, які використовують у системах імітаційного моделювання бойових дій, можна умовно розділити на кілька категорій. Розглянемо їх детальніше.

1. Моделі поведінки окремих об'єктів (юнітів).

Ланчестерські моделі [9] – це сімейство диференціальних рівнянь, які описують динаміку бойових дій між двома ворожими сторонами.

Одне з найпростіших рівнянь Ланчестера має такий вигляд:

$$\begin{aligned} \frac{dx}{dt} &= -ay; \\ \frac{dy}{dt} &= -bx, \end{aligned} \qquad (1)$$

де *x*, *y* – чисельність військ обох сторін відповідно;

a, *b* – коефіцієнти ефективності ураження військ противника.

Розв'язок цієї системи диференціальних рівнянь має такий вигляд:

$$x(t)=\left(x(0)-y(0)\left(\frac{b}{a}\right)\right)exp(-abt)+y(0)\left(\frac{b}{a}\right);$$
$$y(t)=\left(y(0)-x(0)\left(\frac{a}{b}\right)\right)exp(-abt)+x(0)\left(\frac{a}{b}\right), \quad (2)$$

де $x(0), y(0)$ – початкові чисельності військ.

Аналіз цього розв'язку дозволяє оцінити динаміку втрат і визначити переможця бою.

Моделі руху окремих підрозділів [10]. Однією з поширених моделей руху окремих підрозділів є модель на основі системи звичайних диференціальних рівнянь:

$$\frac{dx}{dt}=v\times\cos a;$$
$$\frac{dx}{dt}=v\times\sin a; \quad (3)$$
$$\frac{da}{dt}=u,$$

де *x*, *y* – координати поточного положення підрозділу;

α – курс підрозділу;

v – швидкість руху;

u – кутова швидкість повороту.

Розв'язок цієї системи має такий вигляд:

$$x(t)=x(0)+\int v(\tau)\times\cos a(\tau)d\tau;$$
$$y(t)=y(0)+\int v(\tau)\times\sin a(\tau)d\tau; \quad (4)$$
$$a(t)=a(0)+\int u(\tau)d\tau.$$

За допомогою цієї моделі можна визначити траєкторію руху підрозділу залежно від його маневрів.

Моделі вогневого ураження [11]. Одна з найпростіших моделей вогневого ураження має вигляд рівняння:

$$\frac{dN}{dt}=-\lambda N, \quad (5)$$

де *N* – чисельність цілей (живої сили);

λ – інтенсивність вогню (імовірність ураження однієї цілі за одиницю часу).

Розв'язок цього рівняння:

$$N(t) = N(0)exp(-\lambda t), \tag{6}$$

де $N(0)$ – початкова чисельність цілей.

Ця модель дозволяє розрахувати залишкову чисельність цілей після вогневого впливу. Її можна використовувати для моделювання ефективності артилерійських обстрілів, авіаударів тощо.

2. Моделі бойового середовища.

Моделі місцевості, рельєфу, погодних умов [10]. Однією з поширених моделей рельєфу місцевості є модель у вигляді випадкового поля:

$$h(x,y) = h_0(x,y) + \sigma\xi(x,y), \tag{7}$$

де $h(x,y)$ – висота рельєфу в точці з координатами (x,y);

$h_0(x,y)$ – детермінована складова рельєфу;

$\xi(x,y)$ – випадкове поле (шум);

σ – інтенсивність флуктуацій рельєфу.

Формального розв'язку це рівняння не має. Його використовують для статистичного моделювання рельєфу з урахуванням випадкових варіацій.

Схожі стохастичні моделі можна побудувати і для інших характеристик місцевості: температури, опадів, вітру тощо.

Моделі електромагнітної, акустичної обстановки [12]. Розглянемо приклад математичної моделі для аналізу електромагнітної обстановки.

Рівняння Максвелла для електромагнітного поля в середовищі має такий вигляд:

$$\begin{aligned} \nabla \times E &= -\frac{\mu \partial H}{\partial t}; \\ \nabla \times H &= -\frac{\varepsilon \partial E}{\partial t}, \end{aligned} \tag{8}$$

де E – напруженість електричного поля;

H – напруженість магнітного поля;

μ – магнітна проникність;

ε – діелектрична проникність.

Припустимо, що джерелом електромагнітного випромінювання є диполь із моментом p. Тоді розв'язок цих рівнянь для компонент електричного поля матиме такий вигляд:

$$\begin{aligned} Ex &= \left(\frac{kp2x}{r3}\right) exp(j\omega t); \\ Ey &= \left(\frac{kp2y}{r3}\right) exp(j\omega t), \end{aligned} \tag{9}$$

де $k = \frac{1}{\varepsilon\mu}$ – хвильове число;

ω – циклічна частота.

Отже, модель дозволяє розрахувати просторовий розподіл та частотні характеристики електромагнітного поля.

3. Моделі командного управління.

Теоретико-ігрові моделі прийняття рішень [13]. Однією з теоретико-ігрових моделей для систем імітаційного моделювання бойових дій є диференціальна гра переслідування – ухилення:

$$\frac{dx_1}{dt} = v_1(t);$$
$$\frac{dx_2}{dt} = v_2(t), \tag{10}$$

де x_1 – позиція першого гравця (переслідувача);

x_2 – позиція другого гравця (того, хто ухиляється).

Швидкості гравців v_1 та v_2 є керованими змінними. Кожен із них намагається максимізувати / мінімізувати цільовий функціонал:

$$J = \varphi(x_1(T), x_2(T)) + \int [L_1(x_1, v_1) + L_2(x_2, v_2)dt]. \tag{11}$$

Розв'язок полягає в знаходженні оптимальних швидкостей $v_1(t)$, $v_2(t)$, що задовольняють рівняння Гамільтона – Якобі – Беллмана.

Моделі інформаційного обміну [14]. Однією з моделей інформаційного обміну для імітаційного моделювання бойових дій є модель ss випадковими затримками

$$\tau = \tau_0 + \xi, \tag{12}$$

де τ – затримка доставки повідомлення;

τ_0 – мінімальна затримка;

ξ – випадкова складова затримки.

Припустимо, що ξ підпорядкована показовому розподілу з параметром λ:

$$f(\xi) = \lambda e - \lambda\xi, \xi \geq 0. \tag{13}$$

Тоді математичне сподівання та дисперсія затримки дорівнюють:

$$M[\tau] = \tau_0 + \frac{1}{\lambda};$$
$$D[\tau] = \frac{1}{\lambda^2}. \tag{14}$$

Отже, модель дозволяє врахувати випадкові коливання затримки передачі даних у ході моделювання інформаційного обміну.

4. Комплексні (агреговані) моделі бойових дій для оцінювання ефективності застосування угруповань військ, озброєння тощо [11].

Однією з відомих агрегованих моделей є *модель Ланчестера*, яка описує динаміку втрат двох протиборчих сторін диференціальними рівняннями:

$$\begin{aligned} \frac{dx}{dt} &= -ay; \\ \frac{dy}{dt} &= -bx, \end{aligned} \tag{15}$$

де *x, y* – кількість одиниць техніки або особового складу першої та другої сторони відповідно;

a, b – коефіцієнти ефективності ураження.

Розв’язок цієї системи має такий вигляд:

$$\begin{aligned} x(t) &= \frac{x(0)-y(0)}{\frac{b}{a}} \times exp(-at) + \frac{y(0)}{\frac{b}{a}}; \\ y(t) &= \frac{y(0)-x(0)}{\frac{a}{b}} \times exp(-bt) + \frac{x(0)}{\frac{a}{b}}. \end{aligned} \tag{16}$$

Модель дозволяє аналізувати співвідношення сил і засобів та прогнозувати результат протистояння.

Отже, є широкий спектр математичних моделей, які в тій чи іншій мірі використовуються в СІМБД. Проте розв’язок таких моделей у більшості випадків описано дробовими числами, що в разі обчислення на ЕОМ буде подано двійковим кодом числа з плаваючою комою.

Числа з плаваючою комою в комп’ютерних системах подані за допомогою стандарту IEEE 754, який є найбільш використовуваним для арифметики з плаваючою комою. Стандарт визначає кілька форматів для різних рівнів точності [15]. Розглянемо їх.

Одинарна точність (single precision) – це стандартний формат подання чисел із плаваючою комою з точністю 32 біти в комп’ютерних системах.

Формат одинарної точності:

1) 1 біт знака (0 – додатне, 1 – від’ємне число);

2) 8 біт експоненти;

3) 23 біти мантиси.

Експонента відповідає порядку числа і показує ступінь числа 2, у який піднесена мантиса.

Мантиса містить значущі цифри числа у форматі з фіксованою комою.

Отже, число з одинарною точністю має такий вигляд:

$(-1)^{знак}$ x (1 + мантиса) x $2^{(експонента - 127)}$.

Завдяки цьому формату можна подати числа в діапазоні близько від ±1,18 x 10^{-38} до ±3,4 x 10^{38} з точністю до 7 знаків.

За допомогою формату одинарної точності (32 біти) неможливо точно подати такі числові значення:

дуже великі числа, що перевищують діапазон близько ±3,4 x 10^{38}, оскільки в разі спроби подати їх відбувається переповнення і результатом буде "+∞" або "-∞";

дуже малі числа, менші за ±1,18 x 10^{-38}, оскільки вони будуть просто округлені до нуля;

числа, які неможливо точно подати обмеженою кількістю двійкових цифр. Наприклад, число 0,1 буде подано наближено, оскільки у двійковій системі воно має нескінченну періодичну дробову частину;

деякі раціональні числа, такі як 1/10, 1/3 тощо, оскільки вони також можуть мати нескінченну періодичну дробову частину у двійковому поданні.

Отже, формат 32 біт накладає певні обмеження на числовий діапазон і точність. Для більш точного подання великих або малих чисел потрібно використовувати формат подвійної точності (64 біти).

Формат подвійної точності (double precision) – це 64-бітне подання чисел із плаваючою комою, яке забезпечує більший числовий діапазон і точність, ніж 32-бітний формат одинарної точності.

Структура 64-бітного формату подвійної точності:

1) 1 біт знака;

2) 11 біт експоненти;

3) 52 біти мантиси.

Подання числа аналогічне одинарній точності:

$(-1)^{знак}$ x (1 + мантиса) x $2^{(експонента - 1023)}$.

Основні характеристики подвійної точності:

більший діапазон значень – від ±2,23 x 10^{-308} до ±1,80 x 10^{308};

більша точність – близько 15–17 значущих цифр;

11 біт експоненти замість 8 дозволяють краще подати надвеликі та надмалі числа.

Подвійна точність дозволяє точніше подавати дійсні числа, зменшує похибки округлення та краще працює в наукових й інженерних розрахунках. Проте вона займає більше пам’яті і потребує складніших обчислень.

Формат подвійної точності (64 біти) має суттєво більший числовий діапазон і точність, ніж формат одинарної точності (32 біти). Однак є певні обмеження, через які деякі числові значення неможливо точно подати:

дуже великі та дуже малі числа за межами діапазону від ±2,23 x 10^{-308} до ±1,80 x 10^{308}, оскільки в разі їх подання відбувається переповнення або вони округляються до нуля;

числа, які мають більше 15–17 значущих цифр, оскільки після цієї кількості починається втрата точності через недостатню кількість біт у мантисі;

ірраціональні числа, такі як π, √2 тощо, матимуть наближене значення, оскільки мають нескінченну кількість десяткових знаків;

раціональні числа, які мають нескінченну періодичну дробову частину у двійковому поданні (1/3, 1/10 тощо), також будуть наближеними.

Отже, головне обмеження – скінченна точність 64 бітів. Через це завжди будуть числа, які не можливо подати абсолютно точно.

Розширені формати з плаваючою комою, які забезпечують ще більшу точність, ніж подвійна:

1) 80-бітний формат:

використовується в деяких спеціалізованих процесорах;

1 біт знака, 15 бітів експоненти, 64 біти мантиси;

майже удвічі більша точність.

2) 128-бітний формат (квадруплетна точність):

теоретично дозволяє до 34 значущих десяткових цифр;

підтримується деякими мовами програмування і бібліотеками;

1 біт знака, 15 бітів експоненти, 112 бітів мантиси;

дуже висока точність обчислень, але повільніша обробка.

Ці формати використовують там, де потрібна надзвичайно висока точність: у наукових розрахунках; для оброблення зображень; у фінансовій математиці. Проте вони займають більше пам'яті та потребують спеціальної підтримки процесором [16].

128-бітний формат з плаваючою комою (квадруплетна точність) має дуже великий числовий діапазон, здатний точно подавати числа з 34 десятковими знаками. Проте все одно є певні обмеження:

числа за межами діапазону від $\pm 3.6 \times 10^{-4932}$ до $\pm 1.2 \times 10^{4932}$, оскільки в разі їх подання відбудеться переповнення або округлення до нуля чи $\pm \infty$;

для чисел з більш ніж 34 значущими десятковими цифрами почнеться втрата точності через обмежену кількість бітів у мантисі (112 бітів);

деякі ірраціональні числа все одно матимуть усічене значення (наприклад π, √2 тощо), оскільки мають нескінченну кількість десяткових знаків;

раціональні числа з нескінченною періодичною дробовою частиною у двійковому поданні.

Отже, 128-бітний формат може з високою точністю подавати більшість практичних чисел, але теоретично завжди будуть значення за його межами точності.

Із викладеного вище можна зробити висновок, що основними причинами виникнення похибки в обчисленнях математичних моделей із числами з плаваючою комою є:

помилки округлення (через скінченну точність подання проміжні та кінцеві результати округлюються, що накопичує похибку);

втрата значущих цифр (якщо число має більше значущих цифр, ніж дозволяє формат, то відбувається відсікання цифр молодшого розряду);

переповнення / підповнення (якщо результат виходить за межі діапазону подання, то відбувається переповнення до $\pm\infty$ або округлення до нуля);

нестійкість (помилки округлення можуть накопичуватися та призводити до різких відхилень результату).

Опис рішень

Виходячи із зазначеного вище, ми не можемо вважати результат обчислення математичних моделей систем імітаційного моделювання бойових дій як дійсний, але можемо підвищити точність обчислень із числами з плаваючою комою в такі способи [17, 18]:

1) використовувати формат із більшою точністю: подвійну замість одинарної, розширені формати (80-бітний або 128-бітний замість подвійної);

2) уникати операцій, що накопичують похибки (додавання / віднімання замість множення / ділення), використовувати компенсоване сумування;

3) збільшувати кількість значущих цифр у проміжних обчисленнях, округлюючи результат лише вкінці;

4) використовувати алгоритми з підвищеною стійкістю та зниженням похибок округлення;

5) для дуже великих чисел застосовувати строкове подання або подання у вигляді масивів.

Висновки. У статті розглянуто математичні моделі та підходи до їх рішення, які використовуються в комп'ютерних системах імітаційного моделювання. Ці математичні моделі описані у вигляді рівнянь або системи диференціальних рівнянь, що в процесі їх подання в бінарному коді та машинному розрахунку приводить до використання чисел із плаваючою комою. Відповідно до технічного стандарту IEEE 754 щодо апаратних особливостей комп'ютерної системи імітації бойових дій можливо припустити розмір похибки математичних розрахунків у разі заокруглення чисел або уникнути помилки ділення на 0 у ході обрахунку надмалих чисел, поданих у двійковому коді із плаваючою комою.

Результати дослідження в подальшому будуть використовуватися для створення підходів до зменшення похибок у СІМБД та розроблення методики підрахунку сумарної похибки моделювання.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Шинкарук О., Михайлишин О. Окремі аспекти застосування імітаційного моделювання у підготовці складових сектору безпеки і оборони України // Зб. наук. праць Нац. академії Держ. прикордон. служби України. 2019. № 80 (2). С. 227–241 https://doi.org/10.32453/3.v80i2.201

2. Data Modeling Versus Simulation Modeling in the Big Data era: Case Study of a Greenhouse Control System / Kim B., Kang B., Choi S., Rim T. // SAGE Publications. 2017. № 93 (7). P. 579–594. https://doi.org/10.1177%2F0037549717692866

3. Blake J. Uncertainty and Error in Combat Modeling, Simulation, and Analysis : Dissertation for Philosophiae Doctor 19.12.2019. USA. 2019. 152 p. URL: https://apps.dtic.mil/sti/trecms/pdf/AD1089578.pdf (last accessed: 01.09.2024).

4. Research on Application Method of 3D Digital Simulation Technology in Spacecraft Assembly / Zhang B., Wang Q., Wang X., Liang Y. // Lecture Notes in Electrical Engineering Signal and Information Processing, Networking and Computers. 2019. № 550. P. 400-409. https://doi.org/10.1007/978-981-13-7123-3_47

5. Hatledal L. Protocols and Standard for Simulation Co-Simulation – For Demanding Maritime Operations : Dissertation for Philosophiae Doctor 03.2021/ Trondheim, 2021. 144 p. URL: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2755142

6. Nidhra S., Dondeti J. Black Box and White Box Testing Techniques : a literature review // International Journal of Embedded Systems and Applications (IJESA). 2012. № 2 (2). P. 29–50. http://dx.doi.org/10.5121/ijesa.2012.2204

7. Exploring the Epidemiological Impact of Universal Access to Rapid Tuberculosis Diagnosis Using Agent-Based Simulation / Kasaie P., Sohn H., Kendall E. et al. // Winter Simulation Conference (WSC) 2017. P. 1097–1108. https://doi.org/10.1109/WSC.2017.8247858

8. A Compact Dual-Band Impedance Matching Network Based on All-Pass Coupled Lines / Banerjee D., Saxena A., Hashmi M. et al. // IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS). 2019. P. 937–939. https://doi.org/10.1109/MWSCAS.2018.8623957

9. Ковтун В. Математичні моделі війни на основі рівняння Ланчестера : випускна кваліфікаційна робота бакалавра. Спец. 113 Прикладна математика. Київ, 2023. 55 с. URL: https://ir.library.knu.ua/handle/123456789/5757 (дата звернення: 10.10.2024).

10. Tolk A. Engineering Principles of Combat Modeling and Distributed Simulation : Monograph. New Jersey, 2012. 944 p. https://doi.org/10.1002/9781118180310.fmatter

11. Mikayılov T., Bayramov A. Principles of Using the Mathematical Models of Combat Activities and Means of Destructions During Operational Preparation of the Troops // Сучасні інформаційні системи. 2020. № 4 (1). С. 24–27. https://doi.org/10.20998/2522-9052.2020.1.04

12. Kress M. Lanchester Models for Irregular Warfare // Mathematics. 2020. № 8 (5). P. 737–752. https://doi.org/10.3390/math8050737

13. Fisac J., Sastry S. The Pursuit-Evasion-Defense Differential Game in Dynamic Constrained Environments // IEEE 54th Annual Conference on Decision and Control (CDC). 2015. P. 4549–4556. https://doi.org/10.1109/cdc.2015.7402930

14. Chandler D. Introduction to Modern Statistical Mechanics : Monograph. University of California, Berkley, 1987. 286 p. URL: https://de.scribd.com/document/438766762/David-Chandler-Introduction-to-modern-statistical-mechanics-Oxford-University-Press-1987-pdf (last accessed: 01.10.2024).

15. Jackson D. Classical Electrodynamics : Monograph. 3rd ed. Published by Wiley-VCH, 1998. 833 p. URL: https://ru.scribd.com/doc/48520397/Jackson-Classical-Electrodynamics-3rd-edition (last accessed: 20.08.2024).

16. Basar T., Olsder G. Dynamic Noncooperative Game Theory : Monograph. Published by Society for Industrial and Applied Mathematics, 1999. 519 p. URL: https://epubs.siam.org/doi/book/10.1137/1.9781611971132 (last accessed: 29.09.2024).

17. Kleinrock L. Queueing Systems. Volume 2: Computer Applications : Monograph. Published by Wiley-Interscience, New York, 1976. 549 p. https://doi.org/10.1002/net.3230070308

18. Bracken M. Lanchester Models of the Ardennes Campaign // Naval Research Logistics. 1995. № 42 (4). P. 559–577. https://doi.org/10.1002/1520-6750(199506)42:4<559::AID-NAV3220420405>3.0.CO;2-R

Стаття надійшла до редакції 10.11.2024.

REFERENCES

1. Shynkaruk, O., & Mykhailyshyn, O. (2019). Okremi aspekty zastosuvannia imitatsiinoho modeliuvannia u pidhotovtsi skladovykh sektoru bezpeky i oborony Ukrainy [Some Aspects of Simulation Modeling Usage in the Training of the Components in the Security and Defense Sector of Ukraine]. *Zb. nauk. prats Nats. akademii Derzh. prykordon. sluzhby Ukrainy [Collection of Scientific Works of the National Academy of the State Border Service of Ukraine]*, *80* (2), 227–241 https://doi.org/10.32453/3.v80i2.201 [in Ukrainian].
2. Kim, B., Kang, B., Choi ,S., & Rim, T. (2017). Data Modeling Versus Simulation Modeling in the Big Data era: Case Study of a Greenhouse Control System *SAGE Publications, 93* (7), 579–594. https://doi.org/10.1177%2F0037549717692866
3. Blake, J. (2019). *Uncertainty and Error in Combat Modeling, Simulation, and Analysis: Dissertation for Philosophiae Doctor*. USA. Retrieved from https://apps.dtic.mil/sti/trecms/pdf/AD1089578.pdf
4. Zhang, B., Wang, Q., Wang, X., & Liang, Y. (2019). Research on Application Method of 3D Digital Simulation Technology in Spacecraft Assembly. *Lecture Notes in Electrical Engineering Signal and Information Processing, Networking and Computers, 550*, 400-409. https://doi.org/10.1007/978-981-13-7123-3_47
5. Hatledal, L. (2021). *Protocols and Standard for Simulation Co-Simulation – For Demanding Maritime Operations: Dissertation for Philosophiae Doctor 03.2021*. Trondheim. Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2755142
6. Nidhra, S., & Dondeti, J. (2012). Black Box and White Box Testing Techniques: a literature review. *International Journal of Embedded Systems and Applications (IJESA), 2* (2), 29–50. http://dx.doi.org/10.5121/ijesa.2012.2204
7. Kasaie, P., Sohn, H., & Kendall, E. et al. (2017). Exploring the Epidemiological Impact of Universal Access to Rapid Tuberculosis Diagnosis Using Agent-Based Simulation. *Winter Simulation Conference (WSC)*, 1097–1108. https://doi.org/10.1109/WSC.2017.8247858
8. Banerjee, D., Saxena, A., & Hashmi, M. et al. (2019). A Compact Dual-Band Impedance Matching Network Based on All-Pass Coupled Lines. In *IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, 937–939. https://doi.org/10.1109/MWSCAS.2018.8623957
9. Kovtun, V. (2023). Matematychni modeli viiny na osnovi rivniannia Lanchestera: vypuskna kvalifikatsiina robota bakalavra. Spets. 113 Prykladna matematyka [Mathematical Models of War Based on the Lanchester Equation: Bachelor's Final Qualifying Work. Specialization 113 Applied Mathematics.]. Kyiv. Retrieved from https://ir.library.knu.ua/handle/123456789/5757 [in Ukrainian].
10. Tolk, A. (2012). Engineering Principles of Combat Modeling and Distributed Simulation: Monograph. New Jersey. https://doi.org/10.1002/9781118180310.fmatter
11. Mikayılov, T., & Bayramov, A. (2020). Principles of Using the Mathematical Models of Combat Activities and Means of Destructions During Operational Preparation of the Troops. *Suchasni informatsiini systemy [Modern Information Systems]*, *4* (1), 24–27. https://doi.org/10.20998/2522-9052.2020.1.04
12. Kress, M. (2020). Lanchester Models for Irregular Warfare. *Mathematics, 8* (5), 737–752. https://doi.org/10.3390/math8050737

13. Fisac, J., & Sastry, S. (2015). The Pursuit-Evasion-Defense Differential Game in Dynamic Constrained Environments. In *IEEE 54th Annual Conference on Decision and Control (CDC).* (pp. 4549–4556). https://doi.org/10.1109/cdc.2015.7402930
14. Chandler, D. (1987). *Introduction to Modern Statistical Mechanics: Monograph.* University of California, Berkley. Retrieved from https://de.scribd.com/document/438766762/David-Chandler-Introduction-to-modern-statistical-mechanics-Oxford-University-Press-1987-pdf
15. Jackson, D. (1998). *Classical Electrodynamics: Monograph.* 3rd ed. Published by Wiley-VCH. Retrieved from https://ru.scribd.com/doc/48520397/Jackson-Classical-Electrodynamics-3rd-edition.
16. Basar, T., & Olsder, G. (1999). *Dynamic Noncooperative Game Theory: Monograph*. Published by Society for Industrial and Applied Mathematics. Retrieved from https://epubs.siam.org/doi/book/10.1137/1.9781611971132
17. Kleinrock, L. (1976). *Queueing Systems. Vol. 2: Computer Applications: Monograph*. Published by Wiley-Interscience, New York. https://doi.org/10.1002/net.3230070308
18. Bracken, M. (1995). Lanchester Models of the Ardennes Campaign. *Naval Research Logistics, 42* (4), 559–577. https://doi.org/10.1002/1520-6750(199506)42:4<559::AID-NAV3220420405>3.0.CO;2-R

S. H. Trutniev

SOURCES OF ERRORS WHEN CALCULATING MATHEMATICAL MODELS OF COMBAT ACTIONS IN COMPUTER SIMULATION SYSTEMS

Currently, there are many situations when practically conducting a scientific experiment or recreating this or that situation in order to make an informed decision is impossible or requires significant financial costs. In such cases, computer simulation systems always come to the rescue, which have been used for a long time to make decisions affecting human lives, planning military operations, directions for the development of the types of the Armed Forces and industries, and even the prospects of state formation. But specialists in the relevant fields, based on the results of computer calculations with the representation of numbers in binary floating-point code, do not take into account the peculiarities of the accuracy of calculations in a computer with binary numbers and the influence of binary arithmetic on the results of simulation modeling. As a rule, the mathematical results of computer calculations are considered to be reliable, although they may contain an error that depends on the hardware of the electronic computing machine, namely on the bit rate of the processor bus. This is due to the IEEE 754 technical standard for floating-point arithmetic.

In the article, the authors analyzed the mathematical models used in combat simulation systems and approaches to their solution. The representation of binary floating-point numbers in computer systems of different bit sizes has been detailed, and possible sources of errors when numbers are represented in binary code have been determined, as well as mathematical calculations. This approach allows you to take into account possible error limits at the stage of entering data into computer systems for calculation, as well as directly when performing mathematical calculations in electronic computing systems.

Keywords: *floating-point representation; mathematical model; combat simulation system; computer architecture; modeling errors; rounding errors; precision range of numbers; IEEE 754 standard.*

ISSN 2076-1546
УДК 681.518 DOI: 10.46972/2076-1546.2024.27.04

І. В. Зімчук, Т. М. Шапар, М. В. Ковба

АЛГОРИТМ ФІЛЬТРАЦІЇ ВИМІРЮВАНЬ АКСЕЛЕРОМЕТРИЧНИХ ДАТЧИКІВ У БЕЗПЛАТФОРМЕНИХ ІНЕРЦІАЛЬНИХ СИСТЕМАХ НАВІГАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У безпілотних літальних апаратах малої маси набули широкого застосування безплатформені інерціальні системи навігації, які реалізуються на базі акселерометрів та гіроскопів, виготовлених за технологією мікроелектромеханічних систем. Низька точність мікроелектромеханічних систем обумовлює застосування в системах навігації додаткових етапів оброблення навігаційних вимірювань. Для підвищення точності навігаційних визначень застосовують алгоритми стохастичної фільтрації, зокрема фільтр Калмана та різні його модифікації. Сучасні алгоритми фільтрації характеризуються високою обчислювальною складністю, а інженери стикаються з проблемою їх практичної реалізації через абстрактну форму подання, яка не відображає усіх деталей. Саме тому актуальним є завдання синтезу алгоритмів фільтрації, які будуть відповідати вимогам гарантованої збіжності процесу фільтрації та мінімальної обчислювальної складності щодо своєї реалізації. Остання вимога є надзвичайно важливою для навігаційних систем малих безпілотних літальних апаратів, оскільки їх бортове обладнання має бути дешевим та малоенергоємним. У зв'язку із цим статтю присвячено синтезу та дослідженню алгоритму поліноміальної фільтрації вимірювань акселерометричних датчиків у безплатформених інерціальних системах навігації безпілотних літальних апаратів. Синтез алгоритму виконано за методикою, що ґрунтується на поданні згладжувальних фільтрів як динамічних систем, що описуються дискретними передавальними функціями, які визначаються застосуванням третьої форми умов інваріантності. Відмінною рисою синтезованого алгоритму є урахування в процесі фільтрації не лише поточних, а й попередніх результатів вимірювань, які зважуються власними коефіцієнтами згладжування. Для розробленого алгоритму визначено умови збіжності процесу фільтрації. Завдяки скалярній формі реалізації йому притаманна низька обчислювальна складність. Ефективність алгоритму підтверджено результатами комп'ютерного моделювання за результатами реальних вимірів акселерометра ADXL345, що входить до складу Arduino UNO R3.

Ключові слова: *згладжувальний фільтр; оцінка; вимірювання; безпілотний літальний апарат; акселерометр; система навігації; алгоритм фільтрації.*

Постановка проблеми в загальному вигляді. В останні роки сфера застосування безпілотних літальних апаратів (БпЛА) значно розширилася, відкриваючи нові можливості для різних галузей [1]. Досвід практичного застосування БпЛА в різних країнах свідчить, що військові завдання, які вирішуються з їх застосуванням, порівняно із цивільними, є більш складними та важливими. Саме тому основні тенденції їх сучасного

© І. В. Зімчук, Т. М. Шапар, М. В. Ковба, 2024

та перспективного розвитку пов'язують передусім із військовим призначенням [2, 3].

Виконання поставлених перед БпЛА завдань як в автоматичному, так і в напівавтоматичному режимах польоту потребує наявності інформації про кутову орієнтацію та координати його місцеперебування. Ця задача розв'язується пілотажно-навігаційним комплексом, основу якого складають інерціальна та супутникова навігаційні системи (ІНС та СНС), які, як правило, працюють одночасно та доповнюють одна одну [4].

Висока точність навігаційних вимірювань обумовлює застосування СНС як основної, проте недостатня відповідність вимогам завадозахищеності та надійності певною мірою ускладнює це. ІНС є менш точною, однак більш досконалою щодо автономності й надійності навігаційних визначень. Висока інформативність ІНС висуває її в клас універсальних систем із визначення як траєкторних рухів БпЛА (координат та швидкості польоту), так і кутових координат (кутів крену, тангажа й курсу) та інших параметрів, наприклад, прискорень, кутових швидкостей тощо [5]. Точність вимірювання цих параметрів визначає величину відхилення БпЛА від заданого маршруту та якість виконання поставленого польотного завдання [5].

У БпЛА малої маси широкого застосування набули безплатформені ІНС (БІНС), які реалізовані на базі акселерометрів і гіроскопів, виконаних за технологією мікроелектромеханічних систем (МЕМС), основними перевагами яких є малі габарити й вага, висока завадозахищеність, надійність та автономність. Жоден із вказаних датчиків не вимірює кутового положення БпЛА безпосередньо, проте виміри цих сенсорів використовуються для його розрахунку. Однак, унаслідок дрейфу нуля, у кожного гіроскопа є постійна похибка вимірювань, інтегрування якої спричиняє похибку розрахунків. Крім того, через конструктивні особливості в сигналі цифрового гіроскопа наявний шум, інтегрування якого спричиняє зашумленість результатів розрахунків. Отже, гіроскоп дозволяє розраховувати лише відносне значення кута, яке потребує корекції дрейфу та фільтрації.

Функціонування акселерометра ґрунтується на інших фізичних принципах. Він вимірює проєкції прискорення об'єкта за трьома координатами. Це дає можливість визначати абсолютні значення кутів орієнтації в будь-який момент часу шляхом розрахунку арктангенса для пар проєкцій [6]. Однак у складі вимірів акселерометра наявний адитивний шум, спричинений особливостями конструкції та умовами функціонування, яким властиві стохастичні чинники, пов'язані із середовищем експлуатації: небажані механічні вібрації, електромагнітні перешкоди від інших електромеханічних або механічних елементів тощо. При цьому показник шуму може досягати 0,08 g, що суттєво погіршує якість вимірювань і, як наслідок, не дає можливості використати отримані дані для управління БпЛА. Під час використання акселерометрів одним з основних є питання результативності, репрезентативності та надійності виміряних величин. Тому для зменшення рівня перешкод, які приховують релевантну інформацію, використовують додаткові етапи перетворення та оброблення сигналу, який отримується [7–9].

Аналіз останніх досліджень і публікацій. Класичним способом боротьби з похибками, завадами та помилками в засобах вимірювання й системах автоматизації

є використання різних алгоритмів фільтрації, які враховують відомі властивості сигналів і завад [9]. Досить часто для усунення шуму та похибок акселерометричних датчиків застосовують фільтр Калмана [9], який дозволяє отримати оптимальну в середньоквадратичному сенсі оцінку вектора стану для опису динамічних систем лінійними диференціальними або різницевими рівняннями за лінійними вимірами за умови гаусівського характеру формуючих та вимірювальних шумів [10]. Фільтр Калмана є зручною рекурентною процедурою, що забезпечує отримання не лише самої оцінки, а й відповідної поточної характеристики точності у вигляді розрахункової матриці коваріацій помилок оцінювання. Однак такий алгоритм фільтрації вимагає значних обчислювальних потужностей для своєї реалізації. Крім того, якість роботи фільтра залежить від точності математичної моделі динамічної системи, ускладнення якої передбачає врахування нелінійних елементів, що, у свою чергу, може значно збільшити розрахункову складність.

Традиційний підхід до побудови алгоритмів калманівського типу, які враховують нелінійності, ґрунтується на лінеаризації рівнянь динаміки та вимірюваннях у визначеній точці шляхом розрахунку похідних від відповідних нелінійних функцій. Одним із таких рішень є розширений фільтр Калмана (Extended Kalman Filter – EKF) з різною кількістю змінних стану [11, 12]. Синтез таких алгоритмів фільтрації ґрунтується на лінеаризації нелінійних моделей стану шляхом розкладання їх у ряд Тейлора.

Наступна група алгоритмів калманівського типу – так звані ансцентні (unscented), або сигма-точкові фільтри Калмана (Unscented Kalman Filter – UKF) [13, 14]. У них лінеаризація нелінійних функцій відбувається без розрахунку похідних застосуванням процедури, близької за своїм змістом, до стохастичної лінеаризації. Від розширеного фільтра Калмана такий підхід відрізняється лише способом лінеаризації моделей стану та спостереження.

Розглянуті алгоритми фільтрації належать до алгоритмів калманівського типу і є досить універсальними щодо їх практичного застосування, однак характеризуються високою складністю, бо інженери часто стикаються з проблемою їх практичної реалізації через абстрактну форму опису, яка не відображає усіх деталей.

Альтернативним підходом до розв’язання задачі фільтрації параметрів орієнтації в ІНС є фільтр Маджвіка [15, 16], який обчислює єдину оцінку орієнтації на основі вимірювань акселерометра та гіроскопа. На відміну від алгоритмів калманівського типу задача мінімізації помилок оцінювання вирішується завдяки алгоритму градієнтного спуску, при цьому пошук мінімуму реалізується лише в одну його ітерацію. Для опису орієнтації об’єкта в просторі фільтр використовує кватерніони, що передбачає застосування одного надлишкового параметра і не є наочним для прямого розуміння користувачем. Крім того, алгоритм не є універсальним і був спроєктований під умови конкретної задачі.

Найпростішим варіантом фільтра, здатним розв’язувати задачу фільтрації вимірювань в ІНС, є комплементарний фільтр [16]. Його робота ґрунтується на змішуванні вимірювань акселерометра та гіроскопа у визначеній пропорції для отримання необхідного результату. Інтегрування сигналу гіроскопа робить його менш схильним до шуму, а змішування із сигналом акселерометра дозволяє уникнути дрейфу. Незважаючи

на простоту реалізації алгоритму, точність вихідних значень фільтра нижча, ніж у розглянутих алгоритмів. Крім того, налаштування коефіцієнта згладжування комплементарного фільтра передбачено лише експериментальним шляхом.

Досить часто завдання оцінювання спрощують шляхом обмеження класу алгоритмів, у межах якого здійснюється їх вибір, наприклад, у класі лінійних алгоритмів [14]. Незважаючи на те, що на теперішний час запропоновано досить велику кількість різноманітних алгоритмів фільтрації, завдання їх розроблення залишається актуальним.

Формулювання завдання дослідження. Метою статті є синтез рекурентного алгоритму поліноміальної фільтрації результатів вимірювань акселерометричних датчиків орієнтації в БІНС БпЛА. Він повинен задовольняти вимоги гарантованої збіжності процесу фільтрації та мінімальної обчислювальної складності щодо своєї реалізації. Остання вимога є надзвичайно актуальною в навігаційних системах малих БпЛА, оскільки їх бортове обладнання має бути дешевим, малоенергоємним та з мінімальними масою й об’ємом [4].

Виклад основного матеріалу

Математична постановка задачі. Оскільки обробка навігаційних вимірювань здійснюється цифровими пристроями, у ході розв’язання задачі розглядаються математичні моделі процесів у дискретній формі. Припустимо, що вимірювання акселерометричного датчика описуються рівнянням

$$g(n) = x(n) + f(n), \tag{1}$$

де $x(n)$ – істинне значення інформаційного параметра, подане лінійною моделлю такого виду:

$$x(n) = x(n-1) + \sum_{m=1}^{N} \frac{T^m}{m!} \Delta^m x(n-1), \tag{2}$$

тут $\Delta^m x(n-1)$ – кінцева різниця m-го порядку;

N – порядок моделі;

T – темп обробки інформації;

$n = 0, 1, 2, \ldots$ – нормований відносно інтервалу дискретизації дискретний час;

$f(n)$ – адитивний білий шум із нульовим середнім та дисперсією $R(n) = M\left[f^2(n)\right]$, причому

$$M\left[x(n) f(n)\right] = 0,\ M\left[f(n) f(n-1)\right] = 0,\ i > 0, \tag{3}$$

де M – символ математичного сподівання.

Для дискретного процесу (1) з урахуванням умов (2) та (3) необхідно синтезувати алгоритм фільтрації, який формує оцінку $\hat{x}(n)$, оптимальну за критерієм мінімум дисперсії помилок оцінювання:

$$P(n) = M\left[\varepsilon^2(n)\right] \to \min, \tag{4}$$

де $\varepsilon(n) = x(n) - \hat{x}(n)$ – помилка оцінювання.

Синтез алгоритму фільтрації. У разі розроблення ефективних алгоритмів для розв'язання прикладних задач фільтрації необхідно брати до уваги їх особливості. Зокрема, активно розвиваються методи поліноміальної фільтрації, у яких враховується той факт, що вимірювання навігаційних параметрів є одновимірним потоком даних [10]. Для таких умов у [17] викладено метод, який дозволяє синтезувати рекурентні згладжувальні фільтри для скалярних моделей вхідних дій і дає можливість формувати структуру алгоритмів фільтрації залежно від забезпечення необхідної якості фільтрації в сталому режимі (рис. 1).

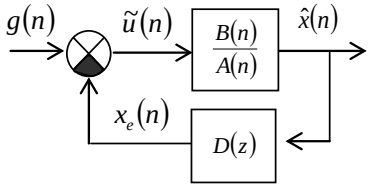


Рис. 1. Структурна схема рекурентного фільтра

На рис. 1 позначено:

$x(n)$ – екстрапольоване значення інформаційного параметра;

$\tilde{u}(n)$ – нев'язка;

$A(z)$ – поліном знаменника передавальної функції алгоритму оцінювання, загальний вигляд якого визначається виразом

$$A(z) = \left(1 - z^{-1}\right)^{\nu}\left[1 + \sum_{i=1}^{k} a_i z^{-i}\right], \tag{5}$$

де $\nu = N + 1$ – порядок астатизму фільтра;

a_i – коефіцієнти полінома, фізичний зміст яких полягає в підвищенні порядку астатизму фільтра до такого значення γ, що $\nu \le \gamma \le \nu + 1$;

$B(z)$ – поліном чисельника передавальної функції алгоритму оцінювання, загальний вигляд якого визначається за таким виразом:

$$B(z) = \sum_{j=0}^{l} b_i z^{-j}, \tag{6}$$

тут b_j – коефіцієнти згладжування, оптимальні значення яких можуть розраховуватися з виразу

$$\frac{\partial P}{\partial b_j} = 0, \tag{7}$$

де $D(z)$ – екстраполюючий поліном, який розраховується в такий спосіб:

$$D(z)=1-A(z). \tag{8}$$

Згідно з методом [17] алгоритм фільтрації синтезується за виразами:

$$\begin{aligned} x_e(n)&=D(z)\hat{x}(n),\\ \tilde{u}(n)&=g(n)-x_e(n),\\ \hat{x}(n)&=\frac{B(z)}{A(z)}\tilde{u}(n). \end{aligned} \tag{9}$$

Для розв'язання поставленої задачі з метою усунення динамічної помилки за $N=1$ згладжувальний фільтр синтезується другого порядку астатизму, тому поліном $A(z)$ достатньо визначити [17] як

$$A(z)=\left(1-z^{-1}\right)^2.$$

Тоді згідно з (8) екстраполюючий поліном матиме такий вигляд:

$$D(z)=2z^{-1}-z^{-2}.$$

Відповідно до (6) для забезпечення якісної фільтрації збурень поліном $B(z)$ визначається в такий спосіб:

$$B(z)=b_0+b_1z^{-1}+b_2z^{-2}.$$

Для визначених поліномів $A(z)$, $B(z)$ та $D(z)$ за виразами (9) синтезується алгоритм фільтрації:

$$\begin{aligned} x_e(n)&=2\hat{x}(n-1)-\hat{x}(n-2),\\ \tilde{u}(n)&=g(n)-x_e(n),\\ \hat{x}(n)&=b_0\tilde{u}(n)+b_1\tilde{u}(n-1)+b_2\tilde{u}(n-2)+x_e(n). \end{aligned} \tag{10}$$

Для визначення умов збіжності процесу фільтрації [17] з виразу

$$C(z)=A(z)+B(z)D(z)$$

розраховується характеристичний поліном

$$C(z)=1-2(1-b_0)z^{-1}+(1-b_0+2b_1)z^{-2}-(b_1-2b_2)z^{-3}-b_2z^{-4},$$

а за алгебричним критерієм стійкості визначаються умови стійкості фільтра:

$$0 < b_0 \le 1,\ b_1 < 0,\ b_2 < 0,\ |b_2| < |b_1| < |b_0|.$$

Результати моделювання. Ефективність синтезованого алгоритму оцінювали з використанням комп'ютерного моделювання. Розроблено імітаційну модель, яка дозволяє шляхом виконання послідовності обчислень із подальшим графічним відображенням результатів імітувати процес фільтрації вхідних сигналів у реальному часі. Досліджували також процес фільтрації кута крену БпЛА (рис. 2), який визначали за результатами вимірювань триосьового акселерометра ADXL345, що входить до складу Arduino UNO R3. У сталому режимі вихідним значенням кута властива дисперсія $D_g = 0{,}96$ кВ. град.

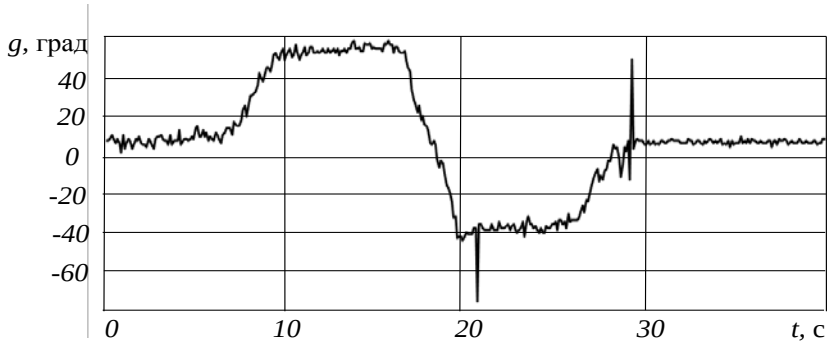


Рис. 2. Зміна кута крену БпЛА, який визначено за результатами вимірювань акселерометра

Вимірювання оброблялися з періодом $T = 0{,}1$ с. Значення коефіцієнтів згладжування обирали з нижньої межі області стійкості: $b_0 = 0{,}15$; $b_1 = -0{,}07$; $b_2 = -0{,}05$. На рис. 3 показано результат фільтрації вимірювань із застосуванням синтезованого алгоритму.

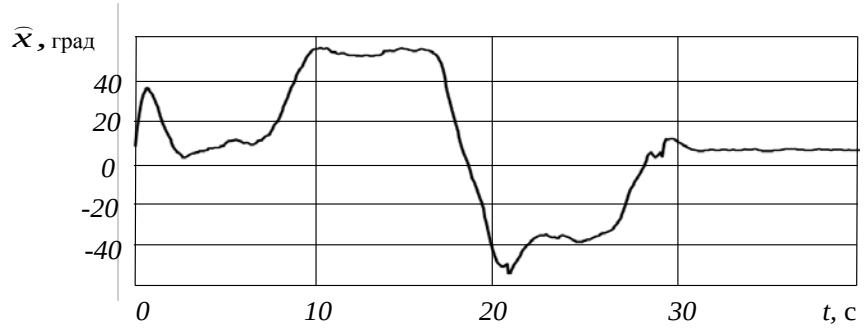


Рис. 3. Результат фільтрації кута крену БпЛА в разі застосування синтезованого алгоритму

Ефективність алгоритму оцінювали за дисперсією D_x оцінки кута крену. Для обраних умов моделювання синтезований алгоритм забезпечив значення дисперсії $D_x = 0{,}12$ кВ. град. У процесі моделювання також визначено, що для $b_2 = 0$ дисперсія оцінки набуває значення $D_x = 0{,}41$ кВ. град., що свідчить про вплив коефіцієнтів полінома $B(z)$ на якість фільтрації.

Отримані результати порівнювали з результатами роботи фільтра Калмана (рис. 3), налаштованого на модель для $N = 1$ [18].

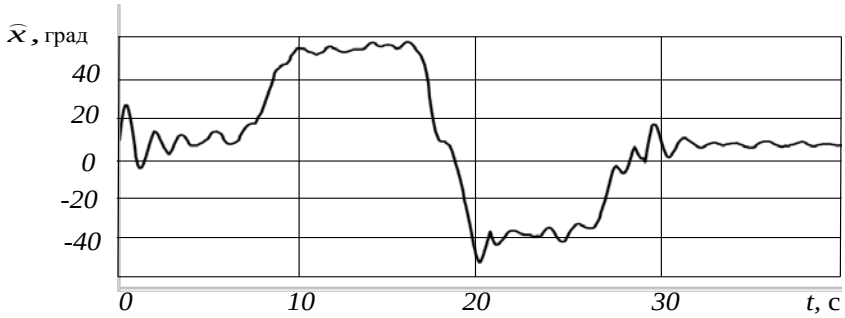


Рис. 4. Результат фільтрації кута крену БпЛА в разі застосування фільтра Калмана

Для фільтра Калмана показник ефективності набув значення $D_x = 0{,}59$ кВ. град. Отже, порівняно з ним у синтезованому алгоритмі з коефіцієнтами згладжування b_0, b_1 та b_2 дисперсія оцінки в 4,9 рази менше.

Слід зазначити, що коефіцієнти згладжування синтезованого фільтра обиралися виключно з нижньої межі умов стійкості. Розрахунок оптимальних значень коефіцієнтів у роботі не розглядався.

Висновки. Застосування алгоритмів фільтрації вимірювань у системах навігації БпЛА є невід'ємним етапом процесу визначення параметрів руху. Саме тому для підвищення точності визначення кутового положення БпЛА у статті синтезовано та досліджено алгоритм фільтрації результатів вимірювань акселерометричних датчиків, які входять до складу БІНС. Синтез алгоритму виконано за методикою, яка ґрунтується на поданні згладжувальних фільтрів як динамічних систем, описаних дискретними передавальними функціями, які визначають за третьою формою умов інваріантності. Відмінною рисою синтезованого алгоритму є застосування для оцінювання як поточних, так і попередніх значень нев'язок, кожна з яких зважується власним коефіцієнтом згладжування. Як показали результати комп'ютерного моделювання, такий підхід дозволив значно покращити якість фільтрації випадкового шуму, який наявний у вимірах акселерометричних датчиків орієнтації.

За напрямок подальших досліджень слід вважати удосконалення синтезованого алгоритму шляхом оптимізації перехідного процесу та розрахунку оптимальних значень коефіцієнтів згладжування.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Апаратно-програмне забезпечення та застосування безпілотних літальних апаратів / Я. Савченко, С. Ягодзінський, Л. Литвиненко, О. Сушинський // Вісник Хмельницького нац. ун-ту. 2024. № 3, Т. 2. С. 273–277. https://doi.org/10.31891/2307-5732-2024-337-3-41

2. Розвиток безпілотної авіації у світі та Україні: аналіз особливостей та технічних характеристик / Ю. О. Бабій, В. В. Поліщук, М. О. Мацишин та ін. // Зб. наук. праць Військ. ін-ту Київського нац. ун-ту ім. Тараса Шевченка. 2022. № 75. С. 5–14. https://doi.org/10.17721/2519-481X/2022/75-01

3. Серватюк В., Лисий М., Мостовий А. Аналіз наукових підходів щодо розвитку і застосування безпілотних літальних апаратів у сучасних воєнних конфліктах // Зб. наук. праць Нац. академії Держ. прикордонної служби України. Серія: Військові та технічні науки. 2024. № 1 (94). С. 97–105.
4. Авіоніка безпілотних літальних апаратів / В. П. Харченко, В. І. Чепіженко, А. А. Тунік, С. В. Павлова. Київ : ТОВ «Абрис-принт», 2012. 464 с. ISBN: 978-966-1653-05-3
5. Захарін Ф. М., Синєглазов В. М., Філяшкін М. К. Алгоритмічне забезпечення інерціально-супутникових систем навігації : монографія. Київ : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. 320 с. ISBN 978-966-598-675-1
6. Удосконалення навігаційної системи пристрою дефектоскопії підземних труб / М. Мельник, Р. Винарович, Ю. Гасюк, М. Шварц // Комп'ютерні системи проєктування. Теорія і практика. 2024. Вип. 6, № 1. С. 117–126. https://doi.org/10.23939/cds2024.01.117
7. Рудик А. В. Акселерометричні інерціальні мікросистеми орієнтації // Вимірювальна та обчислювальна техніка в технологічних процесах : Матеріали XVII Міжнар. наук.-техн. конф. (8–13 червня 2017 р., м. Одеса). Одеса : Одес. нац. акад. зв'язку ім. О. С. Попова; Хмельницький : ХНУ, 2017. С. 103–105.
8. Шуляк М. Л. Аналіз існуючих систем фільтрації даних при експериментальному дослідженні транспортного засобу // Технічний сервіс агропромислового, лісового та транспортного комплексів. 2020. № 21. С. 175–184. https://doi.org/10.37700/ts.2020.21.175-184
9. Розроблення та дослідження сучасних систем електроенергетики та автоматизації : Монографія / В. В. Древецький , С. В. Василець , А. В. Рудик та ін. Рівне : Овід, 2020. 380 с.
10. Stepanov O. A. Optimal and Sub-Optimal Filtering in Integrated Navigation Systems // Aerospace Navigation Systems. Chichester, UK : John Wiley & Sons Ltd, 2016. P. 244–298. https://doi.org/10.1002/9781119163060.ch8
11. Afshari H. H., Gadsden S. A., Habibi S. Gaussian Filters for Parameter and State Estimation: A General Review of Theory and Recent Trends // Signal Processing. 2017. Vol. 135. P. 218–238. https://doi.org/10.1016/j.sigpro.2017.01.001
12. Guoqiang Mao, Sam Drake, Brian D. O. Anderson. Design of an Extended Kalman Filter for UAV Localization // Conference: Information, Decision and Control. IEEE. 2007. P. 224–229. https://doi.org/10.1109/IDC.2007.374554
13. Covariance Matching Based Adaptive Unscented Kalman Filter for Direct Filtering in INS/GNSS Integration / Yang Meng, Shesheng Gao, Yongmin Zhong et al. // Acta Astronautica. 2016. Vol. 120. P. 171–181. https://doi.org/10.1016/j.actaastro.2015.12.014
14. Crassidis J. L. Sigma-Point Kalman Filtering for Integrated GPS and Inertial Navigation // IEEE Transactions on Aerospace and Electronic Systems. 2006. Vol. 42, No. 2. P. 750–756. https://doi.org/10.1109/taes.2006.1642588
15. Фесенко О. Д. Вдосконалений метод орієнтації безпілотного літального апарата в тривимірному просторі за допомогою мікроелектромеханічних систем інерціальної системи навігації на основі фільтра Маджвіка // Авіаційна та ракетно-космічна техніка. 2018. Т. 29 (68), Ч. 1, № 3. С. 35–42. URL: http://nbuv.gov.ua/UJRN/sntuts_2018_29_3%281%29__9 (дата звернення: 10.09.2024).
16. Бугайов Д. В., Аврутов В. В., Нестеренко О. І. Експериментальне порівняння алгоритмів визначення орієнтації на базі компліментарного фільтра та фільтра Маджвіка //

Автоматизація технологічних і бізнес-процесів. 2020. Vol. 12, Iss. 3. P. 9–18. https://doi.org/10.15673/atbp.v12i3.1855
17. Зімчук І. В., Шапар Т. М., Ковба М. В. Синтез алгоритмів фільтрації результатів вимірювань у системах навігації безпілотних літальних апаратів // Вісник НТУУ "КПІ". Серія Радіотехніка, Радіоапаратобудування. 2024. Вип. 96. С. 21–27. https://doi.org/10.20535/RADAP.2024.96.21-27
18. Кожешкурт В. І., Юзефович В. В. Дослідження схем фільтрації алгоритмів трасової обробки // Реєстрація, зберігання і обробка даних. 2010. Т. 12, № 4. С. 3–12. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50481/01-Kozheshkurt.pdf?sequence=1 (дата звернення: 21.10.2024).

Стаття надійшла до редакції 12.11.2024.

REFERENCES

1. Savchenko, Ya., Yahodzinskyi, S., Lytvynenko, L., & Sushynskyi, O. (2024). Aparatno-prohramne zabezpechennia ta zastosuvannia bezpilotnykh litalnykh aparativ [Hardware and Software Support and Application of Unmanned Aerial Vehicles]. *Visnyk Khmelnytskoho nats.un-tu [Bulletin of Khmelnytsky National University], № 3,* Iss. 2, 273–277. https://doi.org/10.31891/2307-5732-2024-337-3-41 [in Ukrainian].
2. Babii, Yu. O., Polishchuk, V. V., & Matsyshyn, M. O. et al. (2022). Rozvytok bezpilotnoi aviatsii u sviti ta Ukraini: analiz osoblyvostei ta tekhnichnykh kharakterystyk [Development of Unmanned Aviation in the World and Ukraine: Analysis of Features and Technical Characteristics]. *Zb. nauk. prats Viisk. in-tu Kyivskoho nats. un-tu im. Tarasa Shevchenka [Collection of Scientific Works of the Military Institute of the Taras Shevchenko National University of Kyiv], 75,* 5–14. https://doi.org/10.17721/2519-481X/2022/75-01 [in Ukrainian].
3. Servatiuk, V., Lysyi, M., & Mostovyi, A. (2024). Analiz naukovykh pidkhodiv shchodo rozvytku i zastosuvannia bezpilotnykh litalnykh aparativ u suchasnykh voiennykh konfliktakh [Analysis of scientific approaches to the development and use of unmanned aerial vehicles in modern military conflicts]. *Zb. nauk. prats Nats. akademii Derzh. prykordonnoi sluzhby Ukrainy. Seriia: Viiskovi ta tekhnichni nauky [Collection of Scientific Works of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences], 1* (94), 97–105. [in Ukrainian].
4. Kharchenko, V. P., Chepizhenko, V. I., Tunik, A. A., & Pavlova, S. V. (2012). *Avionika bezpilotnykh litalnykh aparativ [Avionics of unmanned aerial vehicles]*. Kyiv. ISBN: 978-966-1653-05-3 [in Ukrainian].
5. Zakharin, F. M., Syniehlazov, V. M., & Filiashkin, M. K. (2011). *Alhorytmichne zabezpechennia inertsialno-suputnykovykh system navihatsii: monohrafiia [Algorithmic Support of Inertial-Satellite Navigation Systems: Monograph]*. Kyiv. ISBN 978-966-598-675-1 [in Ukrainian].
6. Melnyk, M., Vynarovych, R., Hasiuk, Yu., & Shvarts, M. (2024). Udoskonalennia navihatsiinoi systemy prystroiu defektoskopii pidzemnykh trub [Improvement of the Navigation System of the Underground Pipe Flaw Detection Device]. *Komp'iuterni systemy proiektuvannia. Teoriia i praktyka [Computer Design Systems. Theory and Practice], Iss. 6,* № 1, 117–126. https://doi.org/10.23939/cds2024.01.117 [in Ukrainian].

7. Rudyk, A. V. (2017). Akselerometrychni inertsialni mikrosystemy oriientatsii [Accelerometric Inertial Orientation Microsystems]. In *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh : Materialy XVII Mizhnar. nauk.-tekhn. konf. [Measuring and Computing Equipment in Technological Processes: Proceedings of the XVII International Scientific-Technical Conference]*. Odesa, June 8–13, 2017. (pp. 103–105). Odesa; Khmelnytskyi [in Ukrainian].
8. Shuliak, M. L. (2020). Analiz isnuiuchykh system filtratsii danykh pry eksperymentalnomu doslidzhenni transportnoho zasobu [Analysis of Existing Data Filtering Systems During Experimental Research of a Vehicle]. *Tekhnichnyi servis ahropromyslovoho, lisovoho ta transportnoho kompleksiv [Technical Service of Agro-Industrial, Forestry and Transport Complexes], 21*, 175–184. https://doi.org/10.37700/ts.2020.21.175-184 [in Ukrainian].
9. Drevetskyi, V. V., Vasylets, S. V., & Rudyk, A. V. et al. (2020). *Rozroblennia ta doslidzhennia suchasnykh system elektroenerhetyky ta avtomatyzatsii: Monohrafiia [Development and Research of Modern Power and Automation Systems: Monograph]*. Rivne [in Ukrainian].
10. Stepanov, O. A. (2016). Optimal and Sub-Optimal Filtering in Integrated Navigation Systems. *Aerospace Navigation Systems, 244–298.* Chichester, UK. https://doi.org/10.1002/9781119163060.ch8
11. Afshari, H. H., Gadsden, S. A., & Habibi, S. (2017). Gaussian Filters for Parameter and State Estimation: A General Review of Theory and Recent Trends. *Signal Processing, 135*, 218–238. https://doi.org/10.1016/j.sigpro.2017.01.001
12. Guoqiang Mao, Sam Drake, Brian D. O. Anderson. (2007). Design of an Extended Kalman Filter for UAV Localization. In *Conference: Information, Decision and Control. IEEE*. (pp. 224–229). https://doi.org/10.1109/IDC.2007.374554
13. Yang Meng, Shesheng Gao, & Yongmin Zhong et al. (2016). Covariance Matching Based Adaptive Unscented Kalman Filter for Direct Filtering in INS/GNSS Integration. *Acta Astronautica, 120*, 171–181. https://doi.org/10.1016/j.actaastro.2015.12.014
14. Crassidis, J. L. (2006). Sigma-Point Kalman Filtering for Integrated GPS and Inertial Navigation. *IEEE Transactions on Aerospace and Electronic Systems, Vol. 42*, Iss. 2, 750–756. https://doi.org/10.1109/taes.2006.1642588
15. Fesenko, O. D. (2018). Vdoskonalenyi metod oriientatsii bezpilotnoho litalnoho aparata v tryvymirnomu prostori za dopomohoiu mikroelektromekhanichnykh system inertsialnoi systemy navihatsii na osnovi filtra Madzhvika [Improved Method of Orientation of Unmanned Aerial Vehicle in Three-Dimensional Space Using Microelectromechanical Systems and Inertial Navigation System Based on the Madzhwick Filter]. *Aviatsiina ta raketno-kosmichna tekhnika [Aviation, Rocket and Space Engineering], 29* (68), Iss. 1, № 3, 35–42. Retrieved from http://nbuv.gov.ua/UJRN/sntuts_2018_29_3%281%29__9 [in Ukrainian].
16. Buhaiov, D. V., Avrutov, V. V., & Nesterenko, O. I. (2020). Eksperymentalne porivniannia alhorytmiv vyznachennia oriientatsii na bazi komplimentarnoho filtra ta filtra Madzhvika [Experimental Comparison of Orientation Determination Algorithms Based on a Complementary Filter and a Madzhwick Filter]. *Avtomatyzatsiia tekhnolohichnykh i biznes-protsesiv [Automation of Technological and Business Processes], Vol. 12,* Iss. 3, 9–18. https://doi.org/10.15673/atbp.v12i3.1855 [in Ukrainian].

17. Zimchuk, I. V., Shapar, T. M., & Kovba, M. V. (2024). Syntez alhorytmiv filtratsii rezultativ vymiriuvan u systemakh navihatsii bezpilotnykh litalnykh aparativ [Synthesis of Algorithms for Filtering Measurement Results in Navigation Systems of Unmanned Aerial Vehicles]. *Visnyk NTUU "KPI". Seriia Radiotekhnika, Radioaparatobuduvannia [Bulletin of NTUU "KPI". Series Radio Engineering, Radio Equipment Manufacturing], 96,* 21–27. https://doi.org/10.20535/RADAP.2024.96.21-27 [in Ukrainian].
18. Kozheshkurt, V. I., & Yuzefovych, V. V. (2010). Doslidzhennia skhem filtratsii alhorytmiv trasovoi obrobky [Research of Filtering Schemes of Route Processing Algorithms]. *Reiestratsiia, zberihannia i obrobka danykh [Registration, Storage and Processing of Data], Vol. 12,* № 4, 3–12. Retrieved from http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50481/01-Kozheshkurt.pdf?sequence=1 [in Ukrainian].

I. V. Zimchuk, T. M. Shapar, M. V. Kovba

FILTERING ALGORITHM OF ACCELEROMETRICAL SENSORS MEASUREMENTS IN PLATFORMLESS INERTIAL NAVIGATION SYSTEMS UNMANNED AIRCRAFT

In unmanned aerial vehicles of low mass, platformless inertial navigation systems are widely used. They are implemented on the basis of accelerometers and gyroscopes, which are made according to the technology of microelectromechanical systems. The low accuracy of microelectromechanical systems determines the use of additional stages of navigation measurement processing in navigation systems.

To increase the accuracy of navigation determinations, stochastic filtering algorithms are used, namely the Kalman filter and its various modifications. Existing filtering algorithms are characterized by high computational complexity due to the abstract form of presentation, which does not reflect the details of implementation. That is why the task of synthesizing filtering algorithms that will meet the requirements of guaranteed convergence of the filtering process and minimal computational complexity regarding its implementation is relevant. This requirement is extremely important for navigation systems of small unmanned aerial vehicles, as their on-board equipment must be cheap and low-energy. The work is devoted to the synthesis and research of the algorithm of polynomial filtering of measurements of accelerometric sensors in platformless inertial navigation systems of unmanned aerial vehicles. The synthesis of the algorithm is performed according to the method based on the presentation of smoothing filters as dynamic systems described by discrete transfer functions, which are determined by the application of the third form of invariance conditions. A distinctive feature of the synthesized algorithm is the consideration in the filtering process of not only current, but also previous measurement results, which are weighted by their own smoothing coefficients. The conditions for the convergence of the filtering process are defined for the synthesized algorithm. Due to the scalar form of the algorithm implementation, low computational complexity is inherent. The effectiveness of the algorithm was confirmed by the results of computer simulation based on the results of real measurements of the ADXL345 accelerometer, which is part of the Arduino UNO R3.

Keywords: *smoothing filter; evaluation; measurement; unmanned aerial vehicle; accelerometer; navigation system; filtering algorithm.*

ISSN 2076-1546
УДК 004.4 DOI: 10.46972/2076-1546.2024.27.05

В. В. Охрімчук, І. А. Охрімчук

АНАЛІЗ ЗАСОБІВ МОДЕЛЮВАННЯ МЕРЕЖ ЩОДО МОЖЛИВОСТІ ЇХ ВИКОРИСТАННЯ ДЛЯ ПРАКТИЧНОЇ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ

Незважаючи на наявні системи інформаційної безпеки, ключовим аспектом ефективного кіберзахисту залишається рівень підготовки персоналу, відповідального за кібербезпеку. Сьогодні підготовка фахівця з кібербезпеки повинна ґрунтуватися на всебічному вивченні сучасних інформаційних технологій, механізмів і шаблонів проведення кібератак, способів протидії їм та включати як теоретичну, так і практичну складові. Встановлено, що найбільш поширеною практикою у провідних навчальних та наукових установах світу й України щодо здійснення практичної підготовки фахівців із кібербезпеки є створення та розгортання складних програмно-апаратних комплексів – кіберполігонів, але це вимагає витрати значних ресурсів. Тому програмні засоби емуляції і симуляції комп'ютерних мереж стають альтернативою отримання початкових практичних навичок із кібербезпеки.

У статті проаналізовано три найпопулярніші безкоштовні інструменти для симуляції та емуляції комп'ютерних мереж: Cisco Packet Tracer, GNS3 і EVE-NG – щодо можливості їх використання для практичної підготовки фахівців із кібербезпеки. У результаті аналізу встановлено, що Cisco Packet Tracer, орієнтований на користувачів-початківців, забезпечує симуляцію мережевих пристроїв виключно компанії Cisco, дозволяє налаштовувати базові протоколи та відпрацьовувати основи кіберзахисту. GNS3 за своїм функціоналом дещо переважає Cisco Packet Tracer, емулює реальні образи операційних систем і підтримує роботу з багатьма вендорами мережевих пристроїв, що робить його корисним для складних навчальних завдань. Крім того, GNS3 надає можливість відтворювати сценарії кібератак, а інтегрований мережевий аналізатор Wireshark дозволяє здійснювати моніторинг трафіку та аналізувати вплив кібератаки на систему. У свою чергу, EVE-NG – потужна платформа для емуляції мереж, яка за своїми функціональними можливостями дуже близька до GNS3. Вона також забезпечує широку підтримку обладнання і надає можливості для розгортання складних мережевих топологій. Проте основною особливістю EVE-NG є її клієнт-серверна архітектура, що дозволяє багатокористувацький формат роботи.

Отже, Cisco Packet Tracer, GNS3 та EVE-NG доповнюють один одного в процесі отримання практичних навичок із кібербезпеки на різних рівнях навчання. Використання всіх трьох інструментів у навчальних програмах дозволить формувати комплексні знання і практичні навички, необхідні для ефективного захисту критичної інформаційної інфраструктури від кібератак.

***Ключові слова**: кібербезпека; кіберзахист; кібератака; емулятор; симулятор; віртуалізація; Cisco; GNS3; EVE-NG.*

© В. В. Охрімчук, І. А. Охрімчук, 2024

Постановка проблеми в загальному вигляді. У сучасному світі, де інформаційні технології інтегровані в усі сфери життя, кібербезпека є ключовим пріоритетом для державних установ, бізнесу та приватних осіб. Такі щоденні кіберзагрози, як: кібератаки на комп'ютерні мережі, викрадення та шифрування даних, а також використання шкідливого програмного забезпечення (ПЗ) – вимагають удосконалення чинних і розроблення новітніх механізмів кіберзахисту. Однак, незважаючи на досягнуті результати фахівців та науковців у галузі кібербезпеки зі створення систем інформаційної безпеки, ключовим аспектом ефективного кіберзахисту залишається рівень підготовки персоналу, відповідального за кібербезпеку.

Сьогодні підготовка фахівця з кібербезпеки повинна ґрунтуватися на всебічному вивченні сучасних інформаційних технологій, механізмів та шаблонів проведення кібератак, способів протидії їм та включати як теоретичну, так і практичну складові.

У світі є достатньо велика кількість установ, що займаються моніторингом, класифікацією та накопиченням відомостей про кіберзагрози. Кожна така організація надає, як правило, відкритий доступ до своїх власних баз кіберзагроз, тому отримання теоретичних знань про них та шляхи їх усунення в сучасному інформаційному суспільстві не є проблемою.

Проте досить гостро постає питання отримання практичних навичок. Передусім це пов'язано із великим різноманіттям топологій комп'ютерних мереж, їх функціональним призначенням, особливостями комутації та маршрутизації в них пакетів, наявністю значної кількості як мережевого, так і кінцевого обладнання з різними операційними системами (ОС) тощо. Тому для відпрацювання практичних питань необхідно створювати мініатюрні моделі реальних комп'ютерних мереж, що з урахуванням викладеного вище є важко реалізовуваним процесом. Інший шлях – використовувати програмні засоби симуляції та емуляції роботи комп'ютерних мереж.

Аналіз останніх досліджень і публікацій. У результаті аналізу доступних джерел [1–6] встановлено, що найбільш поширеною практикою в провідних навчальних і наукових установах світу та України щодо здійснення практичної підготовки фахівців із кібербезпеки є створення й розгортання складних програмно-апаратних комплексів – кіберполігонів. Вони дозволяють проводити наукові дослідження в галузі кібербезпеки, підвищувати ефективність практичної підготовки фахівців із кібербезпеки, відпрацьовувати питання кіберзахисту об'єктів із критичною інформаційною інфраструктурою, а також проводити дво- й багатосторонні навчання та тренування з елементами відпрацювання дій в умовах комплексних кібервпливів.

Незважаючи на всі позитивні внески від кіберполігонів в практичну підготовку фахівців із кібербезпеки, їх створення потребує значних фінансових витрат, а також вимагає наявності висококваліфікованого персоналу для підтримки. Крім того, оскільки кіберполігон, як зазначалося раніше, – це складний програмно-апаратний комплекс, то допуск до практичної роботи на ньому слід здійснювати тільки після отримання базових практичних навичок із забезпечення кібербезпеки. А розгортання таких комплексів для отримання базових практичних навичок є не тільки недоцільним, а й не цільовим. Тому й постає питання, де майбутньому фахівцю отримати первинні практичні навички.

Вирішити цю проблему можливо за допомогою програмних засобів симуляції та емуляції комп'ютерних мереж.

Формулювання завдання дослідження. Сьогодні системні адміністратори, мережеві інженери для отримання практичних навичок із налаштування та адміністрування мереж використовують спеціалізовані програмні засоби емуляції та симуляції роботи комп'ютерних мереж. У світі є достатньо велика кількість вендорів спеціалізованого ПЗ, призначеного для отримання первинних навичок із налаштування мереж та управління ними. Проте далеко не всі вони можуть бути використані для практичного навчання фахівців із кібербезпеки.

Метою статті є аналіз найбільш поширених симуляторів та емуляторів комп'ютерних мереж, оцінювання їх функціональних можливостей, визначення переваг і недоліків, а також встановлення можливості їх використання для отримання первинних практичних навичок із забезпечення кібербезпеки.

Виклад основного матеріалу. Усе спеціалізоване ПЗ, яке використовується для віртуалізації роботи мереж, можна поділити на два типи: симулятори та емулятори [7, 8].

Емулятори – це ПЗ, яке дозволяє імітувати поведінку ОС та обладнання реального пристрою. Вони зазвичай набагато повніші й точніші порівняно із симуляторами, але часто вимагають більше ресурсів комп'ютера. Емулятори використовують для тестування застосунків на різних платформах (наприклад, *Android* на *Windows* або *iOS* на *macOS*). Емулятори можуть бути повільнішими через додатковий шар абстракції, але вони зазвичай надійніші для перевірки реальної взаємодії програм з ОС [8, 9].

Симулятори – це ПЗ, яке також дозволяє імітувати поведінку ОС, але вони, як правило, працюють на вищому рівні – програми. Вони зазвичай менш ресурсоємні, але можуть не забезпечувати 100% точності порівняно з реальними пристроями.

Симулятори частіше використовують для тестування застосунків на різних версіях ОС та роздільних здатностях екрана. Вони зазвичай швидші внаслідок прямішого доступу до ресурсів комп'ютера, але менш точні, оскільки не імітують повністю реальних умов роботи на пристрої [8, 9].

Незважаючи на велике різноманіття наявних на ринку програмних засобів моделювання комп'ютерних мереж, для порівняльного аналізу ми обрали найбільш популярні на сьогодні безкоштовні симулятори та емулятори: *Cisco Packet Tracer, GNS*3 та *EVE-NG*. Розглянемо кожний із них окремо, визначимо особливості їх використання, переваги та недоліки.

Cisco Packet Tracer (*CPT*) – це програмний симулятор роботи мережі, розроблений компанією *Cisco,* який дозволяє користувачам створювати мережеві топології та імітувати сучасні комп'ютерні мережі [10, 11]. Цей програмний продукт широко використовують інструктори та слухачі мережевих академій *Cisco* в усьому світі. Основне призначення *CPT* – допомогти вивчити принципи побудови мереж, а також розвинути практичні навички роботи виключно з мережевим обладнанням *Cisco*.

Ця програма має інтуїтивно зрозумілий графічний інтерфейс (рис. 1) та не пострибує значних системних ресурсів для своєї роботи. Уже після її встановлення без додаткових

налаштувань можна створювати базові мережеві топології простим переміщенням пристроїв та ліній зв'язку між ними на робочу ділянку програми. Інструмент ідеально підходить для тих, хто робить перші кроки у вивченні принципів роботи мереж.

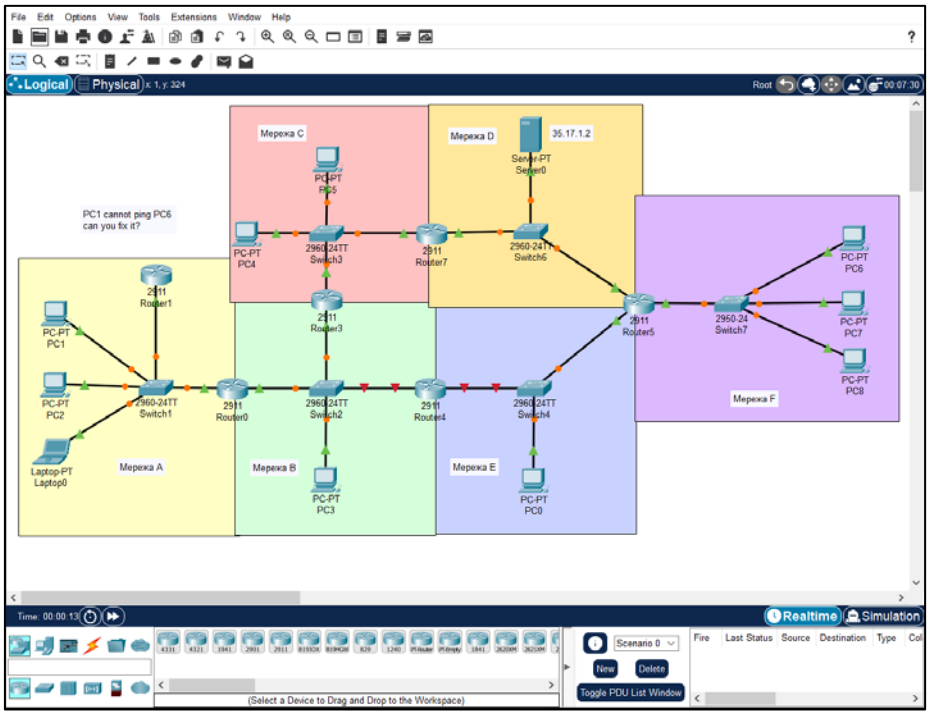


Рис. 1. Інтерфейс Cisco Packet Tracer

Основними можливостями *CPT* є такі [10–12]:

симуляція мережевих (маршрутизаторів, комутаторів, серверів, екранів тощо) та кінцевих (ПЕОМ, *IP*-телефонів, елементів *IoT* тощо) пристроїв. Проте в мережевих пристроях підтримується лише емуляція командного інтерфейсу (*CLI*) *Cisco* і не використовуються реальні образи обладнання. Це означає, що деякі команди та функції можуть бути недоступними або працюватимуть обмежено порівняно з реальними пристроями. Що стосується кінцевого обладнання, то тут здійснюється емуляція виключно ключових функцій, таких як: командний рядок, веббраузер, налаштування *Wi-Fi* під'єднання тощо без прив'язки до конкретної ОС;

конфігурація різних мережевих протоколів та служб (*OSPF, EIGRP, ACL, DHCP, DNS, FTP* тощо);

візуалізація трафіку та моніторинг пакетів.

CPT включає кілька функцій, що можуть бути використані для вивчення основ кібербезпеки, зокрема виключно для кіберзахисту [12]. Наприклад, програма дозволяє:

налаштовувати контроль доступу за допомогою *ACL* (*Access Control List*), що допомагає практикуватися у створенні правил для управління доступом до ресурсів;

моделювати мережеві прості загрози й відпрацьовувати механізми захисту від них, зокрема блокування портів пристроїв у разі несанкціонованого доступу, встановлення фільтрів тощо;

конфігурувати мережеві брандмауери та *VPN*, що імітує реальні сценарії захисту даних;

вивчати принципи роботи таких протоколів безпеки, як: *IPsec, SSL* та *HTTPS,* – які широко використовуються для захисту інформації в разі її передавання мережею.

Основними перевагами використання *CPT є:*

доступність та зручність для моделювання мереж без необхідності в дорогому апаратному забезпеченні. Це надає можливість навчатися в будь-який час і з будь-якого місця, використовуючи звичайний комп'ютер;

інтерактивність: ті, хто навчаються, можуть налаштовувати мережеві компоненти, створювати свої власні топології та експериментувати з конфігураціями без ризику для реальної мережі;

підтримка багатьох протоколів і технологій, що дає можливість отримати повне уявлення про структуру та функціонування мережі.

Разом із тим для *CPT* притаманні обмеження, які мають частковий влив на можливість його використання для відпрацювання питань кібербезпеки, зокрема:

обмежена підтримка складних протоколів. *CPT* не підтримує повного спектра протоколів, що використовуються в реальних мережах, таких як більш складні функції безпеки *Cisco ASA;*

відсутність реальної взаємодії з кіберзагрозами. Хоча ПЗ дозволяє імітувати деякі загрози, реальні атаки часто набагато складніші й потребують використання спеціалізованих платформ;

обмежений у можливостях розширення, тобто *CPT* працює виключно з обладнанням компанії *Cisco* та не підтримує додавання зовнішніх образів устаткування інших вендорів, наприклад *Mikrotik, Juniper* тощо.

Наступним представником програмних засобів моделювання мереж є *GNS*3, його вважають більш професійним, ніж *CPT* [13].

*GNS*3 (*Graphical Network Simulator*) – графічний емулятор комп'ютерних мереж [13, 14]. Його повноцінну роботу забезпечують такі компоненти:

Dynamips – ядро програми, яке дозволяє емулювати образи таких мережевих ОС, як *CiscoIOS, Mikrotik* тощо;

Dynagen – утиліта (текстовий інтерфейс) для *Dynamip,* що дозволяє швидко створювати віртуальні мережі та керувати ними за допомогою конфігураційного файлу типу *INI*;

PEM емулятор брандмауера *CiscoPIX* на основі *Qemu* [15].

*GNS*3 має власний графічний інтерфейс (рис. 2), де необхідні пристрої можна переносити в робочу ділянку та з'єднувати між собою. Цей підхід інтуїтивно зрозумілий. Проте для недосвідченого користувача може виникнути проблема, пов'язана з налаштуванням та першим запуском програми. Передусім це пояснюється тим, що *GNS*3 емулює роботу апаратної частини пристрою, тому для його використання, на відміну від *CPT*, необхідно мати реальний образ ОС цього пристрою, який слід додати до бібліотеки програми, а вже тільки після цих маніпуляцій можливо його використовувати для під'єднання до мережі, що моделюється.

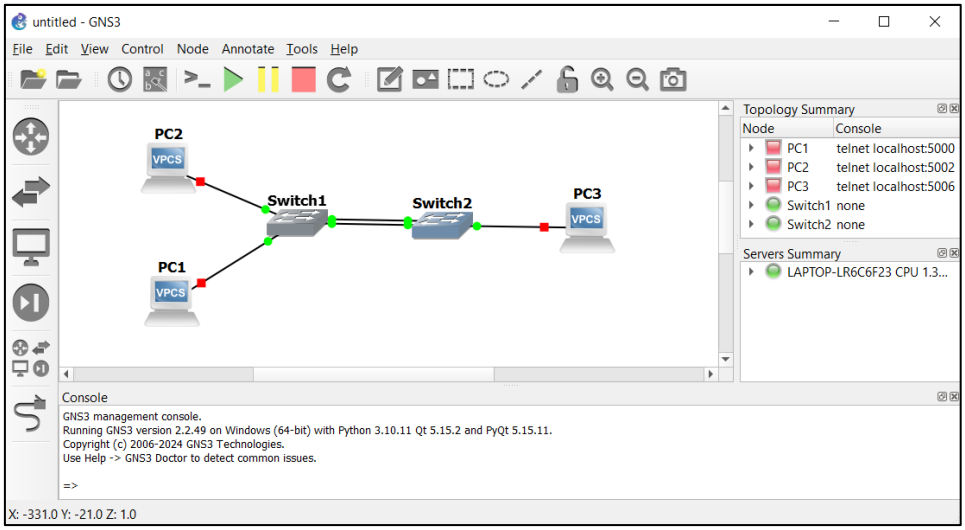


Рис. 2. Інтерфейс GNS3

Що ж стосується кінцевих пристроїв, то тут вже є два варіанти. Перший – використовувати наявний у бібліотеці віртуальний ПЕОМ, функціональні можливості якого значно обмежені. У разі другого варіанта за кінцевий пристрій можливо використати повноцінний віртуальний комп'ютер з *Windows* або *Linux,* чи з будь-якою іншою ОС, оскілки *GNS*3 підтримує технології віртуалізації та інтегровану роботу з такими програмними засобами віртуалізації, як *VirtualBox* або *VMWare.*

Отже, основними можливостями програми *GNS*3 є [14, 16]:

емуляція мережевих пристроїв (маршрутизаторів, комутаторів, серверів) за рахунок їх реальних образів ОС, що дозволяє створювати реалістичні мережеві архітектури;

інтеграція з програмою аналізу мережевого трафіку *Wireshark* для його реального моніторингу та аналізу даних;

підтримка декількох протоколів для налаштування *VPN*, *ACL*, *NAT*, протоколів маршрутизації (*OSPF*, *BGP*);

гнучкість у налаштуванні топологій: використання реальних образів ОС пристроїв, які імітують справжню роботу кінцевих пристроїв;

можливість під'єднання створеної в програмі віртуальної мережі до реальної мережі або Інтернету, що дає змогу максимально реалістично відтворювати складні топології та взаємодію різних мереж.

Зазначені можливості значно підвищують спроможності *GNS*3 порівняно з *CPT* у вивченні питань кібербезпеки.

Для кіберзахисту *GNS*3 дозволяє створювати топології, що включають брандмауери, *VPN*, маршрутизацію з безпечним доступом та сегментацію мережі. Це дає змогу відпрацювати дії з нейтралізації різних типів атак, таких як: відмова в обслуговуванні (*DoS* / *DDoS*), атаки на маршрутизацію (наприклад, *BGP hijacking*), а також спроби обходу брандмауерів. GNS3 також підтримує тестування мережевих інфраструктур на стійкість до атак, що сприяє підготовці до реальних ситуацій. Крім того, завдяки інтеграції з інструментами для аналізу трафіку, зокрема *Wireshark, GNS*3 дозволяє вивчати

структуру мережевого трафіку, аналізувати пакети та виявляти аномалії. Це є критично важливим у навчанні виявлення вторгнень (*Intrusion Detection System, IDS*) та розумінні мережевих атак на рівні даних.

Завдяки використанню в *GNS*3 реальних ОС, наприклад *Kali Linux,* є можливість практикуватися в проведенні тестувань на проникнення або окремих його елементів, таких як: сканування мережі, перехоплення трафіку, виявлення вразливостей тощо.

Отже, перевагами *GNS3* є таке:

використання реальних образів ОС, що робить симуляції максимально наближеними до реальних умов;

підтримка мультивендорних середовищ не тільки пристроїв *Cisco*, але й інших постачальників (наприклад, *Juniper*), що робить *GNS*3 універсальним інструментом;

гнучкість у налаштуванні мережевих топологій: платформа дозволяє створювати складні архітектури, які можуть включати віртуальні машини, брандмауери, *VPN* та інші компоненти;

інтеграція з аналітичними інструментами, можливість підключення до *Wireshark,* що забезпечує аналіз трафіку й тестування безпеки мережевих сегментів.

Попри свої численні переваги, *GNS*3 також має певні обмеження:

високі вимоги до апаратного забезпечення, оскільки може вимагати значних ресурсів комп'ютера, особливо під час емуляції великих топологій із багатьма пристроями.

складність у використанні для початківців, ПЗ має порівняно складний інтерфейс і вимагає певних технічних знань для ефективного налаштування;

обмеження віртуалізації деяких типів пристроїв, зокрема комутаторів серії *Catalyst,* оскільки на них використовується велика кількість специфічних інтегральних мікросхем, які складно емулювати. Це, у свою чергу, дещо обмежує можливість тестування певних конфігурацій;

потреба в образах ОС, тому що для роботи з реальними ОС маршрутизаторів і комутаторів потрібні власні образи, які можуть бути недоступними через ліцензійні обмеження.

Останнім програмним засобом, що розглядяться в рамках цієї статті, є *EVE-NG.*

Emulated Virtual Environment – Next Generation (EVE-NG) – це емульоване віртуальне середовище для професіоналів у сфері мереж, безпеки та *DevOps*, орієнтоване на корпоративних користувачів [17]. *EVE-NG* доступне у двох версіях: *Community* (безкоштовна) та *Professional* (платна). Професійна версія надає більше функцій: додаткові інструменти для спільної роботи та покращене управління топологією. У цілому обидві версії працюють як вебдодаток, а це, в свою чергу, вимагає наявності окремого сервера. Клієнтська частина *EVE-NG* має вебінтерфейс (рис. 3), що дозволяє користувачам працювати через браузер [18].

За своїми функціональними можливостями *EVE-NG* дуже подібний до *GNS*3. Він також підтримує великий вибір мережевого обладнання від різних вендорів. Як і в *GNS*3, є можливість на кінцевих пристроях емулювати реальні ОС. Але ключова відмінність – це клієнт-серверна архітектура *EVE-NG,* завдяки якій спрощується доступ до віртуальних

лабораторій із будь-якого пристрою без необхідності встановлення додаткового ПЗ на клієнтському комп'ютері. Крім того, ця архітектура підтримує мультикористувацький режим, який дозволяє декільком користувачам одночасно працювати в одному середовищі. Це особливо корисно для навчальних закладів, курсів та тренінгів. Проте налаштування сервера та додавання образів як мережевих, так і кінцевих пристроїв є складним процесом, потребує додаткового ПЗ та вимагає від користувача більш глибоких знань управління ОС [19].

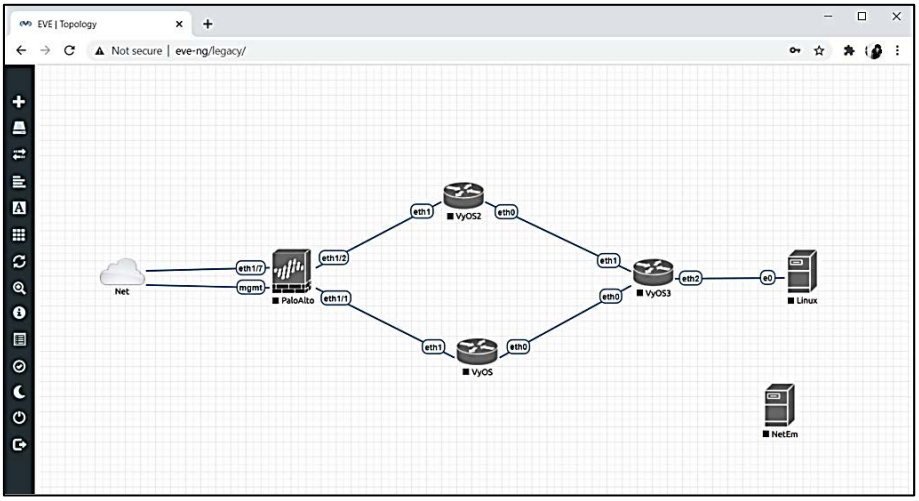


Рис. 3. Інтерфейс EVE-NG

У цілому перевагами використання цієї програми є такі:

реалістичність і повний контроль над середовищем, можливість налаштовувати різні пристрої, платформи та протоколи, створюючи лабораторії, максимально наближені до реальних корпоративних мереж;

доступність великого вибору образів, *EVE-NG* підтримує багато різноманітних пристроїв і мережевих ОС, що надає студентам можливість отримати досвід роботи з різними виробниками мережевого обладнання;

інтеграція з аналітичними інструментами, зокрема можливість використовувати *Wireshark, Splunk, Snort*, що надає тим, хто навчається, глибоке розуміння принципів виявлення та аналізу кіберзагроз.

Крім того, EVE-NG має й певні недоліки:

високі вимоги до апаратного забезпечення, оскільки його сервер потребує значної витрати ресурсів, особливо для великих і складних топологій;

складність для новачків, бо інтерфейс і конфігурації можуть бути незрозумілими для початківців, навчання на *EVE-NG* потребує базових знань у галузі мереж та мережевих технологій;

ліцензійні обмеження, оскільки деякі образи мережевих ОС потребують комерційних ліцензій, що може бути проблемою для навчальних закладів із малим бюджетом.

Узагальнений порівняльний аналіз розглянутих у статті програмних засобів моделювання мереж наведено в табл. 1.

Таблиця 1

Узагальнена порівняльна характеристика програмних засобів моделювання мереж

Характеристика	*CPT*	*GNS3*	*EVE-NG*
Інтерфейс користувача	Зручний	Зручний	Зручний
Можливість використання обладнання різних вендорів	Немає	Є	Є
Використання реальних образів ОС	Ні	Так	Так
Складність додавання нових образів пристроїв	_	Частково	Складно
Потреба в ресурсах ПЕОМ	Низька	Середня	Висока для сервера
Можливість аналізувати трафік	Часткова	Є	Є
Можливість моделювання сценаріїв кіберзахисту	Часткова	Є	Є
Можливість моделювання сценаріїв кібервпливу	Немає	Є	Є

Висновки. *Cisco Packet Tracer, GNS*3 та *EVE-NG* – це три популярні програмні продукти для емуляції та симуляції роботи мереж, які, з урахуванням їх функціональних особливостей можуть бути використані не тільки для формування навичок роботи з комп'ютерною мережею, а й для здобуття практичних навичок із кібербезпеки. Кожен із них має унікальні особливості, які визначають його ефективність у вивченні питань кібербезпеки.

Cisco Packet Tracer доцільно використовувати для навчання та здобуття базових навичок із кібербезпеки. Його перевагами є простий інтерфейс і зручні функції, що дають змогу початківцям вивчити мережеві протоколи, основи маршрутизації та безпекові політики. Однак *CPT* має певні обмеження у відтворенні складних мережевих топологій та кіберзагроз, що знижує його ефективність для глибокого вивчення питань кібербезпеки.

У свою чергу, *GNS*3 є потужнішим інструментом, що забезпечує підтримку реальних образів мережевих пристроїв й емуляцію різних ОС. Це дозволяє створювати більш реалістичні топології, досліджувати роботу складних мережевих протоколів і відпрацьовувати захист від кібератак у віртуальному середовищі. Крім того, він забезпечує гнучкість налаштувань і може бути використаний для навчання мережевій безпеці на середньому та вищому рівнях. Проте його продуктивність дещо знижується у великих топологіях, а конфігурація вимагає значних ресурсів і технічних знань.

EVE-NG є найбільш потужним інструментом для симуляції складних мережевих середовищ і тренувань із кібербезпеки, що потребують умов, максимально наближених до реальних. Завдяки підтримці мультивендорних мережевих образів, можливості багатокористувацької роботи та інтеграції з аналітичними інструментами (*Wireshark* і *Snort), EVE-NG* дозволяє створювати складні лабораторії для відпрацювання виявлення загроз, аналізу трафіку та реагування на інциденти. Цей інструмент є ідеальним для навчальних програм і тренінгів із кібербезпеки на вищому рівні, однак він вимагає значних обчислювальних ресурсів та базових знань у мережевих технологіях.

Отже, *Cisco Packet Tracer, GNS3* та *EVE-NG* доповнюють один одного в процесі отримання практичних навичок із кібербезпеки на різних рівнях навчання. Використання всіх трьох інструментів у навчальних програмах дозволить формувати комплексні знання та практичні навички, необхідні для ефективного захисту критичної інформаційної інфраструктури від кібератак.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Грищук Р. В. Кіберполігон як навчальне середовище з метою підготовки персоналу для боротьби з кіберзлочинністю // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. Одеса : Одеський держ. ун-т внутр. справ, 2017. С. 152–153.
2. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки : монографія / За заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.
3. Даник Ю. Г. Особливості створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. № 1 (34). С. 95–102. https://doi.org/10.33099/2311-7249/2019-34-1-95-102
4. Ciuperca E., Stanciu A., Cîrnu C. Postmodern Education and Technological Development. Cyber Range as a Tool for Developing Cyber Security Skills // INTED 2021 Proceedings. P. 8241–8246. https://doi.org/10.21125/inted.2021.1675
5. Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture // Computers & Security. January 2020. Vol. 88. P. 101636. https://doi.org/10.1016/j.cose.2019.101636
6. Грищук Р. В., Охрімчук В. В. Напрямки підвищення захищеності комп'ютерних систем та мереж від кібератак // Актуальні питання забезпечення кібербезпеки та захисту інформації : тези доп. учасників ІІ Міжнар. наук.-практ. конф. Київ : Вид-во Європейського ун-ту, 2016. С. 60–61.
7. Liu J. A Primer for Real-Time Simulation of Large-Scale Networks // 41st Annual Simulation Symposium. 2008. P. 85–94. https://doi.org/10.1109/anss-41.2008.18
8. Тугай М. Ю., Чорна А. В. Аналіз вільного програмного забезпечення для роботи з комп'ютерними мережами // Сучасний рух науки : тези доп. ІІІ Міжнар. наук.-практ. інтернет-конф. 2018. С. 1354–1359.
9. Емулятори, симулятори чи реальний пристрій – порівнюємо можливості та умови для тестування. URL: https://dou.ua/forums/topic/44451/ (дата звернення: 07.11.2024).
10. Офіційний сайт Мережевої академії Cisco. URL: https://www.netacad.com/ (дата звернення: 01.11.2024).
11. What is Cisco Packet Tracer. URL: https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/ (last accessed: 08.10.2024).
12. Брашовецький В. Є., Семенова О. О. Можливості програми імітаційного моделювання Cisco Packet Tracer версії 7.3.1. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41213/17378.pdf?sequence=3&isAllowed=y (дата звернення: 06.10.2024).

13. Колесник В. В., Вакалюк Т. А. Огляд програмних емуляторів та симуляторів для побудови працездатних моделей мережі. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/7.pdf (дата звернення: 08.11.2024).
14. Офіційний сайт *GNS*3. URL: https://www.gns3.com/ (дата звернення: 08.11.2024).
15. Абрамов В. О. Застосування комбінованих моделей комп'ютерних мереж в навчальному процесі // Кібербезпека: освіта, наука, техніка. 2019. № 4 (4). С. 24–31. https://doi.org/10.28925/2663-4023.2019.4.2431
16. Галата Л. П., Корнієнко Б. Я. Дослідження системи захисту інформації корпоративної мережі на основі *GNS*3 // Наукоємні технології. 2020. № 2 (46). С. 172–179. https://doi.org/10.18372/2310-5461.46.14807
17. Офіційний сайт EVE-NG. URL: https://www.eve-ng.net/ (дата звернення: 08.09.2024).
18. EVE-NG CE Community Edition Cookbook. URL: https://www.eve-ng.net/wp-content/uploads/2024/05/EVE-CE-BOOK-6.2-2024.pdf (last accessed: 08.09.2024).
19. Matkurbanov D., Rakhimjanov K. Analysis of Network Emulation and Simulation Software // Sciences of Europe. 2021. № 79. P. 38–46. https://doi.org/10.24412/3162-2364-2021-79-1-38-46

Стаття надійшла до редакції 12.11.2024.

REFERENCES

1. Hryshchuk, R. V. (2017). Kiberpolihon yak navchalne seredovyshche z metoiu pidhotovky personalu dlia borotby z kiberzlochynnistiu [Cyberrange as a Training Environment for Personnel to Combat Cybercrime]. In *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia : materialy Vseukr. nauk.-prakt. konf. [Cybersecurity in Ukraine: Legal and Organisational Issues: Materials of the All-Ukrainian Scientific and Practical Conference]*. (pp. 152–153). Odesa [in Ukrainian].
2. Danyk, Yu. H., & Hryshchu, R. V. (2016). *Osnovy kibernetychnoi bezpeky: monohrafiia [Basics of cybernetic security: monograph]*. Zhytomyr [in Ukrainian].
3. Danyk, Yu. H. (2019). Osoblyvosti stvorennia kiberpolihoniv dlia doslidzhennia kompleksnykh kiberdii ta pidhotovky fakhivtsiv z kiberbezpeky [Peculiarities of Creating Cyberranges for the Study of Complex Cyber Actions and Training of Cybersecurity Specialists]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony [Modern Information Technologies in the Field of Security and Defence]*, *1* (34), 95–102. https://doi.org/10.33099/2311-7249/2019-34-1-95-102 [in Ukrainian].
4. Ciuperca, E., Stanciu, A., & Cîrnu, C. (2021). Postmodern Education and Technological Development. Cyber Range as a Tool for Developing Cyber Security Skills. *INTED 2021 Proceedings*, 8241–8246. https://doi.org/10.21125/inted.2021.1675
5. Muhammad Mudassar Yamin, Basel Katt, & Vasileios Gkioulos. (2020). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security, 88*, 101636. https://doi.org/10.1016/j.cose.2019.101636
6. Hryshchuk, R. V., & Okhrimchuk, V. V. (2016). Napriamky pidvyshchennia zakhyshchenosti komp'iuternykh system ta merezh vid kiberatak [Directions of Increasing the Security of

Computer Systems and Networks from Cyberattacks]. In *Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii: tezy dop. uchasnykiv II Mizhnar. nauk.-prakt. konf. [Actual Issues of Cybersecurity and Information Protection: Abstracts of the Participants of the II International Scientific and Practical Conference]*. (pp. 60–61. Kyiv [in Ukrainian].
7. Liu, J. (2008). A Primer for Real-Time Simulation of Large-Scale Networks. In *41st Annual Simulation Symposium*. (pp. 85–94). https://doi.org/10.1109/anss-41.2008.18
8. Tuhai, M. Yu., & Chorna, A. V. (2018). Analiz vilnoho prohramnoho zabezpechennia dlia roboty z komp'iuternymy merezhamy [Analysis of Free Software for Working with Computer Networks]. In *Suchasnyi rukh nauky : tezy dop. III Mizhnar. nauk.-prakt. internet-konf. [Modern Scientific Movement: Abstracts of the 3rd International Scientific-Practical Internet Conference]*. (pp. 1354–1359). [in Ukrainian].
9. *Emuliatory, symuliatory chy realnyi prystrii – porivniuiemo mozhlyvosti ta umovy dlia testuvannia [Emulators, Simulators or a Real Device – Comparing Possibilities and Conditions for Testing]*. (n. d.). Retrieved from https://dou.ua/forums/topic/44451/ [in Ukrainian].
10. *Official website of the Cisco Network Academy*. (n. d.). Retrieved from https://www.netacad.com/ [in Ukrainian].
11. *What is Cisco Packet Tracer*. (n. d.). Retrieved from https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/
12. Brashovetskyi, V. Ye., & Semenova, O. O. (n. d.). *Mozhlyvosti prohramy imitatsiinoho modeliuvannia Cisco Packet Tracer versii 7.3.1 [Features of Cisco Packet Tracer simulation software version 7.3.1]*. Retrieved from https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41213/17378.pdf?sequence=3&isAllowed=y [in Ukrainian].
13. Kolesnyk, V. V., & Vakaliuk, T. A. (n. d.). *Ohliad prohramnykh emuliatoriv ta symuliatoriv dlia pobudovy pratsezdatnykh modelei merezhi [An Overview of Software Emulators and Simulators for Building Working Network Models]*. Retrieved from https://conf.ztu.edu.ua/wp-content/uploads/2021/01/7.pdf [in Ukrainian].
14. *Official website of the GNS3*. (n. d.). Retrieved from https://www.gns3.com/
15. Abramov, V. O. (2019). Zastosuvannia kombinovanykh modelei komp'iuternykh merezh v navchalnomu protsesi [Use of Combined Models of Computer Networks in the Educational Process]. *Kiberbezpeka: osvita, nauka, tekhnika [Cyber Security: Education, Science, Technology]*, *4* (4), 24–31. https://doi.org/10.28925/2663-4023.2019.4.2431 [in Ukrainian].
16. Halata, L. P., & Korniienko, B. Ya. (2020). Doslidzhennia systemy zakhystu informatsii korporatyvnoi merezhi na osnovi GNS3 [Research of the Corporate Network Information Security System Based on GNS3]. *Naukoiemni tekhnolohii [Science-Intensive Technologies]*, *2* (46), 172–179. https://doi.org/10.18372/2310-5461.46.14807 [in Ukrainian].
17. *Official website of the EVE-NG*. (n. d.). Retrieved from https://www.eve-ng.net/
18. EVE-NG CE Community Edition Cookbook. (n. d.). Retrieved from https://www.eve-ng.net/wp-content/uploads/2024/05/EVE-CE-BOOK-6.2-2024.pdf
19. Matkurbanov, D., & Rakhimjanov, K. (2021). Analysis of Network Emulation and Simulation Software. *Sciences of Europe, 79,* 38–46. https://doi.org/10.24412/3162-2364-2021-79-1-38-46

ISSN 2076-1546

V. V. Okhrimchuk, I. A. Okhrimchuk

ANALYSIS OF NETWORK MODELLING TOOLS FOR THE POSSIBILITY OF THEIR USE FOR PRACTICAL TRAINING OF CYBERSECURITY SPECIALISTS

Despite the existing information security systems, the key aspect of effective cyber defense remains the level of training of personnel responsible for cyber security. Today, the training of a cybersecurity specialist should be based on a comprehensive study of modern information technologies, mechanisms and patterns of cyberattacks, ways to counter them, and include both theoretical and practical components. It has been established that the most common practice in the leading educational and scientific institutions of the world and Ukraine in terms of practical training of cybersecurity specialists is the creation and deployment of complex software and hardware complexes - cyber training grounds, but this requires significant resources. Therefore, software tools for emulating and simulating computer networks are becoming an alternative to obtaining initial practical skills in cybersecurity.

The article analyses three of the most popular free tools for simulating and emulating computer networks - Cisco Packet Tracer, GNS3 and EVE-NG - with regard to the possibility of their use for practical training of cybersecurity specialists. The analysis found that Cisco Packet Tracer, which is aimed at novice users, provides simulation of network devices exclusively from Cisco, allows you to configure basic protocols and practice the basics of cyber defence. GNS3 is slightly more advanced than Cisco Packet Tracer in terms of functionality, emulates real operating system images and supports many network device vendors, making it useful for complex training tasks. In addition, GNS3 provides the ability to recreate cyberattack scenarios, and the integrated Wireshark network analyser allows you to monitor traffic and analyse the course of a cyberattack on the system. In turn, EVE-NG is a powerful network emulation platform that is very close to GNS3 in terms of functionality. It also provides extensive hardware support and enables the deployment of complex network topologies. However, the main feature of EVE-NG is its client-server architecture, which enables multi-user operation.

Thus, Cisco Packet Tracer, GNS3, and EVE-NG complement each other in the process of acquiring practical cybersecurity skills at different levels of education. The use of all three tools in training programmers will help to develop the comprehensive knowledge and practical skills necessary to effectively protect critical information infrastructure from cyberattacks.

Keywords*: cybersecurity; cyberdefence; cyberattack; emulator; simulator; virtualization; Cisco; GNS; EVE-NG.*

УДК 004.39 DOI: 10.46972/2076-1546.2024.27.06

І. В. Пулеко, В. О. Чумакевич, І. М. Шестак, В. Л. Рикун, І. В. Свистунович

ФУНКЦІЯ ЩІЛЬНОСТІ РОЗПОДІЛУ ЦІЛЕЙ ДЛЯ ПЛАНУВАННЯ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Основною проблемою видової повітряної розвідки є суперечність між розмірами площі огляду та розмірами елементарних об'єктів (цілей). Оскільки площа огляду дуже велика, розміри цілі малі, а миттєве поле зору бортової апаратури обмежене, то час на отримання даних досить значний і обсяги інформації, що підлягають обробленню, є дуже великими. Крім того, через технічні обмеження за часом перебування в повітрі та особливості апаратури видової розвідки один безпілотний літальний апарат не в змозі охопити всю площу за один виліт. Гостроту цієї проблеми можна частково зняти шляхом застосування групи безпілотних літальних апаратів, але як для одного, так і для групи постає завдання планування маршруту руху. Простий гребінчастий огляд зони розвідки є далеко не оптимальним, на практиці застосовують планування маршруту за точками із залученням апріорної інформації про найбільш імовірні місця розташування цілей. Однак цей спосіб досить незручний для автоматичного планування маршруту самим безпілотним літальним апаратом, оскільки точка на карті зазвичай не співвідноситься з висотою польоту, миттєвим полем зору бортової апаратури спостереження, масштабом та детальністю знімка. Для підвищення можливостей оптимізації автоматичного планування польоту запропоновано застосовувати функцію щільності розподілу цілей.

Функція щільності розподілу цілей – це двовимірна математична модель, яка описує умовну відносну ймовірність знаходження цілей у різних точках простору. Вона створюється і задається на основі апріорних даних про місцевість, попередніх спостережень або інтелектуальних оцінок, що відображають розподіл можливих цілей у певній області або для всієї зони розвідки. Функція щільності розподілу цілей дозволяє моделювати простір не як однорідний, а як область із різними ступенями важливості або ж імовірностями знаходження цілей. Слід зауважити, що отримання математично обґрунтованих чи розрахованих за теорією ймовірності або математичної статистики двовимірних дискретних щільностей імовірностей для випадково розміщених цілей фактично не можливе. Тому в статті функція щільності розподілу цілей розглядається як область із різними ступенями важливості огляду, що відображається умовними відносними ймовірностями, отриманими з різних джерел, зокрема й експертним оцінюванням.

Ключові слова: *повітряна розвідка; безпілотний літальний апарат; щільність імовірності; функція щільності розподілу цілей; зона розвідки; параметри знімка.*

Постановка проблеми в загальному вигляді. Війна сьогодення – це битва новітніх технологій, штучного інтелекту та сучасного озброєння, що забезпечує підвищення ефективності вогневого ураження противника й живучість підрозділів Збройних Сил України та інших складових Сил оборони України [1]. Досвід ведення бойових дій

© І. В. Пулеко, В. О. Чумакевич, І. М. Шестак, В. Л. Рикун, І. В. Свистунович, 2024

у російсько-українській війні переконливо свідчить про актуалізацію проблеми групового застосування безпілотних літальних апаратів (БпЛА) для виконання багатьох військових завдань [2]. Особливо актуальною ця проблема постає для груп малих БпЛА, які вже можуть створюватися на основі наявного парку літальних апаратів.

Відомо [3–4], що основною проблемою видової повітряної розвідки є суперечність між розмірами площі огляду та розмірами елементарних об'єктів (цілей). Оскільки площа огляду дуже велика, розміри цілі малі, а миттєве поле зору бортової апаратури обмежене, то час на отримання даних досить значний і обсяги інформації, що підлягають обробленню, є дуже великими. Кім того, через технічні обмеження за часом перебування в повітрі та особливості апаратури видової розвідки один БпЛА не в змозі охопити всю площу за один виліт. Гостроту цієї проблеми можна частково зняти шляхом застосування групи БпЛА, але як для одного, так і для групи постає завдання планування маршруту руху. Простий гребінчастий огляд зони розвідки є далеко не оптимальним, і на практиці застосовують планування маршруту за точками із залученням апріорної інформації про найбільш імовірні місця розташування цілей.

Аналіз останніх досліджень і публікацій. Оскільки тема планування застосування БпЛА є дуже популярною, то останнім часом їй присвячено достатньо велику кількість публікацій [5–12]. У найбільш загальному вигляді огляди підходів та класифікації методів планування здійснено в [5–6].

Стохастичні евристичні алгоритми розглянуто в роботі [7], наведено їх характеристики, напрями вдосконалення, застосування, переваги та недоліки, однак інші види алгоритмів для формування маршрутів руху БпЛА не обговорювалися.

У роботі [8] алгоритми планування маршруту руху групи БпЛА розділено на п'ять видів: оптимізаційні; планування на основі теорії графів; евристичні; ройового інтелекту; нейронно-мережеві.

У статті [9] розглянуто алгоритми ройового інтелекту з таких позицій, як: побудова алгоритмів уникнення зіткнень; розподіл завдань; планування маршруту за точками.

Методологічні аспекти формування інтелектуальної складової агентної системи рою БпЛА розглянуті в [10–11].

Досить цікавий метод планування маршруту ведення повітряної розвідки динамічних об'єктів із використанням БпЛА подано в [12].

Аналіз джерел показує, що, незважаючи на досить велику кількість запропонованих методів планування, більшість із них не враховують особливостей ведення військової повітряної розвідки й дорозвідки, рельєфу місцевості та здебільшого орієнтовані на оптимізацію польотів за точками. У той же час для планування пошуку цілей застосовують гребінчастий, розширювальний чи вільний способи пошуку, однак вони досить незручні для автоматичного планування маршруту самим БпЛА, оскільки точка на карті зазвичай не співвідноситься з висотою польоту, миттєвим полем зору бортової апаратури спостереження, масштабом та детальністю знімка. Для підвищення можливостей оптимізації автоматичного планування польоту пропонуємо застосовувати функцію щільності розподілу цілей (ФЩРЦ).

Формулювання завдання дослідження. Метою цієї статті є введення та формалізація поняття ФЩРЦ у зоні розвідки.

ФЩРЦ – це двовимірна математична модель, яка описує умовну відносну ймовірність знаходження цілей у різних точках простору. Вона створюється та задається на основі даних про місцевість, попередніх спостережень або інтелектуальних оцінок, що відображають розподіл можливих цілей у певній області або для всієї зони розвідки. ФЩРЦ дозволяє моделювати простір не як однорідний, а як область із різними ступенями важливості або ж імовірностями знаходження цілей. Слід зазначити, що отримання математично обґрунтованих чи розрахованих за теорією ймовірності або математичної статистики двовимірних дискретних щільностей імовірностей для випадково розміщених цілей фактично не можливе. Тому в статті ФЩРЦ розглядається як область із різними ступенями важливості огляду, що відображається умовними відносними ймовірностями, отриманими з різних джерел, зокрема й експертним оцінюванням.

Виклад основного матеріалу. Під час ведення бойових дій як наші підрозділи, так і підрозділи противника мають керуватися бойовими статутами щодо свого розміщення та порядку дій [3, 13]. Це призводить до нерівномірного розподілу особового складу, озброєння та техніки на місцевості. Наприклад, на рис. 1. показано типову схему розміщення роти в обороні.

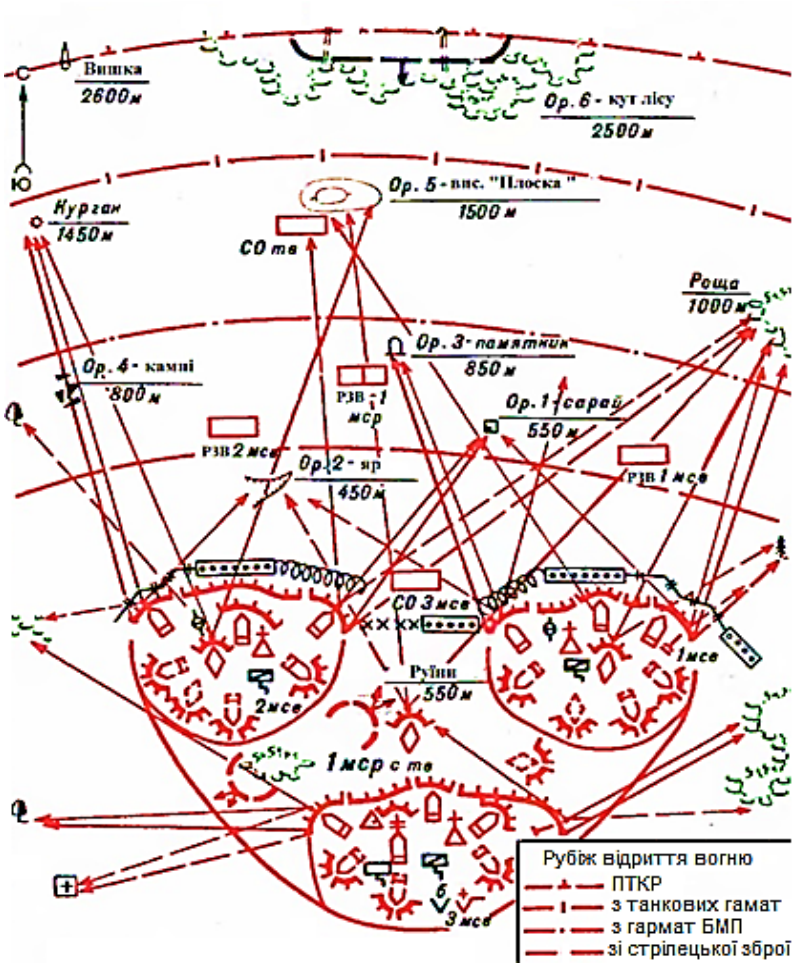


Рис. 1. Приклад типової схеми розміщення роти в обороні

Якщо за цілі розвідки визначити важке озброєння та військову техніку, то, позначаючи кожну ціль окремою крапкою, можна отримати схему, подібну до наведеної на рис. 2.

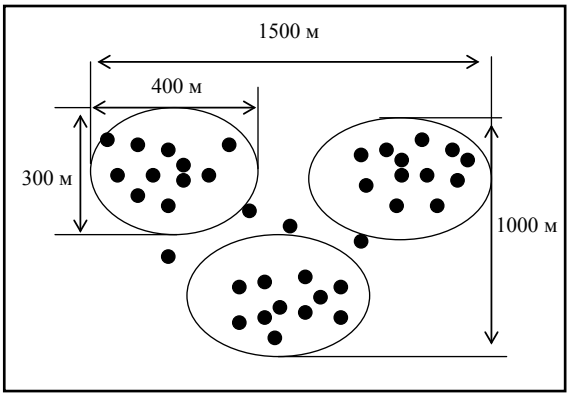


Рис. 2. Умовна схема розміщення цілей на площі розвідки

Як бачимо із рис. 2 у ході побудови бойових порядків на площі цілі розміщуються нерівномірно. Крім того, завжди є якась достовірна чи не зовсім достовірна апріорна інформація (наприклад, від інших видів розвідок) щодо можливих районів розміщення чи зосередження ворога. Якщо описати цю нерівномірність розміщення якоюсь математичною функцією, то така модель дозволить більш якісно планувати маршрути БпЛА та організовувати їх взаємодію в разі групового чи ройового польоту.

Введемо двовимірну функцію, яка описує ймовірність того, що ціль знаходиться в певній точці простору з координатами (x,y) на площині зони дій БпЛА. У загальному вигляді позначимо її як $f(x,y)$:

$$\begin{aligned} &f(x,y)\geq 0 \ \forall(x,y); \\ &\int_A f(x,y)dxdy = 1, \end{aligned} \tag{1}$$

де А – область простору (ділянка земної поверхні), над якою виконується місія.

З погляду математики до побудови такої функції можливі як мінімум чотири підходи: аналітичний, емпіричний, імітаційного моделювання та кластеризації.

Якщо розподіл цілей має певні відомі закономірності або його можна змоделювати математично, то використовують аналітичні моделі. Прикладом може бути гаусівський розподіл цілей у зоні операції:

$$f(x,y)=\frac{1}{2\pi\sigma_x\sigma_y}exp\left(-\frac{1}{2}\left(\frac{(x-\mu_x)^2}{\sigma_x^2}+\frac{(y-\mu_y)^2}{\sigma_y^2}\right)\right), \tag{2}$$

де μ_x, μ_y – середні координати цілей у зоні операції;

σ_x, σ_y – стандартні відхилення для координат *x* та *y*.

Однак цей метод підходить лише для випадків, коли розподіл цілей можна описати як гаусівське "згущення" навколо певної точки, чого в реальних ситуаціях майже ніколи не буває.

Якщо є хронологічні дані про попередні завдання або спостереження за рухом цілей, то можна використовувати їх для побудови функції щільності за допомогою емпіричного методу. У математичній статистиці для цього застосовують, наприклад, ядерне (ядрове, ядро) оцінювання щільності (Kernel Density Estimation – KDE) або двовимірні гістограми. KDE – це один із підходів до оцінювання щільності розподілу точок, що дозволяє згладити розподіл цілей на основі емпіричних даних. Функція щільності для кожної точки (x_i, y_i) з набору спостережень N може бути оцінена за допомогою такої формули:

$$\hat{f}(x,y) = \frac{1}{N h_x h_y} \sum_{i=1}^{N} K\left(\frac{x - x_i}{h_x}\right) K\left(\frac{y - y_i}{h_y}\right), \tag{3}$$

де $\hat{f}(x,y)$ – оцінена функція щільності;

N – кількість точок спостережень;

$K(\cdot)$ – функція ядра, найчастіше використовують гаусівську функцію ядра:

$$K(u) = \frac{1}{2} exp\left(-\frac{u^2}{2}\right);$$

h_x, h_y – параметри згладжування (ширина вікна) за осями x та y;

(x_i, y_i) – координати цілей.

Параметри згладжування h_x, h_y визначають, наскільки широко розташовані ядерні функції навколо кожної точки. Якщо вибрати занадто мале значення h_x, h_y, то щільність буде "рваною", а якщо занадто велике, – то занадто згладженою.

Цей підхід корисний, якщо є достатньо даних про розподіл цілей у минулому.

За умови розробки потужного програмного забезпечення чи моделюючого середовища та наявності достатнього часу можна застосовувати методи імітаційного моделювання. Якщо місцеположення цілі динамічно змінюється або ж залежить від часу, то можна використовувати методи Монте-Карло чи агентного моделювання для симуляції ймовірних траєкторій руху цілей і побудови функції щільності.

Оскільки задача побудови ФЩРЦ полягає в групуванні точок на основі відстані між ними, то можна об'єднувати їх у кластери за ознакою близькості. Алгоритми кластеризації (K-means, DBSCAN) або ієрархічна кластеризація добре підходять для таких задач.

Останні два підходи є дуже перспективними і передбачають застосування методів штучного інтелекту, але їх розвиток стримує відсутність спеціалізованого програмного забезпечення та відповідних наборів даних для навчання. Тому в основу цього дослідження покладені методи другого напрямку.

Припустимо, що є набір точок із координатами (x_i, y_i), де i=1, 2, …, N, що визначають відомі чи передбачувані цілі. Ці координати є положенням точок у двовимірному просторі. При цьому можна скористатися, наприклад, прямокутною системою координат.

Перед тим, як оцінювати щільність, потрібно визначити область (x,y) для оцінювання щільності, тобто розробити свою сітку координат, на якій буде оцінюватися функція щільності (рис. 3).

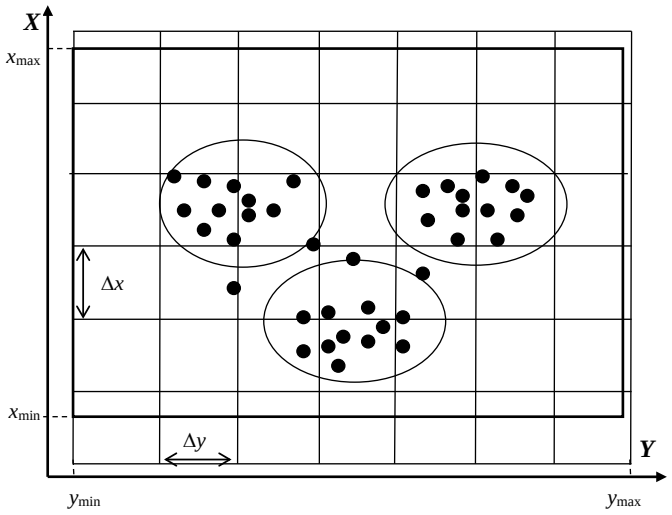


Рис. 3. Умовна схема накладання сітки на площу розвідки

Можна створити сітку точок (X,Y), де

$$X = [x_{min}, x_{max}],\ Y = [y_{min}, y_{max}].$$

Це означає, що ми знаходимо мінімальні та максимальні значення по осях координат *x* та *y* для всієї області, де визначені дані.

Далі необхідно провести дискретизацію та визначити крок сітки Δx і Δy для кожної з координат.

З погляду математики дискретизація двовимірної функції – це заміна безперервного в просторі (x,y) значення функції $F(x,y)$ послідовністю дискретних значень $F(i,j)$.

Найбільш зручним і природним способом дискретизації є подання функції у вигляді вибірок їхніх значень (*відліків*) в окремих, регулярно розташованих точках ($x = i\,\Delta x$, $y = j\,\Delta y$). Послідовність точок ($x = i\,\Delta x$, $y = j\,\Delta y$), у яких беруться відліки, і буде створювати сітку. Математично це описують як згортку певного сигналу з деякою двовимірною функцією $A_Д(u,v)$:

$$F(i,j) \approx \iint I(i\Delta x - u,\ j\Delta y - v) A_Д(u,v)\,du\,dv, \qquad (4)$$

Функцію $A_Д(u,v)$ називають *апертурою дискретизації*.

Набір одержаних значень $F(i,j)$ складає дискретне подання сигналу.

Вибір кроку сітки дискретизації ФЩРЦ є задачею досить суперечливою. З одного боку, вибір малого кроку дискретизації може призвести до появи небажаних провалів у ФЩРЦ та збільшення необхідної кількості дій у ході планування. З іншого боку, занадто великий крок дискретизації призведе до появи значної похибки апроксимації та

нівелювання сенсу самої функції. Тому пропонуємо крок дискретизації ФЩРЦ прив'язати до площі місцевості, що фіксується одним кадром, та безпечних висот польоту БпЛА.

Введемо обмеження, допущення та позначення.

Помилки утримання літака на маршруті такі:

утримання БпЛА на запроєктованій висоті – ±15 м;

поперечне зміщення від осі маршруту – ±10 м;

зміна кута крену БпЛА на маршруті між двома знімками – 10°;

зміна кута тангажа БпЛА на маршруті між двома знімками – 6°.

Параметри знімальної системи (рис. 4):

фокусна відстань оптичної системи – f;

висота фотографування – H;

довжина половини діагоналі матриці – L (для 35 мм кадру вона становить 21,6 мм);

довжина половини діагоналі знімка на місцевості – D.

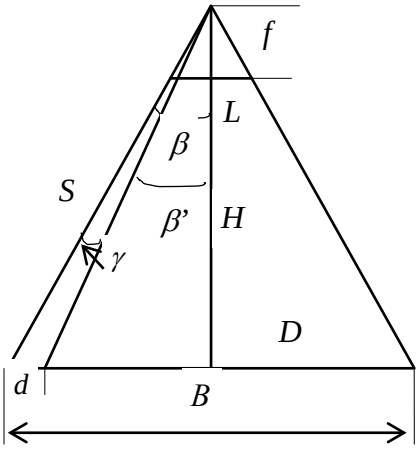


Рис. 4. Геометричні співвідношення проєкції пікселя на місцевість

Відповідно до рис. 4 максимально допустима висота аерофотознімання для забезпечення заданого просторового розрізнення обчислюється за формулою

$$H_{max} = S\cos\beta, \tag{5}$$

де

$$S = \frac{d\cos(\gamma - \beta)}{\sin\gamma}. \tag{6}$$

Тут розрахунок роздільної здатності знімка проводиться для пікселів найбільш віддалених від центра кадру, де вона найгірша.

З урахуванням похибки барометричного датчика висоту польоту H_p можна визначити як

$$H_p = H_{max} - 20\,(\text{м}). \tag{7}$$

Для розрахованої висоти половина ширини захвату місцевості камерою, з урахуванням прийнятих помилок, обчислюється за формулою

$$D = \left(H_p - 15\right) tg\left(\beta - 6\right) - 10\,(\text{м}), \tag{8}$$

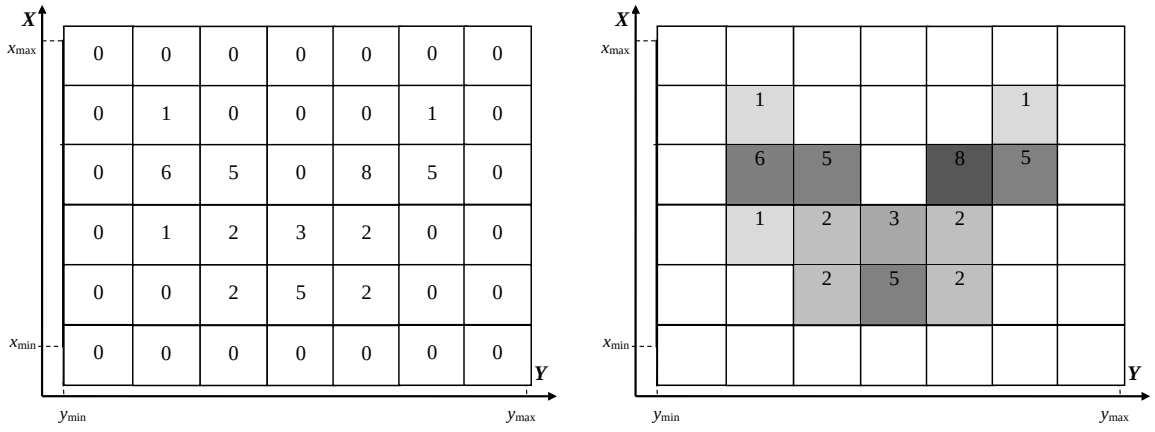
Відповідно, ширина захвату місцевості камерою буде становити

$$B = 2 \cdot K_y \cdot D\,, \tag{9}$$

де K_y – коефіцієнт, що враховує похибку наведення, K_y = 0,9. Для планування маршрутів, за необхідності, цим же коефіцієнтом можна враховувати й 30% поперечного перекриття знімків.

Отже, отримана формула (9) дозволяє розрахувати крок дискретизації ФЩРЦ.

Далі в кожному квадраті підраховується кількість апріорних цілей, які туди потрапили, та формується матриця числових значень (рис. 5а).



а *б*

Рис. 5. Види подання ФЩРЦ

Для наочності ФЩРЦ можна нормувати та відображати у відтінках сірого, насиченість якого тим вища, чим більша кількість цілей потрапила в квадрат сітки (рис. 5б).

У випадках, коли апріорно відомо про велику кількість цілей, однак достовірність даних сумнівна, то, відобразивши їх у прямокутних координатах, доцільно скористатися методом згладжування KDE за формулою (3), а вже потім накладати сітку та визначати середнє значення в межах квадрата.

Наведемо приклад програми для побудови двовимірної KDE за допомогою бібліотек Python, таких як: `scipy, sklearn` або `seaborn`.

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import gaussian_kde

# Дані про цілі
x = np.array([1, 2, 3, 4, 5, 6])  # Координати x точок
y = np.array([2, 3, 4, 5, 6, 7])  # Координати y точок
```

```
# Об'єднуємо дані в один масив
data = np.vstack([x, y])

# Створюємо KDE
kde = gaussian_kde(data)

# Визначаємо сітку для оцінювання щільності
xgrid = np.linspace(min(x), max(x), 100)
ygrid = np.linspace(min(y), max(y), 100)
X, Y = np.meshgrid(xgrid, ygrid)
positions = np.vstack([X.ravel(), Y.ravel()])

# Оцінюємо функцію щільності
Z = np.reshape(kde(positions).T, X.shape)

# Побудова графіка
plt.imshow(np.rot90(Z), extent=[x.min(), x.max(), y.min(), y.max()],
cmap=plt.cm.gist_earth_r)
plt.colorbar()
plt.scatter(x, y, c='red')  # Відображаємо положення цілей
plt.title('Двовимірна функція щільності розподілу цілей')
plt.show()
```

У результаті виконання програми отримаємо графік (рис. 6), що показує оцінену щільність імовірності для двовимірного розподілу цілей у просторі. Цілі позначені точками. Точки з вищою щільністю будуть мати більш інтенсивний колір, що вказує на більшу ймовірність присутності об’єктів у цих місцях.

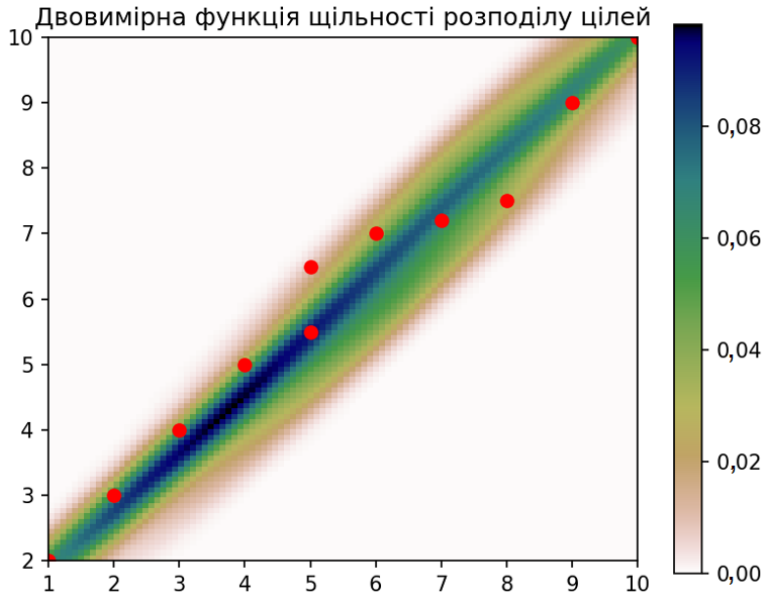


Рис. 6. Приклад KDE оцінювання ФЩРЦ

У випадках, коли апріорної інформації про цілі мало або відомо лише про поодинокі цілі, то ФЩРЦ стає дуже розрідженою. У такому разі пропонуємо підхід на основі експертного оцінювання району за квадратами, до якого залучаються найбільш досвідчені командири та начальники підрозділів розвідок, які на підставі вивчення місцевості, противника та власного досвіду визначають найбільш імовірні райони розміщення ворога та розподіляють їх пріоритетність.

Цілком природно і зрозуміло, що, оскільки противник може динамічно переміщувати цілі, то і ФЩРЦ повинна адаптуватися до нових умов та залежати від часу. Так, у процесі виконання місії БпЛА можуть отримувати нові дані про розташування цілей (наприклад, від бортових сенсорів або від інших дронів, чи з інших джерел). На основі цих даних ФЩРЦ може бути оновлена, що дозволить оперативно коригувати траєкторії БпЛА для ефективнішого виконання місії.

Висновки. Розроблена двовимірна ФЩРЦ дозволяє моделювати простір не як однорідний, а як область із різними ступенями важливості або ж імовірностями знаходження цілей. Розрахунок ФЩРЦ дозволяє оптимізувати планування місій БпЛА, зокрема визначати найбільш імовірні місця знаходження цілей, обирати оптимальні траєкторії для розвідки або ударів і зменшувати час на виконання завдань. Для побудови такої функції можуть використовуватися як емпіричні дані, так і математичні моделі.

Накладання ФЩРЦ на польотну карту дозволить створити так звану карту пріоритетності окремих ділянок місцевості для автоматичного планування місій БпЛА.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. ОП 3-0(46). Застосування безпілотних систем у Силах оборони України : Доктрина. Київ : ЦУБС ГШ ЗС України, 2023. 56 с.

2. Коршець О., Горбенко В. Уроки застосування безпілотних літальних апаратів у російсько-українській війні // Повітряна міць України. 2023. № 1 (4). С. 9–17. https://doi.org/10.33099/2786–7714–2023–1-4–9-17

3. Олексенко О. О., Авраменко О. В., Федоров А. В. Застосування безпілотних літальних апаратів збройними силами російської федерації у війні проти України // Наука і техніка Повітряних Сил Збройних Сил України. 2022. № 4 (49). С. 23–28.

4. Ребрін Ю. К. Оптико-електронне розвідувальне обладнання літальних апаратів. Київ : КВВАІУ, 1988. 450 с.

5. Чумак О. О., Дудко М. В., Дмітрієв О. М. Онтологія методів планування маршрутів руху безпілотних літальних апаратів // Випробування та сертифікація. № 1 (3). 2024. С. 69–77. https://doi.org/10.37701/ts.03.2024.10

6. Кучеренко О. І., Вакалюк Т. А. Класифікація методів та алгоритмів побудови маршрутів БпЛА // Вчені записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки. 2024. Т. 35 (74), № 3. С. 111–116. https://doi.org/10.32782/2663-5941/2024.3.1/18

7. Stochastic Heuristic Algorithms for Multi-UAV Cooperative Path Planning / Zhao C., Liu Y., Yu L., Li W. // In Proceedings of the 2021 40th Chinese Control Conference (CCC). Shanghai, China. July 26–28, 2021. P. 7677–7682. https://doi.org/10.23919/ccc52363.2021.9549984

8. Sun W., Hao M. A Survey of Cooperative Path Planning for Multiple UAVs // In Proceedings of the International Conference on Autonomous Unmanned Systems. Shanghai, China. July 26–28, 2021. P. 189–196. https://doi.org/10.1007/978-981-16-9492-9_20

9. Tang J., Duan H., Lao S. Swarm Intelligence Algorithms for Multiple Unmanned Aerial Vehicles Collaboration: A Comprehensive Review // Artif. Intell. Rev. 2022. P. 1–33. https://doi.org/10.1007/s10462-022-10281-7

10. Методологія формування інтелектуальної складової агентної системи рою безпілотних літальних апаратів : Монографія / О. К. Погудіна, Д. М. Крицький, А. М. Биков та ін. Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харк. авіац. ін-т», 2021. 219 с.
11. Бережний А. О. Методи та інформаційна технологія автоматизованого планування маршрутів польотів безпілотних літальних апаратів для підвищення ефективності пошуку об'єктів : Дис. на здобуття наук. ступеня канд. тех. наук за спец. 05.13.06 – Інформаційні технології. Харків : Харківський нац. ун-т Повітряних Сил ім. Івана Кожедуба, Черкаси : Черкаський держ. технологіч. ун-т, 2020. 192 с.
12. Метод планування маршруту ведення повітряної розвідки динамічних об'єктів з використанням безпілотних літальних апаратів в лісостеповій місцевості / О. І. Тимочко, А. В. Тристан, О. Є. Чернавіна, А. О. Бережний // Системи обробки інформації. 2020. № 3 (162). С. 95–110. https://doi.org/10.30748/soi.2020.162.10
13. Обґрунтування загальних вимог до оперативно-тактиних та тактичних безпілотних авіаційних комплексів / Ю. Г. Даник, І. В. Пулеко, О. В. Соловйов, П. В. Поздняков // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ ДУТ, 2013. Вип. 7. С. 21–31.
14. Пулеко І. В. Інформаційна технологія навігації малого безпілотного літального апарата за оптичним полем Землі в умовах пропадання сигналів супутникових радіонавігаційних систем // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2018. Вип. 15. С. 118–129.
15. Weglarczyk S. Kernel Density Estimation and its Application // ITM Web of Conferences. 2018. 23, 00037. P. 1–8. https://doi.org/10.1051/itmconf/20182300037

Стаття надійшла до редакції 12.11.2024.

REFERENCES

1. *OP 3-0(46). Zastosuvannia bezpilotnykh system u Sylakh oborony Ukrainy: Doktryna [Application of Unmanned Systems in the Defense Forces of Ukraine: Doctrine]*. (2023). Kyiv [in Ukrainian].
2. Korshets, O., & Horbenko, V. (2023). Uroky zastosuvannia bezpilotnykh litalnykh aparativ u rosiisko-ukrainskii viini [Lessons in the Use of Unmanned Aerial Vehicles in the russian-Ukrainian war]. *Povitriana mits Ukrainy [Air Power of Ukraine], 1* (4), 9–17. https://doi.org/10.33099/2786–7714–2023–1-4–9-17 [in Ukrainian].
3 Oleksenko, O. O., Avramenko, O. V., & Fedorov, A. V. (2022). Zastosuvannia bezpilotnykh litalnykh aparativ zbroinymy sylamy rosiiskoi federatsii u viini proty Ukrainy [Application of Unmanned Aerial Vehicles by the Armed Forces of the russian federation in the war against Ukraine]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy [Science and Technology of the Air Forces of the Armed Forces of Ukraine.], 4* (49), 23–28 [in Ukrainian].
4. Rebrin, Yu. K. (1988). *Optyko-elektronne rozviduvalne obladnannia litalnykh aparativ [Optical-Electronic Reconnaissance Equipment of Aircraft]*. Kyiv [in Ukrainian].
5. Chumak, O. O., Dudko, M. V., & Dmitriiev, O. M. (2024). Ontolohiia metodiv planuvannia marshrutiv rukhu bezpilotnykh litalnykh aparativ [Ontology of Methods of Planning Routes of

Unmanned Aerial Vehicles]. *Vyprobuvannia ta sertyfikatsiia [Testing and Certification], 1* (3), 69–77 [in Ukrainian]. https://doi.org/10.37701/ts.03.2024.10

6. Kucherenko, O. I., & Vakaliuk, T. A. (2024). Klasyfikatsiia metodiv ta alhorytmiv pobudovy marshrutiv BpLA [Classification of UAV Route Construction Methods and Algorithms]. *Vcheni zapysky TNU im. V. I. Vernadskoho. Seriia: Tekhnichni nauky [Academic Notes of TNU named after V. I. Vernadskyi. Series: Technical Sciences.], Vol. 35* (74), № 3, 111–116. https://doi.org/10.32782/2663-5941/2024.3.1/18 [in Ukrainian].

7. Zhao, C., Liu, Y., Yu, L., & Li, W. (2021). Stochastic Heuristic Algorithms for Multi-UAV Cooperative Path Planning. In *Proceedings of the 2021 40th Chinese Control Conference (CCC).* Shanghai, China. July 26–28, 2021. (pp. 7677–7682). https://doi.org/10.23919/ccc52363.2021.9549984

8. Sun, W., & Hao, M. (2021). A Survey of Cooperative Path Planning for Multiple UAVs. In *Proceedings of the International Conference on Autonomous Unmanned Systems.* Shanghai, China. July 26–28, 2021. (pp. 189–196). https://doi.org/10.1007/978-981-16-9492-9_20

9. Tang, J., Duan, H., & Lao, S. (2022). Swarm Intelligence Algorithms for Multiple Unmanned Aerial Vehicles Collaboration: A Comprehensive Review. *Artif. Intell. Rev.,* 1–33. https://doi.org/10.1007/s10462-022-10281-7

10. Pohudina, O. K., Krytskyi, D. M., & Bykov, A. M. et al. (2021). *Metodolohiia formuvannia intelektualnoi skladovoi ahentnoi systemy roiu bezpilotnykh litalnykh aparativ : Monohrafiia [Methodology for Forming the Intellectual Component of the Agent System of a Swarm of Unmanned Aerial Vehicles: Monograph]*. Kharkiv [in Ukrainian].

11. Berezhnyi, A. O. (2020). *Metody ta informatsiina tekhnolohiia avtomatyzovanoho planuvannia marshrutiv polotiv bezpilotnykh litalnykh aparativ dlia pidvyshchennia efektyvnosti poshuku ob'iektiv: Dys. na zdobuttia nauk. stupenia kand. tekh. nauk za spets. 05.13.06 – Informatsiini tekhnolohii [Methods and Information Technology of Automated Planning of Flight Routes of Unmanned Aerial Vehicles to Increase the Efficiency of Object Search: PhD Dissertation in specialty 05.13.06 – Information Technologies]*. Kharkiv, Cherkasy [in Ukrainian].

12. Tymochko, O. I., Tristan, A. V., Chernavina, O. E., & Berezhny, A. O. (2020). Metod planuvannia marshrutu vedennia povitrianoi rozvidky dynamichnykh ob'iektiv z vykorystanniam bezpilotnykh litalnykh aparativ v lisostepovii mistsevosti [The Method of Planning the Route of Conducting Aerial Reconnaissance of Dynamic Objects Using Unmanned Aerial Vehicles in the Forest-Steppe Area]. *Systemy obrobky informatsii [Information Processing Systems], 3* (162), 95–110. https://doi.org/10.30748/soi.2020.162.10 [in Ukrainian].

13. Danyk, Yu. G., Puleko, I. V., Solovyov, O. V., Pozdnyakov, P. V. (2013). Obgruntuvannia zahalnykh vymoh do operatyvno-taktynykh ta taktychnykh bezpilotnykh aviatsiinykh kompleksiv [Justification of General Requirements for Operational-Tactical and Tactical Unmanned Aircraft Complexes]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system: zb.nauk. prats [Problems of Construction, Testing, Application and Operation of Complex Information Systems. Scientific journal of Korolov Zhytomyr Military Institute], 7,* 21–31. Zhytomyr [in Ukrainian].

14. Puleko, I. V. (2018). Informatsiina tekhnolohiia navihatsii maloho bezpilotnoho litalnoho aparata za optychnym polem Zemli v umovakh propadannia syhnaliv suputnykovykh

radionavihatsiinykh system [Information Technology of Navigation of a Small Unmanned Aerial Vehicle in the Optical Field of the Earth in Conditions of Loss of Signals of Satellite Radio Navigation Systems]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system : zb. nauk. prats [Problems of Construction, Testing, Application and Operation of Complex Information Systems. Scientific journal of Korolov Zhytomyr Military Institute]*, *15,* 118–129. Zhytomyr [in Ukrainian].

15. Weglarczyk, S. (2018). Kernel Density Estimation and its Application. In *ITM Web of Conferences, 23*, 00037. (pp. 1–8). https://doi.org/10.1051/itmconf/20182300037

I. V. Puleko, V. O. Chumakevych, I. M. Shestak, V. L. Rykun, I. V. Svystunovych

TARGET DENSITY FUNCTION FOR UAV PLANNING

The main problem of special aerial reconnaissance is the contradiction between the dimensions of the survey area and the dimensions of elementary objects (targets). Since the viewing area is very large, the size of the target is small, and the instantaneous field of view of the on-board equipment is limited, the time for obtaining data is quite significant and the amount of information to be processed is very large. Also, due to technical limitations on the time spent in the air and the limitations of the reconnaissance equipment, one UAV is not able to cover the entire area in one flight. The severity of this problem can be partially removed by using a group of UAVs. but both for one person and for a group, the task of planning the route of movement arises. A simple comb survey of the reconnaissance zone is far from optimal, and in practice route planning is used by points with the involvement of a priori information about the most likely locations of targets. However, this method is rather inconvenient for the automatic route planning of the UAV itself, since the point on the map usually does not correlate with the flight height, the instantaneous field of view of the on-board surveillance equipment, the scale and detail of the picture. In order to increase the optimization possibilities of automatic flight planning, it is suggested to use the target distribution density function (TDF).

The density function of the target distribution is a two-dimensional mathematical model that describes the conditional relative probability of finding targets at different points in space. It is created and set on the basis of a priori data about the terrain, previous observations or intellectual assessments, reflecting the distribution of possible targets in a certain area or for the entire reconnaissance area. TDF allows to model the space not as homogeneous, but as an area with different degrees of importance or probabilities of finding targets. It should be noted that obtaining mathematically justified or calculated by the theory of probability or mathematical statistics, two-dimensional discrete probability densities for randomly placed targets is actually impossible. Therefore, here the TDF is considered as an area with different degrees of review importance, which is reflected by conditional relative probabilities obtained from various sources, including expert evaluation.

Keywords: *aerial reconnaissance; unmanned aerial vehicles; probability density; density function of target distribution; reconnaissance zone; picture parameters.*

ISSN 2076-1546
УДК 358+531.8 DOI: 10.46972/2076-1546.2024.27.07

Н. П. Ісмаілова, І. С. Мікрюков, Л. Г. Бикова

ТЕХНІЧНЕ РІШЕННЯ ДЛЯ ПРОЄКТУВАННЯ СПРЯЖЕНИХ ЗУБЧАСТИХ ЗАЧЕПЛЕНЬ ЩОДО ВИЗНАЧЕННЯ ІНТЕРФЕРЕНЦІЇ В ОЗБРОЄННІ ТА ВІЙСЬКОВІЙ ТЕХНІЦІ

У складних реаліях сучасної промисловості України важливим напрямком науково-технічного розвитку є оптимізація технічних рішень для проєктування спряжених зубчастих зачеплень кінематичних пар щодо визначення інтерференції в озброєнні та військовій техніці з підвищеними вимогами до ступеня складності виробів, що проєктуються, і скорочення термінів виконання замовлень. Вплив кризових явищ в економіці та посилення конкурентної боротьби на ринку зумовлюють потребу в розробленні виробів на найсучаснішому технічному рівні.

У статті запропоновано оптимізацію аналітичного технічного рішення для проєктування лінії контакту між осями спряжених зубчастих зачеплень кінематичних пар для визначення інтерференції. Це дозволить у ході проєктування спряжених поверхонь зубчастих зачеплень привести рівняння до параметричної форми, алгоритмізувати та оптимізувати моделювання виробів в озброєнні та військовій техніці, а також спроєктувати контактну поверхню зачеплення.

Технічне вирішення порушеної проблеми належить до зубчастих спряжених механізмів зовнішнього зачеплення, форма зубів коліс яких утворюється огинанням початкового контуру зубчастої рейки, а кількість зубів визначається залежно від призначення механізму, необхідного передавального відношення та діаметральних розмірів. Такі механізми використовуються в різних вузлах й агрегатах озброєння та військової техніки, а саме у вигляді зубчастих коліс редукторів, лебідок, планетарних і хвильових передач та як робочі органи насосів, гідродвигунів, компресорів і двигунів внутрішнього згорання з прямими та гвинтовими зубами. Щоб уникнути інтерференції, на стадії проєктування необхідно проаналізувати технічні криволінійні характеристики спряжених поверхонь. Застосування технічних рішень для опису реальних поверхонь, одержуваних в результаті створення криволінійної моделі, відображає реальний фізичний процес із визначення інтерференції.

Ключові слова: *проєктування; кінематична пара; моделювання; інтерференція; оптимізація; зубчасте зачеплення; спряжена поверхня; технічне рішення; моделювання; параметризація; контактна лінія зачеплення.*

Постановка проблеми в загальному вигляді. На сьогодні в умовах складної економічної ситуації в сучасному воєнно-промисловому комплексі України, зумовленої воєнним станом, особливої значущості набуває проєктування виробів для озброєння та військової техніки. Зокрема оптимізації потребує технічне рішення щодо підвищення точності проєктування спряжених зубчастих зачеплень за умови відсутності інтерференції. Для розв’язання порушеної проблеми необхідно передусім дослідити

© Н. П. Ісмаілова, І. С. Мікрюков, Л. Г. Бикова, 2024

явища інтерференції в проєктуванні спряжених зубчастих зачеплень кінематичних пар, а також перетворення вихідної криволінійної контактної поверхні між профілями зубів [1], що, у свою чергу, дозволить виключити інтерференцію ще на стадії розроблення деталей для озброєння та військової техніки.

Аналіз останніх досліджень і публікацій. Завдання, пов'язані з інтерференцією, виникли з практики [2], тому їх вирішення має велику практичну цінність. Крім того, вони збагачують теорію спряжених зубчастих зачеплень, яка не мислима без своїх великих додатків. У дослідженні [3] надано нове визначення поняття інтерференції, а саме стверджується, що інтерференцією називається будь-який неправильний контакт профілів поза активними ділянками лінії зачеплення, тобто це явище, коли траєкторія кромки одного зуба у відносному русі перетинає профіль спряженого зуба. У ході вивчення технічних рішень у проєктуванні спряжених зубчастих механізмів кінематичних пар було встановлено [4], що відомі методи та способи мають певні складнощі в практичному застосуванні на виробництві й потребують високої кваліфікації виконавців [5]. Проте щодо інтерференції передбачалася побудова великої кількості аксоїдів [6], що робить відповідні дослідження недоцільними в практичному використанні [7]. У [8] проаналізовано переваги й недоліки найбільш поширених на практиці типів кінематичних пар зубчастих спряжених передач. Що стосується технічних рішень і можливостей у їх проєктуванні, то, як показано в працях [9, 10], на сучасному етапі розроблення контактної поверхні між профілями зубів, що визначає інтерференцію, є актуальним.

Формулювання завдання дослідження. Метою статті є оптимізація аналітичного технічного рішення щодо визначення контактної поверхні зачеплення спряжених кінематичних пар, що виключають інтерференцію. Це дозволить із високою точністю визначати інтерференцію ще на стадії проєктування та моделювання спряжених кінематичних пар зубчастих передач у військовій техніці та озброєнні.

Виклад основного матеріалу. Детально розглянемо аналітичне подання вимог, коли вектор $\bar{l}$ є напрямним вектором нормалі до кривої *K*. У такому разі достатньо, щоб скалярний добуток вектора $\bar{l}$ на вектор $\overline{T}$ дорівнював нулю:

$$\bar{l} \cdot \overline{T} = 0. \tag{1}$$

Підставляючи в (1) формули, отримаємо:

$$\left(\bar{t} l_t + \bar{n} l_n\right) \cdot \bar{t} \cdot \left(1 + \frac{dl_t}{dS} - \frac{l_n}{g}\right) + \left(\bar{t} l_t + \bar{n} l_n\right) \cdot \bar{n} \cdot \left(\frac{dl_t}{dS} - \frac{l_t}{g}\right) = l_t + l_t \frac{dl_t}{dS} + l_n \frac{dl_n}{dS} = 0.$$

Якщо $l_t = l\cos\alpha, l_n = l\sin\alpha,$ то попередня рівність набуде такого вигляду:

$$l\left(\cos\alpha + \cos\alpha \left(l\cos\alpha\right)'_s + \sin\alpha \left(l\sin\alpha\right)'_s\right) = 0. \tag{2}$$

Рівняння (2) виконується за $l = 0$, що добре узгоджується з концепцією векторного обчислення та свідчить про довільність напрямку нульового вектора [2]. Оскільки напрям

нульового вектора довільний, то останній можна вважати ортогональним до будь-якого вектора, зокрема й $\overline{T}$. Вираз у дужках у (2) можна значно спростити, урахувавши, що $S = R\varphi$, де R – радіус центроїди деталі, і продиференціювавши складну функцію:

$$\left(\cos\alpha + \cos\alpha\left(l\cos\alpha\right)'_s + \sin\alpha\left(l\sin\alpha\right)'_s\right) = \cos\alpha + \frac{1}{R}\left(l\cos\alpha\right)'_\varphi \cos\alpha + \frac{1}{R}\left(l\sin\alpha\right)'_\varphi \sin\alpha = 0.$$

Підвівши до спільного знаменника й урахувавши, що $R \neq 0$, отримаємо

$$R\cos\alpha + \left(l\cos\alpha\right)'_s \cos\alpha + \left(l\sin\alpha\right)'_s \sin\alpha = 0.$$

Виконавши операцію диференціювання, маємо

$$R\cos\alpha + \left(l'_\varphi \cos\alpha - l\sin\alpha\cdot\alpha'_\varphi\right)\cos\alpha + \left(l'_\varphi \sin\alpha + l\cos\alpha\cdot\alpha'_\varphi\right)'_s \sin\alpha = 0.$$

Розкривши дужки та скоротивши подібні члени рівняння, отримали

$$l'_\varphi + R\cos\alpha = 0. \qquad (3)$$

Рівність (3) або $l = 0$ є необхідною умовою того, що $\overline{l}\cdot\overline{T} = 0$. Якщо виконати всі обчислення у зворотному порядку, то прийдемо до рівності $\overline{l}\cdot\overline{T} = 0$. У такому разі рівність (3) або $l = 0$ є необхідною і достатньою умовою того, що вектор $\overline{l}$ є напрямним вектором нормалі до кривої *K*.

Назвемо центральною точкою профілю *K* точку нормалі, у якій через центр центроїди *C* проходить точка *O* (рис. 1).

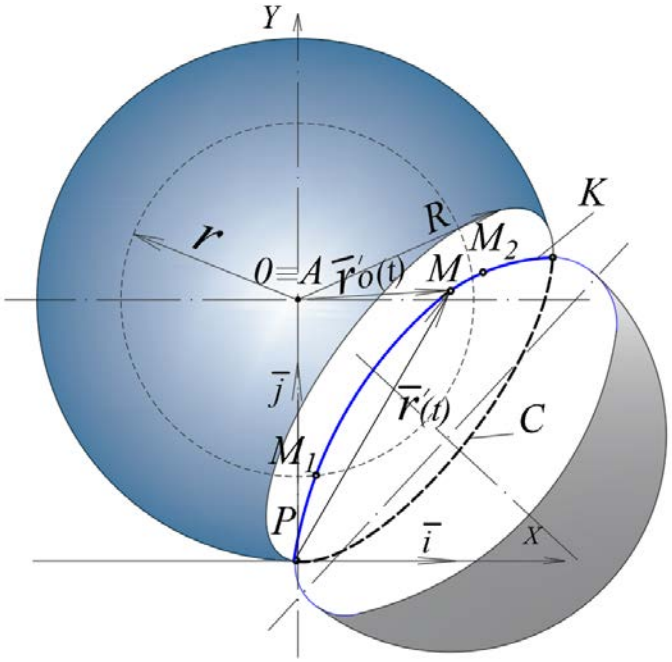


Рис. 1. Коло із центром у центрі центроїди

На практиці найчастіше використовують такі профілі, у яких коло із центром у центрі центроїди перетинає їх двічі (див. рис. 1), це точки M_1 і M_2[3]. Доведемо, що у таких профілях завжди є центральна точка.

Профіль заданий рівняннями в параметричному вигляді:

$$x = x(t),$$

$$y = y(t),$$

де t – деякий параметр.

Тоді $\bar{r}(t) = \bar{i}x(t) + \bar{j}y(t)$;

$$\bar{r}(t) = \bar{r}'(t) - \bar{j}R = \bar{i}x(t) + \bar{j}\left(y(t) - R\right).$$

Векторну функцію скалярного аргументу $\bar{r}(t)$ можна записати в такому вигляді:

$$\bar{r}(t) = \bar{r}(t) \cdot \bar{r}_0(t), \tag{4}$$

де $r(t)$ – модуль вектора $\bar{r}(t)$;

$\bar{r}_0(t)$ – одиничний вектор вектора $r(t)$.

Оскільки точки M_1 і M_2 належать одному колу, то $r(t_1) = r(t_2) = r,$ де r – радіус кола, що проходить через точки M_1 і M_2, t_1 і t_2 – значення параметрів, які відповідають точкам M_1 і M_2.

Розглянемо функцію $r(t)$, вона скалярна, до неї застосовані теореми аналітичного аналізу. Звернемося до теореми Ролля, яка формулюється таким чином: якщо функція $f(x)$ неперервна на інтервалі $(a,b),$ має похідну в кожній точці всередині цього інтервалу, а значення функції на кінцях цього інтервалу рівні, тобто $f(a) = f(b),$ то всередині проміжку є значення $x = C,$ за якого похідна звертається в нуль, тобто $f'(C) = 0.$

Оскільки крива *K* є гладкою, то функція $r(t)$ задовольняє теорему.

Отже, є значення $t_0\left(t_1 \le t \le t_2\right),$ у якому $\frac{dr}{dt} = 0.$ Продиференціюємо (4) за t:

$$\frac{d\bar{r}}{dt} = \frac{dr}{dt}\bar{r}_0 + r\frac{d\bar{r}_0}{dt}.$$

Якщо $t = t_0$, то остання рівність набуде такого вигляду:

$$\left.\frac{d\bar{r}}{dt}\right|_{t=t_0} = r(t_0) \cdot \left.\frac{d\bar{r}_0}{dt}\right|_{t=t_0}. \tag{5}$$

Оскільки $\frac{d\bar{r}}{dt}\Big|_{t=t_0}=0,$ то вектор $\frac{d\bar{r}}{dt}$ є напрямним вектором дотичної і, як випливає з (3), у разі $t=t_0$ він колінеарний вектору $\frac{d\bar{r}_0}{dt}$. Через те, що вектор $\bar{r}_0(t)$ одиничний, $\frac{d\bar{r}_0}{dt}$ йому ортогональний [2], це означає, що $\bar{r}_0(t)$ ортогональний $\frac{d\bar{r}}{dt}\Big|_{t=t_0}$. Оскільки $\bar{r}_0(t)$ – вектор, що йде з точки *O*, а $\frac{d\bar{r}}{dt}\Big|_{t=t_0}$ спрямовує вектор дотичної до кривої *K*, то вектор $\bar{r}_0(t)$ є напрямним вектором нормалі до кривої *K* у точці, що відповідає $t=t_0$, і нормаль у цій точці проходить через центр центроїди *C*. Отже, теорема про наявність центральної точки на гладкому профілі доведена.

Також привертає увагу будова лінії зачеплення в точці, що відповідає центральній точці профілю. Оскільки вектор $\bar{r}_0(t)$ виходить із точки *A*, то пряма, яка проходить через *O* та має своїм напрямним вектором $\bar{r}_0(t)$, буде нормаллю не тільки до профілю, а й до центроїди (центроїда *C* – коло радіусом *R* із центром у точці *O*), тоді кут $\alpha=0,5\pi.$ У разі побудови лінії зачеплення точка, що відповідає центральній, належатиме осі *y*. Розглянемо напрямок дотичної до лінії зачеплення в цій точці. Відповідно до рівняння (5) напрямний вектор дотичної до лінії зачеплення з урахуванням того, що $S=R\varphi,$ буде таким:

$$\overline{T_л}=\bar{t}\left(l_t\right)'_\varphi\frac{1}{R}+\bar{n}\left(l_n\right)'_\varphi\frac{1}{R}$$

або

$$\overline{T_л}=\bar{t}\left(l\cos\alpha\right)'_\varphi\frac{1}{R}+\bar{n}\left(l\sin\alpha\right)'_\varphi\frac{1}{R}.$$

Якщо лінію зачеплення будувати в точці *P* (рис. 1), то замість $\bar{t}$ і $\bar{n}$ братимемо $\bar{i}$ та $\bar{j}$. Крім того, якщо ввести вектор $\overline{T'}_л=\overline{T_л}R,$ то формула для напрямного вектора дотичної до лінії зачеплення набуде такого вигляду:

$$\overline{T_л}=\bar{i}\left(\cos\alpha\right)'_\varphi+\bar{j}\left(l\sin\alpha\right)'_\varphi. \qquad (6)$$

Оскільки

$$\left(l\cos\alpha\right)'_\varphi=l'_\varphi\cos\alpha-l\sin\alpha\cdot\alpha'_{\varphi'}\left(l\sin\alpha\right)'_\varphi=l'_\varphi\sin\alpha+l\cos\alpha\cdot\alpha'_\varphi,$$

то, враховуючи те, що $\cos\left(0,5\pi\right)=0,$ отримуємо із (6) у точці $t=t_0$

$$\overline{T'_л}=\bar{i}\left(-l\cdot\alpha'_\varphi\right)+\bar{j}\left(0\right). \qquad (7)$$

Із наведеного вище виразу (7) маємо, що дотична до лінії зачеплення в точці, яка відповідає центральній, перпендикулярна осі *y* (паралельна осі *x*). Якщо $\alpha'_\varphi = 0,$ то напрямок вектора $\overline{T'_л}$ стає невизначеним. Для знаходження кута нахилу дотичної можна скористатися правилом Лопіталя:

$$tg\delta = \frac{\left(l\sin\alpha\right)'_\varphi}{\left(l\sin\alpha\right)'_\varphi}.$$

У такий спосіб приходимо до висновку, що і в цьому разі дотична перпендикулярна за віссю *y*. За цих умов можна навести і більш наочні міркування. Продиференціюємо вираз (2) за φ:

$$l''_\varphi = R\sin\alpha\frac{d\alpha}{d\varphi}.$$

Звідси випливає, що $\frac{d\bar{r}}{dt}\Big|_{t=t_0}$, тобто $\alpha'_\varphi = 0,$ коли $l''_\varphi = 0.$ З точністю до нескінченно малого третього порядку крива може бути подана дотичним колом. У зв'язку із цим ми можемо стверджувати, що центральна точка не є особливою (профіль деталі взагалі не містить особливих точок). Тоді можна розглядати три основні варіанти: перший, коли дуга кривої поблизу центральної точки описується дугою кола із центром всередині центроїди, а другий варіант – поза центроїдою (ці два варіанти характеризують точки основного типу). Дуга кривої поблизу центральної точки описується двома дотичними колами, центри яких розташовані по різні боки від дотичної в центральній точці (цей варіант придатний для точок перегину). Необхідно відзначити, що профіль може містити точки перегину з розривом за кривизною, саме для цих точок і наведемо третій варіант: якщо на профілі виникає точка перегину (кривизна дорівнює нулю), то її можна розглядати як граничний випадок точки перегину з розривом за кривизною. Для першого варіанта $l = l\left(\varphi\right)$ при $\alpha = 0,5\pi$ (центральна точка) має мінімум і $l''_\varphi < 0,$ для другого – максимум і $l''_\varphi < 0.$

Якщо маємо власну точку перегину, то радіуси малих дуг кіл нескінченно зростають і зливаються в малому з відрізком дотичної в центральній точці. Цей граничний випадок не несе змін до твердження, що дотична до лінії зачеплення в точці, яка відповідає центральній, перпендикулярна осі *y*. Випадок $l = 0$ також призводить до невизначеності, однак рівність нулю величини *l* в центральній точці на практиці не зустрічається, крім того, розглядаючи граничний перехід $l \to 0$, прийдемо до того ж результату. Щодо рівності $l = 0$, то необхідно відзначити, що сама по собі вона зустрічається дуже часто, але не в центральній точці. Тоді лінія зачеплення проходить через полюс *P* і перетинає вісь під кутом, який визначали за допомогою правила Лопіталя.

Кут, який отримано, залежить від співвідношення вищих похідних від проєкцій вектора $\overline{T'_л}$ за φ. Так, наприклад, для евольвентного профілю лінією зачеплення є пряма,

яка проходить через точку з довільним кутом нахилу до осі x. Евольвентний профіль не має центральної точки в тому сенсі, у якому ми її вище визначили, хоча і перетинається двічі колами, що мають своїм центром центр центроїди *C*. Таке відбувається, тому що евольвентний профіль не є гладким, він містить особливу точку повернення першого порядку.

Дослідимо можливість виникнення на ній особливих точок та уявімо, що на лінії зачеплення є особлива точка, тоді вектор $\overline{T_л'}$ невизначений і його проєкції на осі координат дорівнюють нулю:

$$\left(l\cos\alpha\right)'_{\varphi} = \left(l\sin\alpha\right)'_{\varphi} = 0.$$

Вектор $\overline{T_л'}$ має такий вигляд:

$$\overline{T} = \bar{t}\left(1+\frac{d\bar{t}}{dS}-\frac{l_n}{q}\right)+\bar{n}\frac{dl_n}{dS}+\frac{l_t}{q}.$$

Враховуючи, що $l_t = l\cos\alpha,\ l_n = l\sin\alpha,\ S = R\varphi,\ q = R,$ радіус кривизни центроїди *C*, спряженої з вихідним профілем з останньої формули, отримаємо

$$\overline{T} = \bar{t}\left(1+\left(l\cos\alpha\right)'_{\varphi}\right)\frac{1}{R}-\left(l\sin\alpha\right)\frac{1}{R}+\bar{n}\left(l\sin\alpha\right)'_{\varphi}\frac{1}{R}+\left(l\cos\alpha\right)\frac{1}{R}.$$

Якщо вектор $\overline{T'} = \overline{T}R$, то напрямний вектор дотичної до профілю матиме такий вигляд:

$$\overline{T}' = \bar{t}\left(R+\left(l\cos\alpha\right)'_{\varphi}-l\sin\alpha\right)+\bar{n}\left(\left(l\sin\alpha\right)'_{\varphi}+\left(l\cos\alpha\right)\right). \qquad (8)$$

У разі появи особливої точки на лінії зачеплення вираз (8) набуде такого вигляду:

$$\overline{T'} = \bar{t}\left(R-l\cos\alpha\right)+\bar{n}\left(l\cos\alpha\right).$$

Оскільки $\left(l\cos\alpha\right)'_{\varphi} = \left(l\sin\alpha\right)'_{\varphi} = 0,$ то вектор $\bar{l}$ у тій же системі координат, заданій ортами $\bar{l}$ і $\bar{n}$, має такий вигляд:

$$\bar{l} = \bar{t}l_t+\bar{n}l_n = \bar{t}\left(l\cos\alpha\right)+\bar{n}\left(l\sin\alpha\right).$$

Запишемо вираз скалярного добутку векторів $\overline{T'}$ і $\bar{l}$ у точці профілю, що відповідає особливій точці на лінії зачеплення:

$$\overline{T'}\cdot\bar{t} = \left(R-l\sin\alpha\right)\left(l\cos\alpha\right)+\left(l\cos\alpha\right)\left(l\sin\alpha\right) = Rl\cos\alpha. \qquad (9)$$

Оскільки $\bar{l}$ – напрямний вектор нормалі до профілю, то

$$\bar{T} \cdot \bar{l} = 0. \tag{10}$$

З виразу (9) випливає, що рівняння (10) виконується, якщо $\bar{l} = 0,$ тобто в точці лінії зачеплення, що збігається з полюсом *P*, або якщо $\cos\alpha = 0,$ тобто в точці, що відповідає центральній точці профілю. Припустимо, що на лінії зачеплення крім точок, які належать осі *y*, є точки, що відповідають центральній точці профілю (дотична до лінії зачеплення в цій точці перпендикулярна осі *y*, відповідно, може виникнути тільки точка повернення), і ті точки, що збігаються з *P*. Отже, лише саме в цих точках лінія зачеплення може мати особливі точки, які можуть вказувати на виникнення інтерференції, інші ж точки лінії зачеплення звичайні. Якщо $\left(l\cos\alpha\right)'_{\varphi}$ і $\left(l\sin\alpha\right)'_{\varphi}$ не обертаються в нуль одночасно, то на лінії зачеплення може виникнути точка перегину.

Висновки. У результаті проведеного дослідження оптимізовано аналітичне технічне рішення, визначено особливі точки та точку перегину контактної поверхні зачеплення спряжених кінематичних пар, які можуть викликати інтерференцію. Звідси випливає, що в точках перегину, які виникли в точці, що відповідає центральній точці *P*, є рівність нулю перших похідних $\left(l\cos\alpha\right)'_{\varphi}$ і $\left(l\sin\alpha\right)'_{\varphi}$, а відмінною від нуля є похідна радіуса-вектора непарного порядку. В інших точках лінії зачеплення може виникнути точка перегину, яка характеризується тим, що $\left(l\cos\alpha\right)'_{\varphi}$ і $\left(l\sin\alpha\right)'_{\varphi}$ нерівні нулю одночасно.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Podkorytov A. Theoretical Bases of Conjugate Quazihelical Surfaces, Excluding Interference // 10th Intern. Conf. on Engineering Design Graphios and Descriptive Geometry. Texas, USA, Austin. 2002. Vol. 1. P. 43–47.

2. Подкоритов А. М., Ісмаілова Н. П. Загальний ітераційній метод виключення інтерференції спряжених квазігвинтових поверхонь // Сучасні проблеми моделювання. Мелітополь : Мелітопольський держ. пед. ун-т, 2016. Вип. 5. С. 98–103. URL: http://magazine.mdpu.org.ua/index.php/spm/article/view/1488 (дата звернення: 01.10.2024).

3. Подкоритов А. М. Ітераційний метод та алгоритм виключення інтерференції складних спряжених поверхонь за наперед заданими умовами // Прикладна геометрія та інженерна графіка. Міжвідомча наук.-техніч. збірка. Київ : КНУБА, 2000. Вип. 64. С. 109–113.

4. A Model to Determine Mesh Characteristics in a Gear Pair with Tooth Profile Error / Qibin Wang, Peng Hu, Yimin Zhang et al. // Follow Journal. October 2014. Advances in Mechanical Engineering 2014:1-10. URL: https://www.researchgate.net/scientific-contributions/Peng-Hu-2068779212 (last accessed: 15.10.2024).

5. Development of the Method for the Formation of One-Dimensional Contours by the Assigned Interpolation Accuracy / Y. Havrylenko, Y. Kholodniak, O. Vershkov, A. Naidysh // Eastern-

European Journal of Enterprise Technologies. 2018. Vol. 1, Iss. 4 (91). P. 76–82. https://doi.org/10.15587/1729-4061.2018.123921
6. Jacob D., Ramana K., Rao P. Automated Manufacturability Assessment of Rotational Parts by Grinding // International Journal of Production Research. 2004. Vol. 42 (3). P. 505–519. https://doi.org/10.1080/00207540310001613674
7. Saghafi A., Farshidianfar A. An Analytical Study of Controlling Chaotic Dynamics in a Spur Gear System // Mechanism and Machine Theory. February 2016. Vol. 96, Iss. 1. P. 179–191. https://doi.org/10.1016/j.mechmachtheory.2015.10.002
8. Farshidianfar A., Saghafi A. Identification and Control of Chaos in Nonlinear Gear Dynamic Systems Using Melnikov Analysis // Phys. Lett. Sect. A Gen. At. Solid State Phys. 2014. Vol. 378. P. 3457–3463. https://doi.org/10.1016/j.physleta.2014.09.060
9. Linkage Model and Manufacturing Process of Shaping Non-Circular Gears / Fangyan Zheng, Lin Hua, Xinghui Han et al. // Mechanism and Machine Theory. February 2016. Vol. 96, Iss. 1. P. 192–212. https://doi.org/10.1016/j.mechmachtheory.2015.09.010
10. Ismailova N., Bogach V., Lebedev B. Development of a Technique for the Geometrical Modeling of Conjugated Surfaces when Determining the Geometrical Parameters of an Engagement Surface Contact in Kinematic Pairs // Eastern-European Journal Of Enterprise Technologies. Kharkiv: Technology Center, 2020. № 1/4 (106). P. 17–22. https://doi.org/10.15587/1729-4061.2020.209108
11. Ismailova N. P., Mohylyanets T. M., Oliynyk N. V. Graphoanalytical Profiling of Conjugate Curvilinear Surfaces of a Cutting Tool // Collection of Scientific Works of the Military Academy (Odesa). 2023. № 1 (19). P. 23–28. https://doi.org/10.37129/2313-7509.2023.19.23-28

Стаття надійшла до редакції 19.11.2024.

REFERENCES

1. Podkorytov, A. (2002). Theoretical Bases of Conjugate Quazihelical Surfaces, Excluding Interference In *10th Intern. Conf. on Engineering Design Graphios and Descriptive Geometry, Vol. 1*. (pp. 43–47). Texas, USA, Austin.
2. Podkorytov, A. M., & Ismailova, N. P. (2016). Zahalnyi iteratsiinii metod vykliuchennia interferentsii spriazhenykh kvazihvyntovykh poverkhon [General Iterative Method for Eliminating Interference of Conjugate Quasi-Helical Surfaces]. *Suchasni problemy modeliuvannia [Modern Problems of Modeling], 5*, 98–103. Melitopol. Retrieved from http://magazine.mdpu.org.ua/index.php/spm/article/view/1488 [in Ukrainian].
3. Podkorytov, A. M. (2000). Iteratsiinyi metod ta alhorytm vykliuchennia interferentsii skladnykh spriazhenykh poverkhon za napered zadanymy umovamy [Iterative Method and Algorithm for Eliminating Interference of Complex Conjugate Surfaces under Predetermined Conditions]. *Prykladna heometriia ta inzhenerna hrafika. Mizhvidomcha nauk.-tekhnich. zbirka [Applied Geometry and Engineering Graphics. Interdepartmental Scientific and Technical Collection], 64*, 109–113. Kyiv [in Ukrainian].
4. Qibin Wang, Peng Hu, & Yimin Zhang et al. (2014). A Model to Determine Mesh Characteristics in a Gear Pair with Tooth Profile Error. *Follow Journal. Advances in Mechanical*

Engineering. Retrieved from https://www.researchgate.net/scientific-contributions/Peng-Hu-2068779212

5. Havrylenko, Y., Kholodniak, Y., Vershkov, O., & Naidysh, A. (2018). *Development of the Method for the Formation of One-Dimensional Contours by the Assigned Interpolation Accuracy. Eastern-European Journal of Enterprise Technologies, Vol. 1,* Iss. 4 (91), 76–82. https://doi.org/10.15587/1729-4061.2018.123921

6. Jacob, D., Ramana, K., Rao, P. (2004). Automated Manufacturability Assessment of Rotational Parts by Grinding. *International Journal of Production Research, 42* (3), 505–519. https://doi.org/10.1080/00207540310001613674

7. Saghafi A., Farshidianfar A. An Analytical Study of Controlling Chaotic Dynamics in a Spur Gear System // Mechanism and Machine Theory. February 2016. Vol. 96, Iss. 1. P. 179–191. https://doi.org/10.1016/j.mechmachtheory.2015.10.002

8. Farshidianfar, A., & Saghafi, A. (2014). Identification and Control of Chaos in Nonlinear Gear Dynamic Systems Using Melnikov Analysis. *Phys. Lett. Sect. A Gen. At. Solid State Phys., 378*, 3457–3463. https://doi.org/10.1016/j.physleta.2014.09.060

9. Fangyan Zheng, Lin Hua, Xinghui Han, Bo Li, & Dingfang Chen. (2016). Linkage Model and Manufacturing Process of Shaping Non-Circular Gears. *Mechanism and Machine Theory, Vol. 96,* Iss. 1, 192–212. https://doi.org/10.1016/j.mechmachtheory.2015.09.010

10. Ismailova, N., Bogach, V., & Lebedev, B. (2020). Development of a Technique for the Geometrical Modeling of Conjugated Surfaces when Determining the Geometrical Parameters of an Engagement Surface Contact in Kinematic Pairs. *Eastern-European Journal Of Enterprise Technologies, 1/4* (106), 17–22. Kharkiv. https://doi.org/10.15587/1729-4061.2020.209108

11. Ismailova, N. P., Mohylyanets, T. M., & Oliynyk, N. V. (2023). Graphoanalytical Profiling of Conjugate Curvilinear Surfaces of a Cutting Tool. *Collection of Scientific Works of the Military Academy (Odesa), 1* (19), 23–28. https://doi.org/10.37129/2313-7509.2023.19.23-28

N. P. Ismailova, I. S. Mikryukov, L. G. Bykova

TECHNICAL SOLUTION IN DESIGNING COUPLED GEAR ENGAGEMENTS REGARDING THE DETERMINATION OF INTERFERENCE IN WEAPONS AND MILITARY TECHNIQUES

In the complex realities of the modern industry of Ukraine, an important direction of scientific and technical development is the optimization of technical solutions in the design of coupled gears of kinematic pairs regarding the determination of interference in weapons and military equipment with increased requirements for the degree of complexity of the designed products and shortening the terms of order fulfillment. Given the serious pressure of crisis phenomena in the economy and increased competition on the market, these components force us to carry out work at the most modern technical level.

The paper proposes the optimization of the analytical technical solution for designing the contact line between the axes of the coupled gear engagements of kinematic pairs to determine the interference. This will make it possible to reduce the equation to a parametric form, to

algorithmize and optimize the modeling of the product, and to design the contact surface of the gear when designing products in weapons and military equipment.

The technical solution to the given problem refers to gear-coupled mechanisms of external engagement, the shape of the teeth of the wheels is formed by wrapping the initial contour of the gear rack, and the number of teeth is determined depending on the purpose of the mechanism, the required gear ratio and diametrical dimensions. Such mechanisms are used in various units and units of weapons and military equipment, namely in the form of gear wheels of reducers, winches, planetary and wave gears and as working bodies of pumps, hydraulic motors, compressors and internal combustion engines with straight and helical teeth. To avoid interference at the design stage, it is necessary to analyze the technical curvilinear characteristics of the conjugated surfaces. The application of technical solutions for the description of real surfaces obtained as a result of the creation of a curvilinear model reflects the real physical process of determining interference.

Keywords*: design; kinematic couples; modeling; interference; optimization; gear engagement; conjugated surfaces; technical solution; modeling; parameterization; contact line of engagement.*

УДК 623.618:004.932 DOI: 10.46972/2076-1546.2024.27.08

С. В. Тимчук, В. О. Тарасенко

АНАЛІЗ МЕТОДІВ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ ТА ЇХ КЛАСИФІКАЦІЯ

В умовах російсько-української війни виникають нові складнощі для ведення радіоелектронної розвідки. Радіочастотний спектр насичений різноманітними типами сигналів, а сучасні засоби зв'язку мають високий рівень захищеності. Більшість зразків озброєння автоматично розпізнають сигнали за рахунок вимірювання їх параметрів, однак через низьке відношення сигнал-шум цей процес може бути ускладненим. Крім того, майже усі сучасні засоби радіоелектронної розвідки відображають спектрограми, на яких можна чітко визначити сигнал. З урахуванням широкого застосування технологій розпізнавання зображень у різних галузях важливо вивчити наявний досвід, розглянути методи та способи цього процесу й дослідити можливість їх використання для розв'язання проблеми розпізнавання сигналів.

Сучасні алгоритми штучного інтелекту забезпечують аналіз великих обсягів даних із використанням методів машинного навчання. Особливу увагу приділено можливостям глибоких нейронних мереж, які демонструють високі результати у вирішенні складних завдань. Це відкриває нові перспективи для їх застосування у військовій сфері. Підходи, що ґрунтуються на аналізі даних із використанням спектрограм, дозволяють досягати високої точності розпізнавання навіть у складних умовах. Розробка інноваційних методів обробки сигналів є важливою складовою зміцнення обороноздатності держави.

У статті досліджено можливості штучного інтелекту з особливим акцентом на ролі комп'ютерного зору в цій сфері. Проведено класифікацію методів розпізнавання зображень за схемою, розробленою на основі відомих підходів. Крім того, проаналізовано основні етапи комп'ютерного зору, їх функціональні складові та зміст. Окрему увагу приділено методам розпізнавання образів, зокрема їх трьом основним типам, проаналізовано їх переваги та недоліки. У публікації наведено практичні приклади реалізації зазначених методів. Завершальним етапом дослідження став вибір методу для подальших експериментальних і теоретичних досліджень.

Ключові слова: *радіоелектронна розвідка; радіочастотний спектр; сигнали; розпізнавання сигналів; методи розпізнавання зображень.*

Постановка проблеми в загальному вигляді. Швидкість та точність оброблення сигналів є критично важливими для забезпечення переваги в сучасних конфліктах. Застосування технологій комп'ютерного зору в розпізнаванні сигналів відкриває можливості для автоматизації процесів аналізу даних і підвищення ефективності роботи радіоелектронних засобів. Реалізовані в різноманітних засобах радіоелектронної розвідки (РЕР) підходи до розпізнавання сигналів ґрунтуються на вимірюванні їх параметрів та зіставленні з еталонними описами. Однак такий підхід не завжди дозволяє реалізувати процес розпізнавання в режимі часу, близькому до реального. Водночас значного розвитку

© С. В. Тимчук, В. О. Тарасенко, 2024

на сьогодні набули методи комп'ютерного зору, які дозволяють синхронно вирізняти різні об'єкти на зображеннях, тому актуальним є завдання реалізації цих методів для здійснення розпізнавання сигналів радіоелектронних засобів та систем зв'язку.

Аналіз останніх досліджень і публікацій. Тематика розпізнавання зображень на сьогодні є актуальною в різних сферах, зокрема у виробництві, наукових дослідженнях та військовій галузі. Вудс Р., Гонсалес Р. у книзі «Цифрова обробка зображень» [1] надають загальний аналіз алгоритмів та застосувань комп'ютерного зору, що є основою для багатьох сучасних методів розпізнавання зображень.

Форсайт Д. А., Понсе Дж. [2] описують сучасні підходи до розпізнавання зображень за допомогою комп'ютерних технологій, підкреслюючи важливість їх упровадження в практику.

Різні автори класифікують методи розпізнавання зображень залежно від поставлених завдань. Наприклад, у [3] наведено класифікацію методів для розпізнавання у відеопотоці. У статті [4] проаналізовано методи розпізнавання кольорових зображень та запропоновано схему їх загальної класифікації. Публікація [5] містить детальний аналіз нейронних мереж (НМ), а автор [6] виділяє чотири основні групи методів розпізнавання зображень.

Проте загальної класифікації методів, яка б відповідала вирішенню проблем, описаних у цій статті, немає. У [7] розглянуто подібну проблему, однак ведення РЕР має свою специфіку, тому слід зазначити, що питання використання методів розпізнавання зображень у РЕР досліджено недостатньо.

Формулювання завдання дослідження. Для вдосконалення процесу розпізнавання сигналів у системах РЕР необхідна така класифікація методів розпізнавання зображень, яка враховуватиме специфічні вимоги РЕР і забезпечуватиме високу точність та швидкість розпізнавання сигналів у складних умовах експлуатації. Це передбачає дослідження сучасних методів комп'ютерного зору та їх можливостей для розпізнавання сигналів у радіочастотному спектрі, а також розробку класифікації методів розпізнавання зображень на основі відомих підходів і технологій. Важливим етапом є аналіз основних стадій та функціональних компонентів методів комп'ютерного зору, зокрема їх переваг і недоліків. Практичні приклади застосування цих методів у контексті розпізнавання сигналів РЕР дозволять оцінити їхню ефективність і визначити оптимальні підходи. У підсумку метою статті є вибір найбільш ефективного методу для подальших теоретичних та експериментальних досліджень, що сприятиме підвищенню ефективності процесу розпізнавання сигналів у режимі реального часу.

Виклад основного матеріалу. Дослідження розпізнавання зображення доцільно почати з вивчення галузі штучного інтелекту (ШІ) та напрямків, які він охоплює, оскільки ці знання забезпечать фундаментальне розуміння основних принципів і технологій, що використовуються в системах розпізнавання зображень. ШІ – це властивість автоматичних систем брати на себе окремі функції інтелекту людини, наприклад, вибирати й ухвалювати оптимальні рішення на основі раніше одержаного досвіду й раціонального аналізу зовнішніх чинників [8]. ШІ як міждисциплінарна сфера включає в себе машинне навчання, обробку природнього мовлення, комп'ютерний зір,

робототехніку та експертні системи, що є критично важливими для розробки й упровадження ефективних методів оброблення та аналізу візуальної інформації. Дослідження цих сфер дозволяє краще зрозуміти алгоритми та моделі, які застосовуються в розпізнаванні образів, їх переваги та обмеження, а також вплив на практичні додатки в системах РЕР.

Комп'ютерний зір (або машинний зір) – це галузь ШІ, що займається розробкою теоретичних й алгоритмічних основ для автоматичного отримання, оброблення та аналізу зображень. Основна ідея – навчити машини «бачити» та інтерпретувати візуальну інформацію так само, як це робить людина. Комп'ютерний зір включає в себе декілька ключових етапів, кожен із яких є важливим для досягнення повного розуміння та інтерпретації зображень чи відео [9]. Розглянемо основні етапи комп'ютерного зору.

Збір даних – отримання зображень або відео завдяки використанню камер, сенсорів або інших пристроїв для збору візуальних даних.

Попередня обробка зображень – це їх корекція (усунення шумів, нормалізація освітлення, корекція перспективи), а також фільтрація (використання фільтрів для покращення якості зображень).

Сегментація зображень – їх поділ на сегменти (розбиття на кілька частин для полегшення аналізу).

Аналіз та інтерпретація передбачають класифікацію (визначення категорії, до якої належить зображення або об'єкт на ньому) та розпізнавання зображення (ідентифікація та локалізація об'єктів на ньому).

Постоброблення та візуалізація – це аналіз отриманих результатів; їх оцінювання, виявлення помилок та оптимізація моделей, а також візуалізація, яка полягає в наданні результатів у зручному для користувача вигляді, наприклад, накладання розпізнаних об'єктів на зображення.

Окрім того, слід розглянути розпізнавання образів у контексті комп'ютерного зору, оскільки цей підхід дозволяє вирішувати широкий спектр завдань, пов'язаних із автоматичною інтерпретацією візуальної інформації.

Розпізнавання образів є математичним фундаментом розпізнавання зображень, адже саме на основі теорії розпізнавання образів розробляються алгоритми та моделі, що забезпечують здатність комп'ютера відрізняти один об'єкт від іншого. Ця теорія базується на таких математичних принципах, як: статистика, лінійна алгебра, оптимізація, теорія ймовірностей, що дозволяють здійснювати класифікацію об'єктів на основі їх характеристик. Образом може бути цифрова фотографія (розпізнавання зображень), буква або цифра (розпізнавання символів), запис мовлення (розпізнавання мови) тощо.

Для реалізації основних принципів побудови автоматичних систем розпізнавання образів є три основні типи методів: евристичні, математичні та лінгвістичні (синтаксичні). Нерідко системи розпізнавання створюються на основі комбінації цих методів [10]. Розглянемо їх детальніше.

Евристичні методи розпізнавання образів – це група методів, які ґрунтуються на знаннях та досвіді людини, а не на формальних математичних моделях. Вони використовують набори правил, логічних висновків та інтуїтивних уявлень для класифікації образів.

Математичні методи розпізнавання образів базуються на формальних математичних моделях для подання (опису) та класифікації образів. Цей підхід використовує принципи математичної статистики, теорії прийняття рішень, ШІ та інших галузей математики для розроблення алгоритмів, які можуть автоматично класифікувати та інтерпретувати візуальну інформацію.

Лінгвістичні методи (також відомі як синтаксичні) використовують для розпізнавання образів шляхом опису їх структури та взаємозв'язків елементів, подібно до опису речень у мові. Основні принципи цих методів:

розподіл образу на складові (базові компоненти), які називають непохідними елементами;

граматика образів: створюється формальна граматика, яка описує правила комбінування та зв'язку непохідних елементів для формування допустимих образів;

аналіз та розпізнавання: за допомогою граматики й алгоритмів аналізу образ розпізнається та класифікується.

З урахуванням напрямків ШІ, а також основних етапів комп'ютерного зору та методів розпізнавання образів пропонуємо класифікацію розпізнавання зображення (рис. 1).

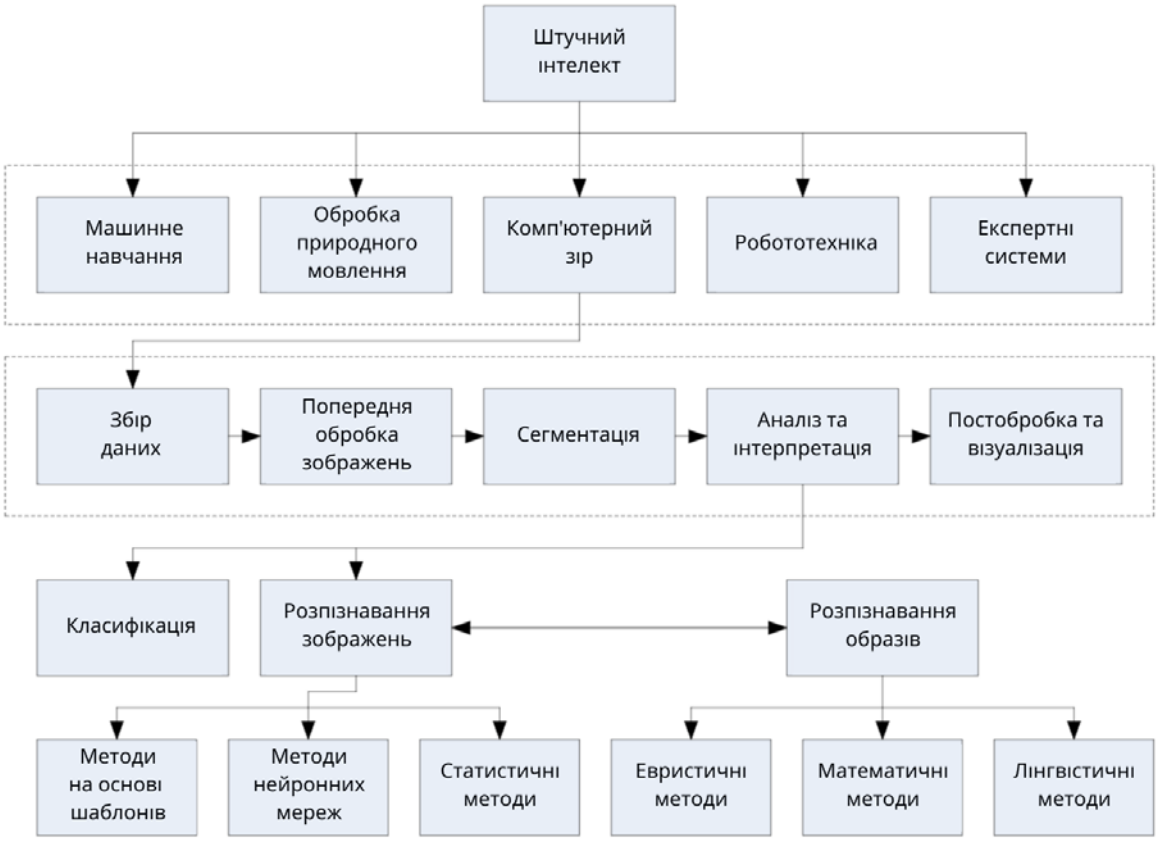


Рис. 1. Схема класифікації методів розпізнавання образів і зображень, а також їх зв'язок зі ШІ

Відповідно до наведеної схеми розглянемо найважливіший етап – розпізнавання зображення, яке ґрунтується на принципах розпізнавання образів, але використовує спеціалізовані методи й алгоритми, оптимізовані для роботи з візуальними даними.

Розпізнавання зображень – це розділ сучасного ШІ, який дозволяє комп'ютерам ідентифікувати візерунки чи об'єкти на цифрових зображеннях, а також людей, місця чи тексти [11].

На сьогодні відома велика кількість методів розпізнавання зображень, проте особливу увагу слід приділити трьом основним групам: методам на основі шаблонів, НМ та статистичним методам.

Методи розпізнавання зображень на **основі шаблонів** ґрунтуються на порівнянні вхідного зображення з набором прототипів (шаблонів, зразків). Для кращого зіставлення застосовується геометрична нормалізація, яка вирівнює та масштабує зображення. Потім розраховується відстань між вхідним зображенням та кожним прототипом. Відповідність визначається як прототип, для якого відстань є мінімальною. Перевагами цього методу є:

простота;

швидкість (пошук відповідностей у наборі шаблонів обчислювально ефективний);

стійкість до шуму (деякі методи стійкі до шуму та деформацій вхідного зображення).

Серед недоліків варто вказати на:

залежність від шаблонів (ефективність методу дуже залежить від якості та кількості шаблонів у наборі);

обмежена узагальнюваність (ці методи можуть мати обмежену здатність узагальнювати нові дані, які не включені до набору шаблонів);

складність роботи з великими обсягами даних (збільшення набору шаблонів може призвести до експоненціального зростання часу, необхідного для пошуку відповідностей).

Основний метод – це зіставлення шаблонів, або, як його ще називають, лінійна просторова фільтрація. Він використовує шаблонне зображення (маску фільтра), адаптоване до певної функції пошукових зображень для виявлення. Цю техніку можна легко застосувати на сірих зображеннях або тих, де додаткова змінна кольору або відсутня, або нерелевантна.

Методи взаємної кореляції порівнюють подібність пошукових і шаблонних зображень. Їх результати мають бути найвищими в тих місцях, де структура зображення відповідає структурі шаблону, тобто де великі значення зображень пошуку множаться на великі значення зображень шаблону.

Цей метод зазвичай реалізується шляхом вибору частини пошукового зображення для використання як шаблону. $S(x,y)$ описують значення пікселя пошукового зображення, де (x,y) – це координати пікселя в пошуковому зображенні. Для простоти припустимо, що піксельні значення є скалярними, як у сірому зображенні. Так само нехай $T(x_t,y_t)$ є значенням пікселя шаблону, де (x_t,y_t) описує координати пікселя в зображенні шаблону. Щоб застосувати фільтр, просто перемістимо центр (або початок) шаблонного зображення над кожною точкою пошукового зображення та обчислимо суму добутків, подібно до скалярного добутку , між значеннями пікселів у пошуковому запиті та шаблонних зображеннях у всій області, охопленій шаблоном. Більш формально, якщо (0, 0) є центром (або джерелом) зображення шаблону, то потім взаємну кореляцією $T*S$ у кожній точці (x,y) у пошуковому зображенні можна обчислити як

$$(T * S)(x,y) = \sum_{(x_t,y_t)\in T} T(x_t,y_t) * S(x_t + x, y_t + y), \quad (1)$$

де $(T * S)(x,y)$ – значення перехресної кореляції шаблону T і пошукового зображення S у точці (x,y) пошукового зображення;

$T(x_t,y_t)$ – значення пікселя шаблону в координатах (x_t,y_t);

$S(x_t + x, y_t + y)$ – значення пікселя пошукового зображення в координатах;

$(x_t + x, y_t + y)$ – точка, де шаблон зміщено на (x,y)відносно початкової точки пошукового зображення;

$(x_t,y_t) \in T$ – усі координати, що входять до області шаблону T.

Для зручності T позначає значення пікселів зображення шаблону, а також його домен та межі. Враховуються всі можливі позиції шаблону щодо пошукового зображення. Оскільки значення перехресної кореляції є найбільшими, коли значення пікселів пошуку та шаблону вирівнюються, то найкраща відповідна позиція (x_m,y_m) відповідає максимальному значенню $T * S$.

Інший спосіб вирішення проблеми розпізнавання зображень за допомогою зіставлення шаблонів – це порівняння інтенсивності пікселів за допомогою вимірювання суми абсолютних різниць (*SAD*). Нехай $I_S(x_s,y_s)$ та $I_T(x_t,y_t)$ позначають інтенсивність світла пікселів у пошукових і шаблонних зображеннях із координатами (x_s,y_s) та (x_t,y_t) відповідно. Потім переміщуємо центр (або початок) шаблону в точку (x,y) у пошуковому зображенні, як і раніше, сума абсолютних різниць між інтенсивністю пікселів шаблону та пошуку в цій точці дорівнює

$$(SAD)(x,y) = \sum_{(x_t,y_t)\in T} I_T(x_t,y_t) * I_S(x_t + x, y_t + y), \quad (2)$$

де $(SAD)(x,y)$ – значення суми абсолютних різниць між шаблоном T і пошуковим зображенням S у точці (x,y);

$I_T(x_t,y_t)$ – інтенсивність (значення) пікселя в шаблоні з координатами (x_t,y_t);

$I_S(x_t + x, y_t + y)$ – інтенсивність (значення) пікселя пошукового зображення в координатах (x_t,y_t), де шаблон зміщено на (x,y) відносно початкової точки пошукового зображення;

$(x_t,y_t) \in T$ – усі координати, що входять до області шаблону T.

За допомогою цього показника найменша *SAD* дає найкращу позицію для шаблону, а не найбільша, як у випадку перехресної кореляції. Спосіб *SAD,* як правило, відносно простий для впровадження та розуміння, але він також має тенденцію до повільного виконання. Методи розпізнавання зображень на основі шаблонів пропонують простий та ефективний підхід до їх класифікації. Однак обмежена узагальнюваність та залежність від якості шаблонів роблять ці методи менш придатними для складних завдань розпізнавання зображень, де доступні великі обсяги даних [12].

Метод НМ використовує штучні НМ для навчання моделі розпізнавання на основі великого набору даних зображень та їх відповідних міток. НМ можуть вивчати складні закономірності даних і досягати високої точності розпізнавання.

Розпізнавання образів ШІ за допомогою НМ (рис. 2.) у наш час є найпоширенішим методом виявлення образів. НМ, що базуються на паралельних субодиницях, називаються нейронами, які імітують процес прийняття рішень людиною. Цей метод можна розглядати як масово паралельні обчислювальні системи, що складаються з величезної кількості простих процесорів із безліччю взаємозв'язків (нейронів). Найбільш популярною та успішною формою машинного навчання є глибоке навчання, яке застосовує глибокі згорткові НМ. Сьогодні розпізнавання образів НМ має перевагу над іншими методами, оскільки може неодноразово змінювати ваги на ітераційних образах.

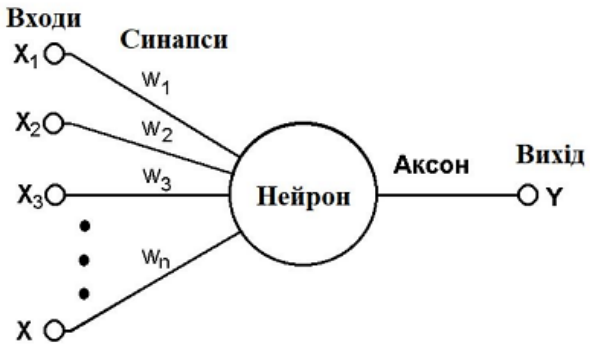


Рис. 2. Концепція НМ

На основі нечітких алгоритмів застосовується концепція нечіткої логіки, яка використовує значення істинності від 0 до 1. У нечіткій моделі можуть діяти деякі правила для відповідності даного входу певним результатам. Ця модель дає хороші результати, оскільки підходить для невизначених областей [13].

Для розпізнавання складних об'єктів створюють системи на основі НМ. Вони можуть мати топологію, орієнтовану на розв'язання конкретної задачі з урахуванням властивостей об'єкта: просторово-часової орієнтації, масштабу, геометричних параметрів, зокрема координат, кутового положення, лінійного розміру, відстані тощо. У той же час істотним недоліком типових НМ є відсутність ефективних засобів для розв'язання задач розпізнавання динамічних образів. Основною проблемою інтерпретації динамічних візуальних сцен є висока розмірність простору ознак, наявність геометричних перетворень над об'єктом. Стискання простору ознак виконують методом витягу інтегральних й інваріантних до геометричних перетворень параметрів зображень. Метод геометричних та більш загальних алгебричних інваріантів відіграє значну роль у розв'язанні задач розпізнавання зображень. Так, наприклад, інваріанти, зокрема інваріантні моменти, були успішно використані для розпізнавання профілів літаків і танків, друкованих і рукописних букв, параметрів стикувального вузла космічного апарата, а також багатьох інших об'єктів. Математичне обґрунтування інваріантних особливостей напівтонових зображень базується на теорії алгебричних інваріантів.

Суть НМ полягає в тому, що мережа складається з елементів, які називаються формальними нейронами. Кожен нейрон приймає набір сигналів, що надходять на його входи від одної групи таких самих нейронів, обробляє сигнали з урахуванням попередніх сигналів й адаптації до них на основі процедур навчання та передає результати обробки іншій групі нейронів. Зв'язки між ними кодуються вагами, що відображають важливість їх інформації для визначення загального результату. Основний принцип налаштування НМ полягає в застосуванні процедур оптимізації та адаптації на основі певних критеріїв, здатності до перенавчання. Однією з переваг НМ є те, що всі елементи можуть функціонувати паралельно, тим самим істотно підвищуючи ефективність розв'язання задач, особливо в ході оброблення зображень у реальному часі. Системи розпізнавання об'єктів зображення, що ґрунтуються на НМ, використовують ієрархічну архітектуру. Спочатку вектор ознак обробляється грубою з високим рівнем похибок, але швидкою мережею, далі, якщо вектор не був класифікований як не об'єкт, то алгоритм розв'язання корегується більш точною і більш повільною мережею.

Переважна кількість прикладних нейронних систем передбачає використання багатошарових персептронів (назва походить з англійського perceptron – сприйняття, оскільки перші зразки таких структур слугували для моделювання зору). Популярність персептронів зумовлена широким колом доступних для них задач. Загалом вони вирішують задачу апроксимації багатовимірних функцій, іншими словами – побудову багатовимірного відображення $F: x \to y$, яке узагальнює заданий набір прикладів (еталонних пар даних) $\left\{x^a, y^a\right\}$.

Залежно від типу вихідних змінних (тип вхідних не має вирішального значення) апроксимація функції може набувати вигляду:

класифікації (дискретний набір вихідних значень);

регресії (неперервні вихідні дані).

Множина практичних задач розпізнавання зображень, фільтрації шумів, передбачення часових рядів та інших зводиться до цих базових задач. Причина популярності персептронів у тому, що для свого кола задач вони є універсальними та ефективними (з погляду обчислювальної складності) пристроями.

Недоліком використання НМ є їх перенавантаження в разі надмірного збільшення кількості нейронів у мережі. Іншим недоліком є великий клас функцій, які неможливо розділити за допомогою одношарової мережі. Про ці функції говорять, що вони є лінійно нероздільними, і саме вони накладають вагомі обмеження на можливості одношарових мереж [14].

НМ є потужним інструментом для розпізнавання зображень, вони забезпечують високу точність і автоматизацію процесу виділення ознак. Хоча НМ вимагають значних обчислювальних ресурсів і великих обсягів даних для навчання, їх переваги значні, що робить їх незамінними в сучасних задачах комп'ютерного зору.

Перші **статистичні методи** ґрунтувалися на аналізі взаємного положення відтінків сірого кольору зображення та частоти їх появи, що характеризувалася двовимірною функцією щільності ймовірності. Для класифікації та розпізнавання текстур за допомогою

функції щільності ймовірності було визначено такі чотири характерні ознаки: кутовий момент; контрастність; кореляція; ентропія.

До статистичних методів належить кореляційний аналіз зображень. На основі кореляційного підходу найбільш успішним є метод матриць взаємозв'язку. Ці матриці характеризують частоту пар різних градацій сірого кольору, що присутні в зображенні, і визначаються шляхом кореляційного аналізу пікселів зображення, при цьому, якщо піксель відповідає вибраній градації, то він враховується як одиничне значення, якщо ні, то як нульове. У разі кольорових зображень цей підхід використовують для аналізу кожного з трьох базових кольорів. Як випливає з методу формування матриць взаємозв'язку, вони найкраще підходять для розв'язання задач класифікації текстур.

Разом із статистичним аналізом у просторовій області використовують аналогічний аналіз у спектральній області із застосуванням двовимірного дискретного перетворення Фур'є у базисі різних ортогональних функцій – дискретних експоненціальних функцій, косинусних, Уолша – Адамара, Хаара та інших. Для аналізу текстур користуються методом гістограм розподілу спектральних коефіцієнтів. Загальною характеристикою такого підходу є те, що гістограми спектральних коефіцієнтів, отримані в результаті інтегральних перетворень, більш стійкі та надійні, ніж гістограми розподілу окремих пікселів чи груп пікселів. Цей метод також не чутливий до наявного в зображенні шуму, але це є водночас і недоліком у разі його використання для розв'язання задачі розпізнавання незначних за розміром об'єктів на текстурованому фоні. Крім того, спектральні методи згладжують різкі межі між об'єктами зображення.

Статистичний аналіз пікселів та спектральних коефіцієнтів на основі гістограм в основному використовують для класифікації статичних текстур, а для дослідження динамічних текстур – методи на основі кореляційного аналізу.

Статистичні методи розпізнавання зображень є важливим інструментом у комп'ютерному зорі, що дозволяє ефективно класифікувати та ідентифікувати текстури й об'єкти. Їх застосування варіюється від таких простих завдань, як аналіз гістограм, до більш складних методів: кореляційний аналіз та спектральний підхід. Незважаючи на певні обмеження, статистичні методи залишаються фундаментальними та широко використовуваними в різних галузях.

Отже, запропонована на рис. 1 схема відображає взаємозв'язок між процесами розпізнавання зображень і образів, що підкреслює важливість кожного етапу в контексті ШІ та комп'ютерного зору. Вона також дозволяє чітко структурувати різні підходи та методи, які використовуються для розв'язання задач розпізнавання зображень, з акцентом на комплексному підході до аналізу та обробки візуальної інформації.

Багато проєктів розпізнавання зображень базуються на гібридних моделях для підвищення його продуктивності залежно від типу та наявності даних. Наприклад, методи глибокого навчання досягають значних результатів, але є досить затратними, тоді як простіші математичні методи зазвичай є більш ефективними. На нашу думку, використання гібридної моделі підвищить продуктивність усієї програми або системи виявлення.

Висновки. Здійснено комплексний аналіз методів розпізнавання зображень та їх класифікацію. Зокрема, розглянуто три основні групи методів розпізнавання: методи на основі шаблонів, статистичні методи та НМ. Усі вони мають свої унікальні переваги та недоліки, які визначають їхню ефективність у різних контекстах застосування.

Найперспективнішим методом, що виділяється на тлі інших, є метод НМ. Це обумовлено низкою причин, зокрема їхньою здатністю до глибокого навчання та адаптивності в умовах великих і складних наборів даних. НМ показують відмінні результати в задачах розпізнавання образів, зокрема розпізнавання сигналів на частотному спектрі. Вони здатні автоматично виділяти важливі ознаки із необроблених даних без необхідності в ручному їх визначенні. Це дозволяє НМ ефективно справлятися з такими складними задачами, як класифікація зображень, обробка сигналів у частотному спектрі. У випадках, коли розпізнавання здійснюється на основі аналізу частотних компонентів сигналу (наприклад, у задачах розпізнавання звуків, електромагнітних хвиль тощо), вони демонструють високу точність і надійність. НМ здатні навчатися відмінностей у спектральних характеристиках різних класів сигналів, що робить їх незамінним інструментом у таких задачах.

Отже, результати проведеного дослідження вказують на те, що НМ є найбільш перспективним підходом для розпізнавання зображень і сигналів, особливо в контексті аналізу частотних спектрів. Вони відкривають нові можливості для створення більш інтелектуальних й автономних систем, здатних вирішувати складні завдання безпеки. Подальший розвиток методів НМ у РЕР та їх адаптація до специфічних умов застосування сприятиме підвищенню ефективності й точності систем розпізнавання в реальності.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Woods R. E., Gonzalez R. C. Digital Image Processing. Pearson, 2017. 1192 p.
2. Forsyth D. A., Ponce J. Computer Vision: A Modern Approach. Pearson Education, Limited, 2015. 793 p.
3. Мозговенко А. А., Зінов'єва О. Г. Аналіз методів комп'ютерного зору в задачах ідентифікації осіб у відеопотоці // Таврійський науковий вісник. 2023. № 3. С. 56–62.
4. Яровий А., Власюк Р. Аналіз методики нейромережевого розпізнавання кольорових зображень у контексті її універсальності. Вінниця : ВНТУ, 2009. С. 255–262.
5. Могилевич Д., Хміль Р. Аналіз методів розпізнавання образів на основі нейронних мереж // Вчені записки ТНУ ім. В. І. Вернадського. 2023. Т. 34 (73), Техн. науки. С. 46–52. https://doi.org/10.32782/2663-5941/2023.5/09
6. Самусько Б. М., Майданюк В. П. Класифікація методів для розпізнавання зображень. Вінниця : ВНТУ, 2021. С. 181–182.
7. Machine Vision and Deep Learning for Classification of Radio SETI Signals / G. R. Harp et al. 2019. P. 1–31.
8. Савченко А. С., Синельніков О. О. Методи та системи штучного інтелекту. Київ : НАУ, 2017. 137 с.
9. Davies E. R. Computer Vision: Theory, Algorithms, Practicalities. Elsevier Science & Technology Books, 2017. 900 p.

10. Tou J., Gonzalez R. Pattern Recognition Principles. Addison-Wesley Publishing Company, 1974. 377 p.
11. Вовк С., Гнатушенко В., Бондаренко М. Методи обробки зображень та комп'ютерний зір. Дніпропетровськ : ЛІРА, 2016. 147 с.
12. Template matching // Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Template_matching (last aceessed: 22.07.2024).
13. Використання комп'ютерного зору для розпізнавання образів // Матеріали 2-ї Міжнар. студ. наук. конф. 2021. Т. 1. С. 108–110.
14. Комп'ютерне моделювання систем та процесів. Методи обчислень. Ч. 2 / Р. Квєтний та ін. Вінниця : ВНТУ, 2013. 235 с.

REFERENCES

1. Woods, R. E., & Gonzalez, R. C. (2017). *Digital Image Processing*. Pearson.
2. Forsyth, D. A., & Ponce, J. (2015). *Computer Vision: A Modern Approach*. Pearson Education, Limited.
3. Mozghovenko, A. A., & Zinov'ieva, O. H. (2023). Analiz metodiv komp'iuternoho zoru v zadachakh identyfikatsii osib u videopototsi [Analysis of Computer Vision Methods in the Tasks of Face Identification in Video Streams]. *Tavriiskyi naukovyi visnyk [Tavriysky Scientific Bulletin], 3,* 56–62 [in Ukrainian].
4. Yarovyi, A., & Vlasiuk, R. (2009). *Analiz metodyky neiromerezhevoho rozpiznavannia kolorovykh zobrazhen u konteksti yii universalnosti [Analysis of Neural Network Recognition Methodology for Color Images in the Context of its Universality]*. Vinnytsia [in Ukrainian].
5. Mohylevych, D., & Khmil, R. (2023). Analiz metodiv rozpiznavannia obraziv na osnovi neironnykh merezh [Analysis of Methods of Image Recognition Based on Neural Networks]. *Vcheni zapysky TNU im. V. I. Vernadskoho [Scientific Notes of TNU Named After V. I. Vernadsky], Vol. 34* (73), Tekhn. Nauky [Technical Sciences], 46–52. https://doi.org/10.32782/2663-5941/2023.5/09 [in Ukrainian].
6. Samusko, B. M., & Maidaniuk, V. P. (2021). *Klasyfikatsiia metodiv dlia rozpiznavannia zobrazhen [Classification of Methods for Image Recognition]*. Vinnytsia [in Ukrainian].
7. Harp, G. R., et al. (2019). *Machine Vision and Deep Learning for Classification of Radio SETI Signals.*
8. Savchenko, A. S., & Synelnikov, O. O. (2017). *Metody ta systemy shtuchnoho intelektu [Methods and Systems of Artificial Intelligence]*. Kyiv [in Ukrainian].
9. Davies, E. R. (2017). *Computer Vision: Theory, Algorithms, Practicalities.* Elsevier Science & Technology Books.
10. Tou J., & Gonzalez R. (1974). *Pattern Recognition Principles.* Addison-Wesley Publishing Company.
11. Vov, S., Hnatushenko, V., & Bondarenko, M. (2016). *Metody obrobky zobrazhen ta komp'iuternyi zir [Image Processing Methods and Computer Vision]*. Dnipropetrovsk [in Ukrainian].
12. Template matching. (n.d.). *Wikipedia, the free encyclopedia.* Retrieved from https://en.wikipedia.org/wiki/Template_matching

13. Vykorystannia komp'iuternoho zoru dlia rozpiznavannia obraziv [Using Computer Vision for Pattern Recognition]. (2021). In *Materialy 2-i Mizhnar. stud. nauk. konf. [Proceedings of the 2nd International Student Scientific Conference], Vol. 1*. (pp. 108–110) [in Ukrainian].
14. Kvietnyi, R., et al. (2013). Komp'iuterne modeliuvannia system ta protsesiv. Metody obchyslen [Computer Modeling of Systems and Processes. Methods of Calculations]. Part 2. Vinnytsia [in Ukrainian].

Стаття надійшла до редакції 25.11.2021.

S. V. Tymchuk, V. O. Tarasenko

ANALYSIS OF IMAGE RECOGNITION METHODS AND THEIR CLASSIFICATION

In the context of the Russian-Ukrainian war, new challenges arise for electronic intelligence. The radio frequency spectrum is saturated with various types of signals, and modern communications have a high level of security. An important stage of signal processing at electronic intelligence posts is their recognition. Most weapons automatically recognize signals by measuring their input parameters, however, due to the low signal-to-noise ratio, this process can be difficult. Nevertheless, almost all modern electronic intelligence equipment displays spectrograms on which the signal can be clearly recognized by human vision. Given the widespread use of image recognition technologies in various industries, it is important to consider the methods and techniques of this process and explore the possibility of using them to solve the problem of signal recognition.

The article discusses the concept of artificial intelligence with a special emphasis on the role of computer vision in this field. A classification of image recognition methods is carried out according to the scheme developed on the basis of approaches. In addition, the main stages of computer vision are analyzed, including their functional components and content. Particular attention is paid to the methods of pattern recognition, in particular to the three main types of these methods. The three main types of image recognition methods are distinguished, and their advantages and disadvantages are analyzed. The article also provides practical examples of the implementation of these methods. The final stage of the study was the selection of a method for further experimental and theoretical research.

Keywords: *electronic intelligence; radio frequency spectrum; signals; signal recognition; image recognition method; classification.*

УДК 354.42 DOI: 10.46972/2076-1546.2024.27.09

В. С. Ахтирцева, А. Р. Весельська

ТЕОРЕТИЧНІ ВИКЛИКИ ТА ПРАКТИЧНІ МОЖЛИВОСТІ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХОДІВ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

У статті розглянуто теоретичні виклики та практичні можливості оцінювання ефективності заходів психологічних операцій в умовах сучасних збройних конфліктів. Проаналізовано роль психологічних операцій, які є важливим компонентом гібридної війни, спрямованим на маніпулювання інформаційним простором та психологічним станом противника. Основну увагу приділено використанню таких сучасних технологій для здійснення інформаційно-психологічного впливу, як: радіоелектронні засоби, безпілотні літальні апарати, кіберінструменти та соціальні мережі.

Сучасні збройні конфлікти характеризуються інтенсивним використанням технологій, що дозволяють суттєво розширити масштаби психологічних операцій. Завдяки інноваційним засобам комунікації, зокрема автоматизованим системам аналізу даних, алгоритмам штучного інтелекту та технологіям великих даних (Big Data), з'являються нові можливості для оцінювання реакцій противника в режимі реального часу. Такий підхід дозволяє забезпечити більш точну й своєчасну корекцію заходів психологічного впливу залежно від результатів.

У публікації досліджено різноманітні методи психологічного впливу: деморалізацію противника, поширення дезінформації, маніпуляцію громадською думкою, формування негативного інформаційного фону серед цивільного населення ворога, а також підтримку морального духу власних військ. Особливе значення мають інформаційно-аналітичні операції, які здатні впливати не лише на індивідуальні рішення командування противника, але й на стратегічні процеси управління.

Крім того, акцентовано на важливості оцінювання ефективності таких операцій, зокрема через використання кількісних і якісних метрик, що дозволяють визначити вплив на противника, зміну його поведінки та морального стану. Так, кількісні показники включають рівень інформаційного охоплення цільової аудиторії, кількість змін у поведінці або прийнятті рішень командування противника. Якісні показники аналізують глибші аспекти: емоційну стійкість особового складу, зміну рівня довіри до командування, деморалізацію населення в зоні бойових дій.

Особливу увагу приділено методам оцінювання ефективності психологічних операцій, зокрема аналізу реакцій противника, моніторингу змін у його поведінці, а також вимірюванню впливу на інформаційні та комунікаційні системи ворога. Важливою складовою є аналіз результатів дезінформаційних кампаній, а саме оцінка їх тривалого впливу на суспільну думку. Стаття показує важливість комплексного підходу до визначення результатів психологічних операцій, який поєднує різні типи аналізу для досягнення стратегічних цілей у сучасних військових конфліктах.

Ключові слова: *психологічна операція; інформаційний вплив; кіберінструмент; соціальна мережа; оцінювання ефективності; психологічний стан; збройний конфлікт.*

© В. С. Ахтирцева, А. Р. Весельська, 2024

Постановка проблеми в загальному вигляді. У сучасних умовах, питання психологічних операцій (ПсО) набуло надзвичайної актуальності. Це пов'язано з тим, що сучасні конфлікти виходять за рамки традиційної фізичної війни та включають у себе інформаційно-психологічний вплив, який здійснюється на різні аудиторії для досягнення стратегічних цілей. ПсО виконують спеціалізовані підрозділи, зокрема: Сили спеціальних операцій, розвідувальні органи, центри інформаційних операцій та кіберпідрозділи. Вони займаються деморалізацією противника, маніпуляцією громадською думкою, поширенням дезінформації та захистом інформаційного простору. Це ключовий елемент сучасної гібридної війни. Витрачені ресурси на проведення заходів ПсО в умовах війни мають бути доцільними, що порушує питання визначення результативності цих заходів. Усі дії в рамках ПсО є складноформалізованими, а тому оцінювання їх ефективності – це актуальне завдання.

Аналіз останніх досліджень і публікацій. Дослідження ПсО в умовах сучасних військових конфліктів висвітлюють їх ключову роль у гібридній війні, спрямованій на маніпулювання інформаційним простором і психологічним станом противника. Наукові роботи підкреслюють важливість інтеграції таких сучасних технологій для ефективного інформаційного впливу, як: безпілотні літальні апарати (БпЛА), радіоелектронні засоби (РЕЗ), кіберзброя та соціальні мережі. Ці інструменти дозволяють поширювати дезінформацію, деморалізувати противника та підтримувати моральний дух власних військ [1]. Проте на сьогодні відсутні чіткі стандарти для оцінювання ефективності заходів. Особливу увагу приділено питанням, як визначити зміни в поведінці чи моральному стані противника. Для цього розробляються такі багатофакторні моделі, що поєднують кількісні (статистичні) та якісні (поведінкові) методи аналізу: моніторинг реакцій противника, аналіз перехоплених переговорів й оцінка змін у громадській думці через соціальні мережі [2]. Сучасні дослідження демонструють, що соціальні медіа стали потужним інструментом ПсО, вони дозволяють швидко охоплювати широку аудиторію. Використання ботів і фейкових акаунтів створює інформаційні хвилі, які можуть впливати на суспільну думку, підривати довіру до керівництва противника або викликати паніку серед населення. Крім того, кіберзброя надає можливість проникати в мережі противника, поширюючи дезінформацію чи виводячи з ладу критичні системи [3]. Практичні можливості оцінювання ефективності ПсО ґрунтуються на аналізі реакцій противника. Використовуються кількісні метрики, зокрема частота здачі в полон або зміна тактики, та якісні, наприклад, моральний стан противника. БпЛА й радіопередачі активно застосовуються для доставляння повідомлень, що деморалізують, а також для впливу на комунікаційні системи ворога. Наприклад, перехоплення перемовин дозволяє оцінити паніку чи деморалізацію серед особового складу противника [4].

Формулювання завдання дослідження. Дослідження щодо оцінювання ефективності ПсО в умовах сучасного збройного конфлікту повинно охопити вивчення методів ПсО, зокрема використання РЕЗ, мобільних платформ, БпЛА, соціальних мереж і кіберзброї для трансляції інформації, поширення дезінформації та психологічного впливу на противника і його населення. Воно також має включити розроблення

показників для оцінювання впливу на моральний стан противника, визначення кількості випадків здачі в полон, зміни в поведінці ворога, ефекту від пропагандистських та деморалізуючих повідомлень. Необхідно вивчити, як комбінація РЕЗ, БпЛА, кіберінструментів і соціальних мереж може підсилити психологічний вплив на ворога, а також забезпечити ефективну координацію інформаційної війни. Важливим аспектом є дослідження реальних прикладів використання цих технологій у сучасних конфліктах, зокрема в контексті війни в Україні, для оцінювання їх практичної ефективності. На основі отриманих даних необхідно розробити рекомендації щодо покращення стратегій ПсО з урахуванням новітніх технологій і методів, що дозволить глибше зрозуміти, як сучасні технології та інформаційні операції впливають на бойові дії, моральний стан противника та громадську думку.

Виклад основного матеріалу. В епоху цифрових технологій контроль над інформацією став потужним інструментом впливу, який дозволяє формувати суспільну думку, мобілізувати населення і військових, а також деморалізувати противника. ПсО відіграють ключову роль у створенні потрібних наративів, поширенні як дезінформації, так і правдивої інформації, здатної послабити моральний дух ворога. У контексті конфлікту такі операції спрямовані на те, щоб деморалізувати його, сіяти сумніви серед його населення та військових щодо доцільності подальшої боротьби. Це досягається через розповсюдження інформації про втрати, невдачі на фронті чи політичну нестабільність, що впливає на готовність противника до опору. Сучасний кіберпростір та соціальні мережі стали новим полем бою, де ПсО активно використовуються для швидкого поширення інформації. Завдяки соціальним платформам можна ефективно впливати на емоційний стан аудиторії, викликаючи паніку, дезорієнтацію або, навпаки, підвищуючи впевненість і бойовий дух. Отже, інформаційна війна стала важливим компонентом сучасних збройних конфліктів.

Для ведення ПсО в сучасних умовах використовують як спеціалізовані технічні засоби, так і традиційні зразки озброєння, адаптовані для інформаційного впливу на противника та цивільне населення, що підтверджується бойовим досвідом ефективного використання цих засобів. Наприклад, для втручання в радіоефір противника активно застосовують такі РЕЗ: радіостанції, спеціальні передавачі, мобільні платформи радіоперешкод тощо. Ефективність цих операцій полягає в здатності глушити зв’язок ворога, транслювати пропагандистські матеріали та навіть впливати на емоційний стан через постійний психологічний тиск.

Крім того, досить часто вдаються до дезінформації через радіо- і мобільний зв’язок: українські сили застосовують методи радіодезінформації, коли противнику передається фальшива інформація через захоплені канали зв’язку або спеціальні радіопередачі. Наприклад, передавалися неправдиві відомості про позиції чи переміщення українських підрозділів для введення противника в оману. Російські сили поширювали дезінформацію через мобільний зв’язок: надсилаючи повідомлення населенню або військовим із заявами про нібито успішні атаки або знищення важливих об’єктів, що могло викликати паніку або зневіру.

Обидві сторони активно використовували можливості радіоелектронної боротьби для трансляції деморалізуючих повідомлень із закликами до здачі в полон, вказували на високі втрати і пропонували гарантоване збереження життя. Такі заходи здійснювалися як через радіо, так і через SMS-повідомлення. Зокрема, українські військові створювали повідомлення, спрямовані на російських солдатів, спонукаючи їх здаватися та пояснюючи наслідки продовження участі в бойових діях. RIAB система забезпечує передачу аудіосигналу через FM-частоти, що дозволяє здійснювати трансляцію безпосередньо на звичайні FM-радіоприймачі. Це особливо ефективно в умовах, коли необхідно швидко й масово донести інформацію до широкої аудиторії, цивільного населення та військових противника.

Одним із найпоширеніших способів використання є мобільні радіостанції, встановлені на автомобілях або бронетехніці, які дозволяють транслювати інформаційні або пропагандистські повідомлення в зоні конфлікту, особливо в районах, де немає доступу до традиційних медіа. Наприклад, це можуть бути заклики до співпраці, інструкції для населення або мотивуючі послання для підтримки морального духу. Система також ефективно використовується для психологічного впливу на противника через FM-трансляції. Вона дозволяє передавати аудіоматеріали, спрямовані на підрив морального духу противника, наприклад, повідомлення про їхні втрати, невдачі або заклики здаватися. Система також може застосовуватися для ізоляції ворога від правдивої інформації, замінюючи сигнал місцевих радіостанцій на бажаний контент. Це дозволяє створювати наративи, які підтримують стратегічні цілі операції. Окрім цього, вона корисна для власних військових – через трансляції новин про успіхи на фронті, мотивуючих промов або музики, що підвищують бойовий дух у складних умовах.

БпЛА стали одним із ключових інструментів для ведення ПсО завдяки можливості доставляти інформаційні матеріали (листівки) або транслювати аудіоповідомлення на території, контрольовані ворогом. Деякі моделі використовуються для демонстрації сили та залякування, що може впливати на психологічний стан противника, особливо якщо супроводжується загрозою ударів або постійним патрулюванням. Традиційні листівки, що скидаються з літаків або доставляються дронами, усе ще мають ефект, особливо в районах, де доступ до Інтернету обмежений. Такі матеріали можуть містити інструкції щодо здачі в полон, інформацію про можливості евакуації або деморалізуючі повідомлення про втрати противника.

Використання потужних гучномовців, розміщених на мобільних платформах, дозволяє транслювати заклики до складання зброї, поширювати деморалізуючі повідомлення або аудіозаписи, які підкреслюють перевагу своїх сил. Такі засоби особливо ефективні на передовій лінії фронту або в регіонах із високою концентрацією противника.

Застосування кіберінструментів для проникнення у комунікаційні системи противника та поширення дезінформації є важливою частиною сучасних ПсО. Кіберзброя дозволяє розповсюджувати фальшиві повідомлення серед військових і цивільного населення, впливати на інформаційні ресурси та навіть маніпулювати ключовими сайтами і платформами.

Інформаційні кампанії, які здійснюються через соціальні мережі, спрямовані на широку аудиторію для формування потрібного наративу. Використання ботів і фейкових

акаунтів дозволяє створювати інформаційні хвилі, що можуть підірвати довіру до уряду чи військових лідерів противника, впливати на настрої громадськості та знижувати рівень підтримки конфлікту.

В умовах динамічного ведення бойових дій необхідне оцінювання їх ефективності, що є складноформалізованою задачею. Основним показником результативності необхідно вважати реакцію противника. Відомі такі загальні підходи до оцінювання ефективності ПсО:

1) кількісний аналіз: використання статистичних даних щодо реакцій противника або населення (здача в полон, зміна тактики, перехід на бік противника);

2) якісний аналіз: визначення морального стану противника за допомогою розвідданих або опитувань полонених;

3) комплексний підхід: поєднання кількісних і якісних показників для створення загальної картини ефективності ПсО.

Ці методи допоможуть визначити, наскільки успішно проведені операції впливають на бойові дії та моральний стан противника. Розглянемо більш детально метрики для оцінювання ефективності різних методів ПсО.

РЕЗ та радіодезінформація: показник збоїв у комунікації противника (вимірюється частота й тривалість переривання зв'язку ворога); аналіз перехоплених сигналів (оцінюється, наскільки вдалося ввести противника в оману завдяки переданню фальшивої інформації); психологічна реакція противника (аналіз перехоплених переговорів чи повідомлень може свідчити про ступінь паніки чи дезорганізації); моніторинг пропагандистських наративів (визначається, чи почав противник поширювати контрпропаганду або змінювати тактику комунікації).

БпЛА для інформаційних операцій: охоплення аудиторії (кількість доставлених листівок або охоплення територій аудіоповідомленнями); реакція на листівки або аудіо (визначення кількості випадків здачі в полон або контактів із відповідними силами через вказані в листівках інструкції); психологічний вплив (вимірюється на основі змін у поведінці противника, наприклад, зменшення активності або інша тактика після психологічного впливу); аналіз відео з дронів (візуальне оцінювання поведінки солдатів противника під час трансляцій чи демонстрації сили).

Гучномовні установки: кількість випадків здачі в полон (статистика, яка відображає ефективність закликів до капітуляції); аналіз морального стану противника (здійснюється шляхом перехоплення переговорів або опитуванням полонених); оцінювання зниження бойового духу (спостереження за змінами в поведінці противника (відмова від наступальних дій, підвищена кількість дезертирів тощо)).

Кіберзброя: ступінь проникнення в мережі противника (кількість і важливість зламаних систем або отриманих даних); вплив дезінформації (аналіз реакцій на фальшиві повідомлення, вимір паніки або дезорганізації в комунікаційних каналах ворога); оцінювання ефективності фішинг-атак чи зламів (частота успішних атак, кількість уражених систем тощо).

Соціальні мережі та цифрові платформи: охоплення аудиторії (кількість переглядів, репостів і коментарів до інформаційних матеріалів); моніторинг настроїв (Sentiment Analysis) (аналіз тональності публікацій і коментарів у соціальних мережах для

оцінювання впливу кампанії); інтерактивність (вимірювання залученості аудиторії, зокрема кількості реакцій на публікації); виявлення змін у суспільній думці (порівняння даних соціологічних опитувань до та після кампанії).

Оцінювання ефективності використання системи RIAB для ПсО може базуватися на кількісних і якісних показниках з урахуванням специфіки її завдань та результатів впливу на противника і власні сили.

Кількісний аналіз: оцінювання аудиторії охоплення (визначення радіуса дії трансляцій і кількості населення або військових противника, які потенційно могли почути повідомлення, з урахуванням даних про переміщення військових підрозділів, а отже, зони впливу); вимірювання реакції (фіксація змін у поведінці ворога після трансляцій, наприклад, збільшення випадків здачі в полон, дезертирства чи змін у тактиці); визначення кількості контактів або звернень до своїх військових чи цивільних, спрямованих на виконання рекомендацій, озвучених у трансляціях (здача в полон, евакуація тощо).

Якісний аналіз: дослідження морального стану (опитування полонених або дезертирів про їхнє сприйняття змісту трансляцій); аналіз повідомлень розвідки про моральний стан противника в регіонах, де працювала система RIAB; контент-аналіз (перевірка того, як противник реагує на конкретний тип повідомлень: деморалізуючі, заклики до складання зброї, інструкції для цивільного населення; аналіз тем, що викликають найбільший резонанс, для адаптації змісту подальших трансляцій.

Усі ці засоби стають потужнішими в поєднанні, коли операції координуються на різних рівнях: від кіберпростору до фізичної демонстрації сили. Це дозволяє створити багаторівневий психологічний вплив, що підриває моральний дух противника та формує сприятливі умови для власних військ.

Висновки. ПсО в сучасних умовах ведення війни стали важливим компонентом стратегічного впливу, що дозволяє ефективно маніпулювати інформаційним простором та психологічним станом противника. Використання таких сучасних технологій, як: РЕЗ, БпЛА, кіберінструменти та соціальні мережі, – дозволяє здійснювати потужний інформаційний вплив, спрямований на деморалізацію ворога, маніпуляцію громадською думкою та підвищення морального духу власних військ. Успішність таких операцій залежить від комплексного підходу до оцінювання їх ефективності, що включає кількісні та якісні метрики. Аналіз реакцій противника, змін у його поведінці та моральному стані є основними показниками результативності вжитих заходів. З огляду на швидку еволюцію технологій та інформаційних платформ ПсО стають дедалі більш динамічними та потужними, що робить їх ключовим елементом у сучасних збройних конфліктах.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Інформаційні війни: проблеми, загрози та протидія / З. М. Бржевська, Н. М. Довженко, Р. В. Киричок та ін. // Кібербезпека: освіта, наука, техніка. 2019. № 3 (3). С. 88–96. https://doi.org/10.28925/2663-4023.2019.3.8896

2. FM 3-05.301 Psychological Operations Tactics, Techniques, and Procedures. 2003, dec. URL: https://fas.org/irp/doddir/army/fm3-05-301.pdf (last accessed: 03.09.2024).

3. Історія інформаційно-психологічного протиборства : навч. посіб. / [Я. Жарков, Л. Компанцева, В. Остроухов та ін.] ; за заг. ред. Є. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.
4. Інформаційно-психологічні операції: планування, протидія, технології : монографія / Г. В. Пєвцов., С. В. Залкін, С. О. Сідченко, К. І. Хударковський. Харків : ДІСА ПЛЮС, 2020. 252 с.
5. Шевчук П. І. Інформаційно-психологічна війна Росії проти України: як їй протидіяти // Демократичне врядування. 2014. № 13. С. 1–11
6. Ковалевич Б. В. Соціальні мережі як новий інструмент ведення інформаційних війн у сучасному світі // Соціологія. 2014. № 4 (108). С. 118–121.
7. Мороз Ю., Твердохліб Ю. Інформаційно-психологічні операції в умовах гібридної війни // Вісник Львівського університету. 2016. № 38. С. 97–105. https://doi.org/10.30970/vir.2016.38.0.2354.
8. Лужецький В. А., Дудатьєв А. В. Концептуальна модель системи інформаційного впливу. 2017. https://doi.org/10.18372/2225-5036.23.11550
9. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики // GOAL : веб сайт. URL: http://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/ (дата звернення: 06.11.2024).
10. ВСТ 01.004.007-2017(1). Видання. Воєнна політика, безпека та стратегічне планування. Система стратегічних комунікацій держави у воєнній сфері. Терміни та визначення [Чинний від 2017.12.20]. Вид. офіц. Київ, 2017. 46 с.

Стаття надійшла до редакції 03.12.2024.

REFERENCES

1. Brzhevska, Z. M., Dovzhenko, N. M., & Kyrychok, R. V. et al. (2019). Informatsiini viiny: problemy, zahrozy ta protydiia [Information Wars: Problems, Threats and Countermeasures]. *Kiberbezpeka: osvita, nauka, tekhnika [Cybersecurity: Education, Science, Technology]*, *3* (3), 88–96. https://doi.org/10.28925/2663-4023.2019.3.8896 [in Ukrainian].
2. *FM 3-05.301 Psychological Operations Tactics, Techniques, and Procedures.* (2003, dec.). Retrieved from https://fas.org/irp/doddir/army/fm3-05-301.pdf
3. Zharkov, Ya., Kompantseva, L., & Ostroukhov, V. et al. (2012). *Istoriia informatsiino-psykholohichnoho protyborstva [History of Informational and Psychological Confrontation]*. Kyiv [in Ukrainian].
4. Pievtsov, H. V., Zalkin, S. V., Sidchenko, S. O., & Khudarkovskyi, K. I. (2020). *Informatsiino-psykholohichni operatsii: planuvannia, protydiia, tekhnolohii : monohrafiia [Information-Psychological Operations: Planning, Counteraction, Technologies: Monograph]*. Kharkiv [in Ukrainian].
5. Shevchuk, P. I. (2014). Informatsiino-psykholohichna viina rosii proty Ukrainy: yak yii protydiiaty [Information-Psychological War of russia against Ukraine: How to Counter It]. *Demokratychne vriaduvannia [Democratic Governance]*, *13*, 1–11 [in Ukrainian].

6. Kovalevych, B. V. (2014). Sotsialni merezhi yak novyi instrument vedennia informatsiinykh viin u suchasnomu sviti [Social Networks as a New Tool for Waging Information Wars in the Modern World]. *Sotsiolohiia [Sociology], 4* (108), 118–121 [in Ukrainian].
7. Moroz, Yu., & Tverdokhlib, Yu. (2016). Informatsiino-psykholohichni operatsii v umovakh hibrydnoi viiny [Information-Psychological Operations in the Conditions of Hybrid War]. *Visnyk Lvivskoho un-tu [Visnyk of the Lviv University], 38,* 97–105. https://doi.org/10.30970/vir.2016.38.0.2354 [in Ukrainian].
8. Luzhetskyi, V. A., & Dudatiev, A. V. (2017). *Kontseptualna model systemy informatsiinoho vplyvu [Conceptual Model of the Information Influence System]*. https://doi.org/10.18372/2225-5036.23.11550 [in Ukrainian].
9. Derkachenko, Ya. (n.d.). Informatsiino-psykholohichni operatsii yak suchasnyi instrument heopolityky [Information and Psychological Operations as a Modern Tool of Geopolitics]. *GOAL: website.* Retrieved from http://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/ [in Ukrainian].
10. VST 01.004.007-2017(1). *Vydannia. Voienna polityka, bezpeka ta stratehichne planuvannia. Systema stratehichnykh komunikatsii derzhavy u voiennii sferi. Terminy ta vyznachennia [Edition. Military Policy, Security and Strategic Planning. The System of Strategic Communications of the State in the Military Sphere. Terms and Definitions]*. Kyiv [in Ukrainian].

V. S. Akhtyrtseva, A. R. Veselska

THEORETICAL CHALLENGES AND PRACTICAL POSSIBILITIES OF ASSESSING THE EFFECTIVENESS OF PSYCHOLOGICAL OPERATIONS

The article discusses theoretical challenges and practical possibilities of assessing the effectiveness of psychological operations in modern armed conflicts. The author analyses the role of psychological operations, which are an important component of hybrid warfare aimed at manipulating the information space and the psychological state of the enemy. The main attention is paid to the use of modern technologies, such as electronic means, unmanned aerial vehicles, cyber tools and social networks for information and psychological influence.

Modern armed conflicts are characterised by the intensive use of technology, which allows for a significant expansion of psychological operations. Thanks to innovative communication tools such as automated data analysis systems, artificial intelligence algorithms and big data technologies, new opportunities are emerging to assess enemy reactions in real time. This approach allows for a more accurate and timely correction of psychological influence measures depending on the results.

The article examines various methods of psychological influence: demoralisation of the enemy, spreading disinformation, manipulation of public opinion, creating a negative information background among the enemy's civilian population, and maintaining the morale of own troops. Particular importance is attached to information and analytical operations, which can influence not only individual decisions of the enemy command, but also strategic management processes.

In addition, the importance of evaluating the effectiveness of such operations is emphasised, in particular through the use of quantitative and qualitative metrics that allow to determine the impact on the enemy, changes in his behaviour and morale. In particular, quantitative indicators include the level of information coverage of the target audience, the number of changes in the behaviour or decision-making of the enemy command. Qualitative indicators analyse deeper aspects, such as the emotional stability of personnel, changes in confidence in the command, and demoralisation of the population in the combat zone.

Particular attention is paid to methods of assessing the effectiveness of psychological operations, including analysing the enemy's reactions, monitoring changes in his behaviour, and measuring the impact on the enemy's information and communication systems. An important component is the analysis of the results of disinformation campaigns, in particular, the assessment of their long-term impact on public opinion. The article emphasises the importance of a comprehensive approach to determining the results of psychological operations, which combines different types of analysis to achieve strategic goals in modern military conflicts.

Keywords: *psychological operation; information influence; cyber tool; social network; effectiveness assessment; psychological state; armed conflict.*

ISSN 2076-1546
УДК 519.816 DOI: 10.46972/2076-1546.2024.27.10

О. О. Гребенюк

МАТЕМАТИЧНА МОДЕЛЬ СИГНАЛУ ІЗ ЗАДАНИМИ ПОЛЯРИЗАЦІЙНИМИ ПАРАМЕТРАМИ В ОРТОГОНАЛЬНОМУ ПОЛЯРИЗАЦІЙНОМУ БАЗИСІ

Досвід ведення бойових дій в умовах широкомасштабного вторгнення російської федерації проти України свідчить, що сучасний рівень розвитку радіоелектронного озброєння характеризується великою різноманітністю видів та типів радіоелектронних засобів, а також застосуванням багатофункціональних засобів зі змінюваними в широких межах параметрами сигналів та режимами роботи. Так, у сучасних (новітніх) наземних, повітряних та морських радіолокаційних станціях за різних режимів бойової роботи, залежно від завдань та умов складної радіоелектронної обстановки, здійснюється навмисна зміна частотно-часових, а також поляризаційних параметрів випромінюваних сигналів. Наявність відмінностей у поляризаційних параметрах сигналів об'єктивно створює передумови для їх урахування в обробці для покращення показників виявлення, розпізнавання та пеленгування системами радіомоніторингу. В основі підходу лежить застосування антен з ортогональними за поляризацією антенними елементами, що дозволяє подавати сигнали у вигляді поляризаційних векторів. У ході оброблення необхідно враховувати вплив поляризаційних характеристик антенної системи на параметри поляризаційного вектора (зміну поляризаційного базиса), що є актуальним, оскільки сигнали надходять до антенної системи з різних кутових напрямків.

Важливою умовою отримання об'єктивних результатів у дослідженні ефективності алгоритмів поляризаційної обробки є застосування коректної математичної моделі сигналів із заданими поляризаційними параметрами в окресленому ортогональному поляризаційному базисі, а також використання сигналів від реальних радіотехнічних засобів, поляризаційні параметри яких можуть бути визначені в поляризаційному базисі, відмінному від заданого. У статті запропоновано математичну модель, яка дозволяє виразити складові поля через параметри еліпса поляризації, а також наведено вирази, які описують взаємозв'язок поляризаційних векторів та їх коваріаційних матриць у різних поляризаційних базисах антенної системи.

Ключові слова: *поляризаційний еліпс; поляризаційні характеристики; ступінь поляризації; ортогональний поляризаційний базис; матриця перетворення.*

Постановка проблеми в загальному вигляді. Використання в сучасних радіотехнічних засобах (РТЗ) сигналів зі змінюваними поляризаційними параметрами обумовлює необхідність застосування в засобах радіомоніторингу (РМ) антен з ортогональними за поляризацією елементами та розроблення алгоритмів обробки, які враховують поляризаційну структуру виділених антеною складових сигналів (поляризаційних векторів (ПВ)) у відповідному їй поляризаційному базисі (ПБ). Відомо, що поляризаційні характеристики антен у межах діаграми спрямованості (ДС) не

© О. О. Гребенюк, 2024

є сталими, це є причиною викривлення ПБ у разі надходження сигналу з напрямку, відмінного від максимуму ДС [1, 4].

Оскільки роль поляризаційного фільтра на вході систем РМ виконують різні за типом, параметрами та характеристиками антенні системи, то сформованому на виході антени ПВ буде відповідати ПБ, який забезпечує антена. У зв'язку із цим під час дослідження алгоритмів просторової обробки об'єктивно виникає необхідність перерахунку ПВ та їх коваріаційних матриць у потрібний ПБ.

Аналіз останніх досліджень і публікацій. Дослідженню поляризаційної теорії електромагнітних хвиль та антен присвячено велику кількість зарубіжних і вітчизняних наукових робіт. У контексті цієї статті можна виділити такі напрямки:

загальні аналітичні вирази теорії поляризації радіохвиль, опис радіохвиль в ортогональних ПБ [1–3];

результати досліджень характеристик поляризаційних діаграм опромінювачів та антен, які використовуються в радіолокації та РМ [1, 4];

розкладання антенною системою електромагнітної хвилі на ортогонально поляризовані складові [1, 5, 6];

врахування неортогональності поляризаційного вимірювального базису для обчислення коваріаційних матриць ПВ [7].

Формулювання завдання дослідження. Метою статті є розроблення математичної моделі сигналу із заданими поляризаційними параметрами та ступенем поляризації в ортогональному ПБ.

Виклад основного матеріалу. Поляризація електромагнітної хвилі (ЕМХ) є її просторово-часовою характеристикою, що визначається видом траєкторії, яку описує кінець проєкції вектора електричного поля $\vec{E}$. Фігуру, що утворюється кінцем вектора $\vec{E}$ за період коливання високої частоти, прийнято називати поляризаційною діаграмою або поляризаційним еліпсом [1].

Розрізняють поляризацію простого виду, складну та випадкову. До поляризації простого виду належать еліптична, колова та лінійна. Складний вид включає поляризацію, що змінюється в часі за довільним, але певним чином визначеним законом. Складний вид отримують шляхом модуляції поляризації простого виду [2]. За випадкової поляризації вектор $\vec{E}$ описує в просторі фігуру невизначеної форми.

Для кількісної характеристики поляризації хвиль використовують геометричні параметри поляризаційної діаграми (поляризаційного еліпса). Абсолютне значення коефіцієнта еліптичності k_e визначається як відношення малої b та великої a напівосей еліпса:

$$k_e = b/a. \tag{1}$$

Значення модуля k_e обмежуються очевидними межами $0 \le |k_e| \le 1$. Залежно від напрямку обертання вектора $\vec{E}$ коефіцієнту еліптичності надають той чи інший знак.

Разом із коефіцієнтом k_e для характеристики форми еліпса й напрямку обертання вектора $\vec{E}$ використовують кут еліптичності $\alpha = arctg\, k_e$, за умови $-0{,}25\pi \le \alpha \le 0{,}25\pi$. Орієнтацію еліпса знаходять за значенням кута β, утвореного віссю $0x$ обраної системи координат і великою віссю еліпса. При однозначному визначенні положення еліпса значення β лежать у межах $-0{,}5\pi \le \beta \le 0{,}5\pi$.

Залежно від того, змінюються параметри поляризаційної діаграми з часом чи залишаються постійними, ЕМХ поділяють на три групи: повністю поляризовані, частково поляризовані й неполяризовані. Повністю поляризованою називається хвиля з незмінними в часі параметрами поляризації. За наявності безперервних відносно повільних змін параметрів поляризаційної діаграми ЕМХ називають частково поляризованою. Неполяризована чи хаотично поляризована хвиля характеризується швидкими флуктуаціями вектора E як за модулем, так і за напрямком обертання. У цьому разі поляризаційна діаграма набуває всіх можливих форм й орієнтацій [2].

Проєкції e_x і e_y вектора E на ортогональні осі координат $0x$ і $0y$ можна подати у такому вигляді:

$$e_x = E_x \cos(\omega_o t + \phi_x), \tag{2}$$

$$e_y = E_y \cos(\omega_o t + \phi_y). \tag{3}$$

Для розрахунків значень складових сигналу (2) і (3) використовують вирази, що дозволяють описати складові поля через параметри еліпса поляризації a, k_e і β [1]:

$$E_x = a\left(\cos^2\beta + k_e \sin^2\beta\right)^{0,5}, \tag{4}$$

$$E_y = a\left(\sin^2\beta + k_e \cos^2\beta\right)^{0,5}, \tag{5}$$

$$\Delta\phi = \phi_y - \phi_x = arctg\,\frac{2k_e}{\left(1-k_e^2\right)\sin 2\beta}. \tag{6}$$

Для реалізації моделей сигналів, різних за ступенем поляризації, необхідно, щоб поляризаційні параметри приймали значення:

а) для повністю поляризованого сигналу: $a = const$, $\beta = const$;

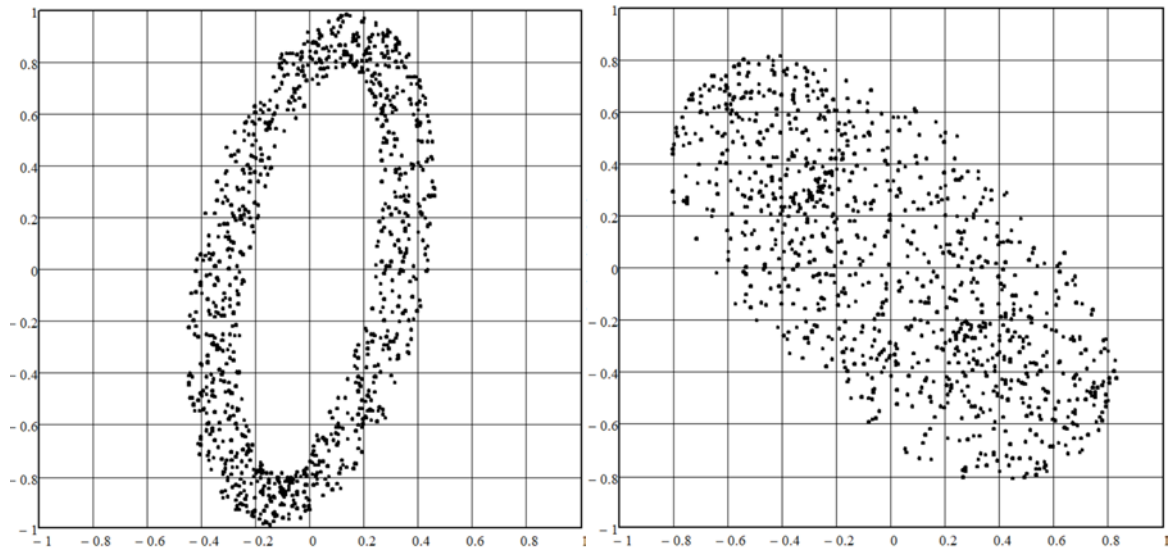
б) для хаотично поляризованого сигналу: $a \ne const$, $0 \le k_e \le 1$, $-0{,}5\pi \le \beta \le 0{,}5\pi$.

Суттєво, що частково поляризований сигнал можливо подати у вигляді суми двох статистично незалежних компонентів:

$$E_Ч = m_p E_П + \left(1 - m_p\right)E_X, \tag{7}$$

які визначають регулярну (повністю поляризовану) $E_П$ і хаотично поляризовану E_X складові сигналу, при цьому коефіцієнт m_p приймає значення $m_p = 0...1$ і відповідає заданому ступеню поляризації.

На рис. 1 показані миттєві положення вектора $\vec{E}$ на інтервалі спостереження (1000 вибірок) частково поляризованих сигналів із заданими поляризаційними параметрами, змодельованих за виразами (2)–(7) у програмному середовищі Mathcad.



а) *б)*

Рис. 1. Нормований поляризаційний еліпс сигналів із заданими поляризаційними параметрами:

а) $m_p = 0{,}9$; $k_e = 0{,}4$; $\beta = 80^\circ$;

б) $m_p = 0{,}7$; $k_e = 0{,}4$; $\beta = -45^\circ$.

У ході проведення поляризаційних досліджень зазвичай обмежуються розкладом поляризованих хвиль по двох ортогональних комплексних в загальному випадку ортах, що знаходяться у фазовій площині хвилі в дальній зоні антени радіолокаційної станції. Пара ортонормованих комплексних векторів $\dot{\vec{e}}_1$ та $\dot{\vec{e}}_2$ називається ПБ та позначається $\left[\dot{\vec{e}}_1, \dot{\vec{e}}_2\right]$ [8].

Під ортонормованим базисом деякого простору в загальному розуміють таку систему ортонормованих векторів $\left(\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\right)$, якщо виконується умова

$$\vec{e}_k \vec{e}_l = \begin{cases} 1, & при\ k \neq l \\ 0, & при\ k = l \end{cases}, \ k, l = \overline{(1, n)}, \tag{8}$$

де n – кількість векторів, що збігаються з розмірністю простору [8].

Для аналізу поляризаційних параметрів ЕМХ застосовують ортогональні двомірні ПБ. Таким базисом може бути лінійний, еліптичний або коловий. Будь-який ПБ можна вважати заданим, якщо відомі коефіцієнт еліптичності k_{e1} та кут орієнтації β_1 одного з ортів, тому що для іншого орта (через їхню ортогональність) завжди правильне співвідношення $k_{e_2} = -k_{e_1}$, $\beta_2 = \beta_1 \pm \pi/2$. Тому базис $\left[\dot{\vec{e}}_1, \dot{\vec{e}}_2\right]$ можна позначити у вигляді $[k_e, \beta]$, де $k_e = k_{e1}$ а $\beta = \beta_1$.

Довільний комплексний вектор $\vec{\dot{E}}$, компланарний ортам базису $\vec{e}_1$ та $\vec{e}_2$, може бути поданий у такому вигляді [1, 2]:

$$\vec{\dot{E}} = \left(\vec{\dot{E}}, \vec{e}_1^{\,*}\right)\vec{e}_1 + \left(\vec{\dot{E}}, \vec{e}_2^{\,*}\right)\vec{e}_2 = \dot{E}_1\vec{e}_1 + \dot{E}_2\vec{e}_2, \tag{9}$$

де $\vec{\dot{E}}_1 = \left(\dot{E}_1, \vec{e}_1^{\,*}\right)$ та $\vec{\dot{E}}_2 = \left(\dot{E}_2, \vec{e}_2^{\,*}\right)$ – проєкції вектора $\vec{\dot{E}}$ на напрямки ортів $\vec{e}_1$, $\vec{e}_2$, вони називаються комплексними координатами вектора $\vec{\dot{E}}$ в базисі $\left[\vec{e}_1, \vec{e}_2\right]$.

Якщо вектор $\vec{\dot{E}}$ створює еліптичну поляризацію деякої хвилі, то модулі та аргументи комплексних координат є амплітудами та фазами еліптично поляризованих компонентів цієї хвилі, причому кожний компонент спрямовано паралельно відповідному орту ПБ. Отже, (9) описує розклад еліптично поляризованої хвилі на дві ортогонально-поляризовані складові, кожна з яких характеризується своєю амплітудою та фазою.

У зв'язку із цим використовують матричний запис координат комплексного вектора $\vec{\dot{E}}$

$$\vec{\dot{E}} = \left(\vec{\dot{E}}_1 \quad \vec{\dot{E}}_2\right)^T, \tag{10}$$

де $\vec{\dot{E}}_1$ та $\vec{\dot{E}}_2$ – комплексні амплітуди ортогональних компонент поля, модулі та аргументи яких є амплітудами та фазами еліптично поляризованої хвилі, причому амплітудою хвилі еліптичної поляризації є модуль комплексного вектора $\vec{\dot{E}}$:

$$E_m = \sqrt{\dot{E}_1\dot{E}_1^* + \dot{E}_2\dot{E}_2^*}, \tag{11}$$

де $(*)$ означає комплексно-спряжене число, а фаза визначається фазою лінійно поляризованої компоненти, що збігається з великою віссю еліпса [2, 5, 6].

Отже, відношення (9) також описує розклад еліптично поляризованої хвилі на дві ортогонально поляризовані компоненти в довільному базисі $\left[\vec{e}_1, \vec{e}_2\right]$. Таке аналітичне подання є зручним та дозволяє використовувати для аналізу поляризаційних властивостей хвиль апарат матричного обчислення.

У разі необхідності переходу від одного довільного ортонормованого базису до іншого (від $\left[\vec{e}_1^{\,0}, \vec{e}_2^{\,0}\right]$ до $\left[\vec{e}_1^{\,1}, \vec{e}_2^{\,1}\right]$) здійснюється перетворення ортогонально-поляризованих компонент вектора $\vec{\dot{E}}$ шляхом домноження на комплексну унітарну матрицю перетворення [1]:

$$\vec{\dot{E}}^1 = \dot{Q}\vec{\dot{E}}^0, \tag{12}$$

де $\dot{Q} = \begin{pmatrix} \dot{q}_{11} & \dot{q}_{12} \\ \dot{q}_{21} & \dot{q}_{22} \end{pmatrix}$ – матриця перетворення.

Оскільки вибір одного з ортів базису є довільним, то дія (12) може бути виконана нескінченною кількістю способів. На практиці найбільш поширеним є розклад у ПБ із

двох лінійно поляризованих або двох поляризованих за колом компонент, які, відповідно, мають назву лінійного та колового ПБ [1, 3, 5].

Матриця перетворення ЕМХ, визначеної в початковому ортогональному ПБ, який характеризується поляризаційними параметрами α_0, β_0, з параметрами ортів α_1, β_1 та α_2, β_2 має такий вигляд [1]:

$$\dot{Q}_\alpha = \begin{pmatrix} cos\alpha_1 & -jsin\alpha_2 \\ -jsin\alpha_1 & cos\alpha_2 \end{pmatrix}, \tag{13}$$

де α – кут еліптичності.

Іншою матрицею перетворення є матриця повороту будь-якого ПБ на кут β у фазовій площині хвилі:

$$Q_\beta = \begin{pmatrix} cos\beta_1 & sin\beta_2 \\ -sin\beta_1 & cos\beta_2 \end{pmatrix}. \tag{14}$$

Таким чином, розглянуті ПБ, визначені в них ПВ та їхні інваріанти можуть бути використані для вирішення завдань із виявлення та подальшого оброблення корисних сигналів на фоні завадових.

Взаємозв'язок коваріаційних матриць ПВ у різних ПБ антенної системи (випадок пасивної локації – ведення РМ)

Розглянемо взаємозв'язок між ПВ у різних ПБ. Для цього запишемо ПВ у формі поляризаційної матриці (ПМ) розміром 2 х 2 за аналогією до ПМ розсіювання [9], яку використовують у радіолокації, прирівнявши до нуля елементи матриці 1,2 та 2,1. Застосування такого подання ПВ пояснюється тим, що під час РМ поляризаційно чутлива антена приймає тільки ортогонально поляризовані складові сигналів, які випромінюють джерела радіовипромінювань.

ПМ у довільному базисі може бути визначена в такий спосіб [1]:

$$\dot{S}_\alpha = \dot{Q}_\alpha^{\,*} \cdot \dot{S}_Л \cdot \dot{Q}_\alpha^{\,T*}, \tag{15}$$

де $\dot{S}_Л$ – ПМ у лінійному базисі;

$\dot{Q}_\alpha$ – матриця переходу від лінійного ПБ до довільного, яка враховує вплив кута еліптичності α (14).

Аналогічним чином враховується вплив кута β на параметри ПМ у довільному базисі:

$$\dot{S}_\beta = Q_\beta^{\,*} \cdot \dot{S}_Л \cdot Q_\beta^{\,T*}, \tag{16}$$

де Q_β – матриця переходу від лінійного ПБ до довільного, яка враховує вплив кута орієнтації поляризаційного еліпса (15).

Тоді ПМ у довільному ПБ можна записати як добуток ПМ у лінійному базисі та відповідних матриць перерахунку:

$$\dot{S}_{\beta\alpha} = Q_{\beta}^{*}\dot{Q}_{\alpha}^{*} \cdot \dot{S}_{Л} \cdot \dot{Q}_{\alpha}^{T*}Q_{\beta}^{T*}. \quad (17)$$

Для коваріаційних матриць ПВ буде справедливим вираз

$$\dot{M}_{\beta\alpha} = \left[Q_{\beta}^{*} \otimes \dot{Q}_{\alpha}^{*}\right] \cdot \dot{M}_{Л} \cdot \left[\dot{Q}_{\alpha}^{T*} \otimes Q_{\beta}^{T*}\right], \quad (18)$$

де $\otimes$ – знак кронекерівського множення [7, 8].

Вираз (18) визначає зв'язок коваріаційної матриці в лінійному та довільному ПБ.

Висновки. Застосування в сучасних радіолокаційних станціях сигналів зі змінними поляризаційними параметрами спонукає до їх врахування в обробці для покращення показників виявлення, розпізнавання та пелентування засобів і комплексів РМ.

Запропонована в статті математична модель відтворює через параметри еліпса поляризації в лінійному ПБ ортогональні складові ПВ, які формуються на виході ортогональних поляризаційних каналів антенної системи. Вибірки ПВ, визначені в довільному ПБ, можуть бути перераховані в заданий ПБ шляхом математичних обчислень. За аналогією також є зв'язок між коваріаційними матрицями, розрахованими в різних ПБ.

Розроблену математичну модель доцільно використовувати для отримання об'єктивних результатів у ході дослідження алгоритмів виявлення, пелентування та розпізнавання джерел зі змінними поляризаційними параметрами сигналів під час ведення РМ у складних умовах сучасної радіоелектронної обстановки.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Казаков Е. Л. Радиолокационное распознавание космических объектов по поляризационным признакам. Одесса : ОИУМ, 1999. 230 с.

2. Giuli D. Polarization Diversity in Radars. Institute of Electrical and Electronics Engineers. 2005. P. 245–269.

3. Ільницький Л. Я., Сібрук Л. В., Габрусенко Є. І. Особливості колового ортогонального поляризаційного базису // Електроніка та системи управління. 2007. № 1. С. 54–61.

4. Нарбут В. П., Хмель В. Ф. Поляризация излучения зеркальных антенн / Київ : Вища школа, 1978. 279 с.

5. Ільницький Л. Я., Фецун А. В. Розкладання антенною системою електромагнітної хвилі на ортогонально поляризовані складові // Матер. VI Міжнар. наук.-техн. конф. АВІА-2003. Київ, 2003. С. 24.1–24.4.

6. Ilnytskiy L. Y., Fetsun A. V. The Requirements to Dipole Orientation on the Assumption of Polarization Orthogonalization // Proc. of the IV International Conference on Antenna Theory and Techniques. Sevastopol, 2003. P. 739–741. https://doi.org/10.1109/icatt.2003.1238852

7. Методика аналізу впливу поляризаційних характеристик антен на відмінності параметрів областей локалізації поляризаційних векторів сигналів та завад / О. О. Мартинчук, О. Д. Флоров, О. П. Гребенюк, С. А. Волювач // Системи озброєння і військова техніка. Харків : ХУПС, 2007. № 2 (10). С. 71–75.

8. Bronshtein I. N., Semendyayev K. A. Handbook of Mathematics. SPRINGER, New York Incorporated, 2007. 1109 p.
9. Сухаревский О. И., Василец В. А. Рассеяние электромагнитных волн воздушными и наземными радиолокационными объектами : монография. Харьков : ХУПС, 2009. 468 с.

Стаття надійшла до редакції 11.12.2024.

REFERENCES

1. Kazakov, E. L. (1999). *Radiolokatsionnoe raspoznavanie kosmicheskikh ob"ektov po poliarizatsionnym priznakam [Radar Recognition of Space Objects by Polarization Features]*. Odesa [in Russian].
2. Giuli, D. (2005). *Polarization Diversity in Radars.* Institute of Electrical and Electronics Engineers.
3. Ilnytskyi, L. Ya., Sibruk, L. V., & Habrusenko, Ye. I. (2007). Osoblyvosti kolovoho ortohonalnoho poliaryzatsiinoho bazysu [Features of the Circular Orthogonal Polarization Basis]. *Elektronika ta systemy upravlinnia [Electronics and Control Systems], 1,* 54–61 [in Ukrainian].
4. Narbut, V. P., & Khmel', V. F. (1978). *Poliarizatsiia izlucheniia zerkal'nykh antenn [Polarization of Specular Radiation Radiation]*. Kyiv [in Russian].
5. Ilnytskyi, L. Ya., & Fetsun, A. V. (2003). Rozkladannia antennoiu systemoiu elektromahnitnoi khvyli na ortohonalno poliaryzovani skladovi [Decomposition of an Electromagnetic Wave into Orthogonally Polarized Components by an Antenna System]. In *Mater. VI Mizhnar. nauk.-tekhn. konf. AVIA-2003 [Mater. VI International Scientific and Technical Conference AVIA-2003]*. (pp. 24.1–24.4). Kyiv [in Ukrainian].
6. Ilnytskyi, L. Ya., & Fetsun, A. V. (2003). The Requirements to Dipole Orientation on the Assumption of Polarization Orthogonalization. In *Proc. of the IV International Conference on Antenna Theory and Techniques.* Sevastopol. (pp. 739–741). https://doi.org/10.1109/icatt.2003.1238852
7. Martynchuk, O. O., Florov, O. D., Hrebeniuk, O. P., & Voliuvach, S. A. (2007). Metodyka analizu vplyvu poliaryzatsiinykh kharakterystyk anten na vidminnosti parametriv oblastei lokalizatsii poliaryzatsiinykh vektoriv syhnaliv ta zavad [Methodology for Analyzing the Influence of Polarization Characteristics of Antennas on the Differences in the Parameters of the Localization Areas of Polarization Vectors of Signals and Interference]. *Systemy ozbroiennia i viiskova tekhnika [Armament Systems and Military Equipment], 2* (10), 71–75. Kharkiv [in Ukrainian].
8. Bronshtein, I. N., & Semendyayev, K. A. (2007). *Handbook of Mathematics.* SPRINGER, New York Incorporated.
9. Sukharevskii, O. I., Vasilets, V. A. (2009). *Rasseianie elektromagnitnykh voln vozdushnymi i nazemnymi radiolokatsionnymi ob'ektami: monografiia [Scattering of Electromagnetic Waves by Air and Ground Radar Objects: Monograph]*. Kharkiv [in Russian].

ISSN 2076-1546

O. O. Hrebeniuk

MATHEMATICAL MODEL OF A SIGNAL WITH SPECIFIED POLARISATION PARAMETERS IN THE ORTHOGONAL POLARISATION BASIS

The experience of combat operations in the context of the large-scale invasion of Ukraine by the russian federation shows that the current level of development of electronic weapons is characterised by a wide variety of types and types of electronic means, the use of multifunctional means with widely variable signal parameters and operating modes. For example, modern (state-of-the-art) ground, air and sea radar stations use deliberate changes in the frequency, time and polarisation parameters of emitted signals in different modes of operation, depending on the tasks and conditions of a complex electronic environment. The presence of differences in the polarisation parameters of signals objectively creates prerequisites for their consideration in processing in order to improve the detection, recognition and direction finding performance of radio monitoring systems in a complex electronic environment. The approach is based on the use of antennas with orthogonal polarisation antenna elements, which allows signals to be represented as polarisation vectors. During the processing, it is necessary to take into account the influence of the polarisation characteristics of the antenna system on the parameters of the polarisation vector (change of the polarisation basis), which is relevant since the signals are received by the antenna system from different angular directions.

An important condition for obtaining objective results when studying the efficiency of polarisation processing algorithms is the use of a correct mathematical model of signals with given polarisation parameters in a certain orthogonal polarisation basis, as well as the use of signals from real radio equipment whose polarisation parameters can be determined in a polarisation basis other than the specified one. The article presents a mathematical model that allows expressing the field components through the parameters of the polarisation ellipse, and also gives expressions describing the relationship between polarisation vectors and their covariance matrices in different polarisation bases of the antenna system.

Keywords: *polarisation ellipse; polarisation characteristics; degree of polarisation; orthogonal polarisation basis; transformation matrix.*

УДК 004.39 DOI: 10.46972/2076-1546.2024.27.11

Ю. Л. Бондаренко, М. Д. Петрук, Д. Є. Ступак, І. А. Іщенко

СПОСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ТРИФАЗНОГО ГЕНЕРАТОРА ШЛЯХОМ АДАПТИВНОГО ПЕРЕРОЗПОДІЛУ ПОТУЖНОСТІ МІЖ ОДНОФАЗНИМИ СПОЖИВАЧАМИ

У статті описано спосіб підвищення ефективності роботи трифазного генератора шляхом застосування системи перерозподілу його потужності між однофазними споживачами. Проаналізовано можливі підходи та методи вирішення проблеми виникнення асиметрії навантаження джерел живлення. Запропоновано структурну схему системи електроживлення однофазних споживачів, яка реалізує рівномірне навантаження фаз у разі виникнення асиметрії навантаження. Обґрунтовано порядок функціонування такої схеми в різних режимах роботи системи перерозподілу потужності між споживачами, а також на його основі запропоновано алгоритм функціонування. Наведено обґрунтування схемного рішення адаптивної системи перерозподілу потужності між однофазними споживачами під керуванням однокристального мікроконтролера та розроблено варіант її принципової схеми. Сформульовано вимоги та на їх основі спроєктовано варіант побудови інвертора, який відповідає особливостям запропонованої структурної схеми за рівнем вхідної напруги. Розроблено та досліджено функціонування програмного коду роботи однокристального мікроконтролера за запропонованим алгоритмом. Наведено результати практичної перевірки функціонування запропонованої системи електроживлення, які продемонстрували підвищення ефективності трифазного генератора шляхом застосування системи перерозподілу його потужності між однофазними споживачами. З'ясовано, що модернізація пристрою можлива через реалізацію функції підмішування потужності. За результатами експерименту сформульовано напрямки подальших досліджень щодо удосконалення запропонованої схеми.

Ключові слова: *трифазний генератор; ефективність; асиметрія навантаження; адаптація; однокристальний мікроконтролер; перерозподіл потужності; широтно-імпульсна модуляція; диференційний захист; алгоритм перерозподілу потужності.*

Постановка проблеми в загальному вигляді. В умовах інтенсивного вогневого ураження противником об'єктів енергетичної інфраструктури нашої держави в ході збройної агресії російської федерації проти України гостро постало питання забезпечення енергопостачанням критично важливих військових та цивільних об'єктів за рахунок широкого застосування автономних джерел електроживлення (АДЖ). Значна частина АДЖ, які використовуються із цією метою, є трифазними генераторами різної потужності, які забезпечують можливість живлення як однофазних, так і трифазних споживачів електроенергії та характеризуються високими показниками економічності й енергоефективності.

© Ю. Л. Бондаренко, М. Д. Петрук, Д. Є. Ступак, І. А. Іщенко, 2024

У той же час більшість споживачів, зокрема й військового призначення, потребують саме однофазного живлення. Як правило, вони підключаються до однієї з фаз трифазного генератора. За такого підключення користувачів до АДЖ забезпечити рівномірне завантаження кожної з трьох фаз генератора практично не можливо через випадковий характер споживання ними електроенергії. Це обумовлено не тільки неможливістю здійснення контролю за підключенням споживачів до відповідної електромережі, але й через динамічні зміни рівня споживання ними в часі, що призводить до типової ситуації, коли в певний момент одна чи дві фази є перевантаженими, а решта – не завантаженими. При цьому завантаження кожної з фаз генератора в часі змінюється непередбачувано.

Нормальний режим функціонування трифазного генератора передбачає симетричне навантаження, за якого на кожну з фаз припадає приблизно однакова потужність (в ідеалі – 33% від загальної потужності). При цьому забезпечується найкраща ефективність його роботи.

У разі асиметричного навантаження фаз максимальна потужність на одну з них допускається не більше 40% від номінальної потужності генератора (за умови, що сумарне навантаження на двох інших не перевищує 30% від номінальної потужності). Це призводить до неефективного використання потужності трифазного генератора та ненормальних режимів роботи електромережі [2].

Отже, ефективність роботи трифазного генератора суттєво знижується внаслідок асиметрії навантаження, що створюється однофазними споживачами.

Аналіз останніх досліджень і публікацій. Підходи до вирішення завдання рівномірного розподілу однофазних споживачів для симетрування потужності наведено в різних джерелах.

У [1] розглянуто метод розподілу навантаження за фазами, що передбачає рівномірне підключення споживачів до кожної з трьох фаз. Але цей метод може бути застосований тільки в стаціонарних мережах з усталеним і контрольованим навантаженням.

У [5] описано метод оптимізації розподілу навантаження за рахунок аналізу середнього навантаження на кожну з фаз із подальшою перекомутацією споживачів між фазами. Проте це не дозволяє проводити оперативну перекомутацію споживачів у разі виникнення асиметричного навантаження.

У [1] запропоновано спосіб рівномірного завантаження фаз шляхом підключення споживачів до АДЖ через випрямляч Ларіонова, що не можливо застосувати для тих, які споживають змінну напругу.

У [7] розглянуто схему з подвійним перетворенням. Напруга спочатку випрямляється схемою Ларіонова після чого за допомогою інвертора формується 220 В 50 Гц. Основним недоліком такого методу є висока вартість його реалізації та необхідність застосування спеціалізованих інверторів (напруга після випрямлення становить близько 518 В) або знижувального трансформатора перед випрямленням.

У [1] як спосіб розв’язання проблеми асиметрії наведено метод моніторингу з подальшою корекцією. Регулярний моніторинг навантаження на кожній фазі дозволяє виявити дисбаланс і вжити заходи для його корекції. Це може включати перенесення деяких споживачів з однієї фази на іншу. Але цей метод підходить лише для стаціонарно розгорнутих систем.

У [3] досліджено метод усунення асиметрії шляхом під'єднання споживачів через симетруючий трансформатор, увімкнений за схемою «зигзаг-зірка». Такі трансформатори допомагають вирівняти навантаження між фазами, зменшуючи перекоси та втрати енергії. Вони працюють на основі принципів електромагнітної індукції, адаптуючи струми й напруги таким чином, щоб мережа залишалася збалансованою навіть за умов нерівномірного розподілу навантаження. При цьому розподіл потужності відбувається у співвідношенні 50% на перевантажену фазу і по 25% на інші. Також слід зазначити високу вартість та масогабаритні показники (такі пристрої мають великий розмір і вагу, що може ускладнювати їх транспортування, установлення та інтеграцію в наявні системи).

У [5] розглянуто використання автоматичних балансувальних пристроїв, які автоматично, умовно рівномірно розподіляють навантаження між фазами. Вони можуть бути корисними в системах із динамічним навантаженням, де споживання енергії змінюється з часом. Проте такі системи розгортають стаціонарно, крім того, вони потребують програмно керованих розподільчих шаф.

Отже, завдання підвищення ефективності роботи трифазного генератора в умовах асиметричного навантаження, створюваного однофазними споживачами, є актуальним, оскільки відомі підходи до симетрування навантаження не дозволяють вирішити проблему перерозподілу потужності трифазного генератора за умови динамічних змін її споживання однофазними споживачами.

Метою статті є розроблення способу підвищення ефективності роботи трифазного генератора в умовах асиметрії навантаження шляхом адаптивного перерозподілу потужності між однофазними споживачами.

Виклад основного матеріалу. Випадковість виникнення асиметрії навантаження між фазами трифазного генератора в ході живлення електромережі обумовлює два режими його роботи:

перший, коли генератор працює в умовах відсутності розбалансу потужності між фазами або якщо такий розбаланс не перевищує допустимих меж;

другий, коли є значний розбаланс навантаження з перевантаженням однієї чи двох фаз.

У першому режимі забезпечується максимальна ефективність роботи генератора, оскільки 99% виробленої енергії передається споживачам. Тому в такій ситуації необхідно реалізувати пряму каналізацію енергії генератора до споживачів без зайвих перетворень та втрат.

У другому режимі необхідно забезпечити, з одного боку, безперебійність постачання електроенергії споживачам (тобто унеможливити ситуацію аварійного вимкнення генератора через перенавантаження в одній із фаз), а з іншого – найефективнішу роботу генератора в умовах асиметричного навантаження, тобто передачу максимально можливого обсягу енергії до споживачів.

Отже, пропонований спосіб підвищення ефективності роботи генератора повинен реалізовувати: у першому режимі – передавання потужності від генератора до споживачів без будь-яких перетворень; у другому – можливість рівномірного завантаження усіх фаз за рахунок додаткових перетворень напруги живлення генератора.

Для того, щоб забезпечити роботу генератора в другому режимі, пропонуємо передбачити в складі схеми живлення споживачів такі елементи (рис. 1):

трифазний генератор як основне джерело електроенергії;

однофазні споживачі, поділені на групи, кожна з яких підключена до однієї з фаз генератора;

комутатор, який реалізує функцію підключення споживачів або безпосередньо до генератора (у першому режимі), або до перетворювача (у другому);

систему аналізу споживаної потужності, яка формує керуючий сигнал для управління роботою комутатора;

перетворювач, який дозволяє перетворити трифазну напругу генератора в однофазну, придатну для живлення споживачів у другому режимі.

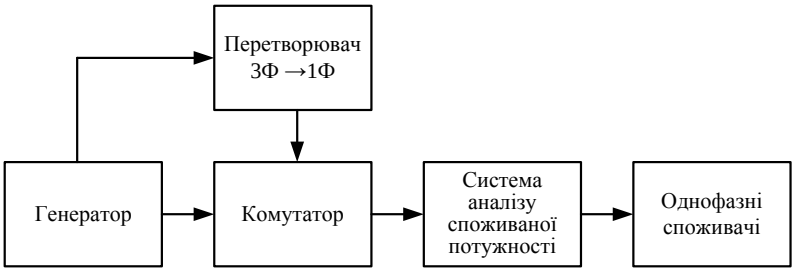


Рис. 1. Пропонована схема електроживлення споживачів

Щодо забезпечення рівномірності завантаження фаз найкращим варіантом перетворювача є випрямляч, побудований за схемою Ларіонова [1], яка придатна для живлення лише споживачів постійного струму. Для живлення споживачів змінного струму після випрямляча встановлюють інвертор. Більшість інверторів промислового зразка передбачає живлення вихідного каскаду інвертора напругою 310 В. Проте на виході схеми Ларіонова напруга становить 518 В, тому перед нею встановлюють трифазний знижувальний трансформатор (рис. 2а), що підвищує вартість схеми та збільшує її масу й габарити.

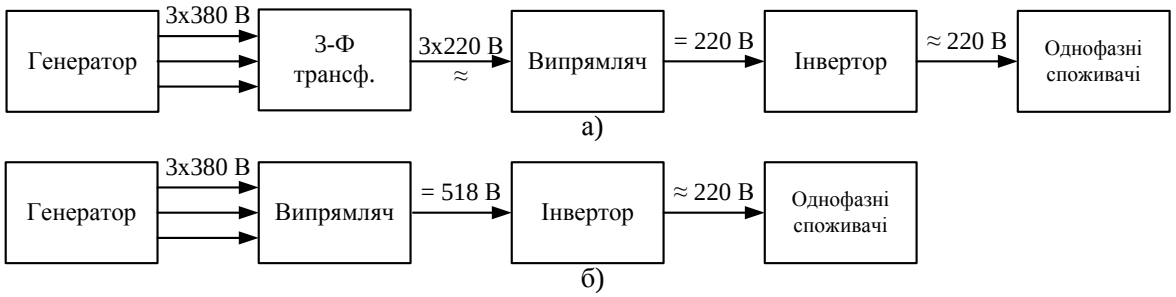


Рис. 2. Структурна схема системи перетворювача напруги 3Ф-1Ф

Для усунення зазначених недоліків та спрощення схеми перетворювача пропонуємо виключити з неї знижувальний трансформатор, але при цьому застосувати спеціалізований інвертор, який дозволяє його живлення напругою до 600 В. Його виготовлення обійдеться значно дешевше, ніж використання в схемі знижувального трансформатора.

Запропоновану структурну схему, що реалізує спосіб підвищення ефективності роботи трифазного генератора в умовах асиметричного навантаження, наведено на рис. 2б.

У виборі варіанта побудови спеціалізованого інвертора доречно зважати на те, що на вхід спеціалізованого інвертора з випрямляча буде надходити постійна напруга близько 518 В, тому немає сенсу застосовувати схему інвертора з двоступеневим перетворенням, що спрощує його схемне рішення. При цьому на виході інвертора повинен бути гармонічний сигнал 220 В 50 Гц. Для забезпечення такого вихідного сигналу пропонуємо спосіб його формування на основі широтно-імпульсної модуляції (ШІМ), шпаруватість якого описується функцією синуса. Це можливо реалізувати шляхом застосування як керувального елемента однокристального мікроконтролера (ОМК).

Для реалізації своїх функцій система аналізу споживаної потужності має містити у своєму складі блок вимірювання трифазного струму (БлВТС) та блок прийняття рішень (БлПР).

БлВТС – це набір датчиків, що повинні забезпечувати вимір струму кожної фази в межах від 0 А до максимального значення з урахуванням запасу (20% від максимального показника).

БлПР має забезпечувати виконання таких функцій: оброблення й перерахунок виміряних струмів у потужність, аналіз отриманої інформації та вироблення відповідного сигналу керування комутатором за відповідним алгоритмом прийняття рішень. Оскільки вихідним сигналом датчиків у БлВТС є напруга, описана поліномом, то отримання придатних для подальшої обробки даних потребує відповідних розрахунків. Це вимагає застосування у БлПР блоку обчислення на основі ОМК.

Схема побудови комутатора повинна відповідати таким вимогам:

забезпечувати можливість передачі електроенергії споживачам як прямо від генератора, так і від перетворювача;

мати достатньо високу швидкодію для уникнення ситуації переривання в живленні споживачів;

бути здатною забезпечити комутацію усієї потужності генератора на будь-яку з фаз у другому режимі;

працювати під управлінням сигналів від БлПР.

Запропоновану структурну схему реалізації способу підвищення ефективності роботи генератора в другому режимі наведено на рис. 3.

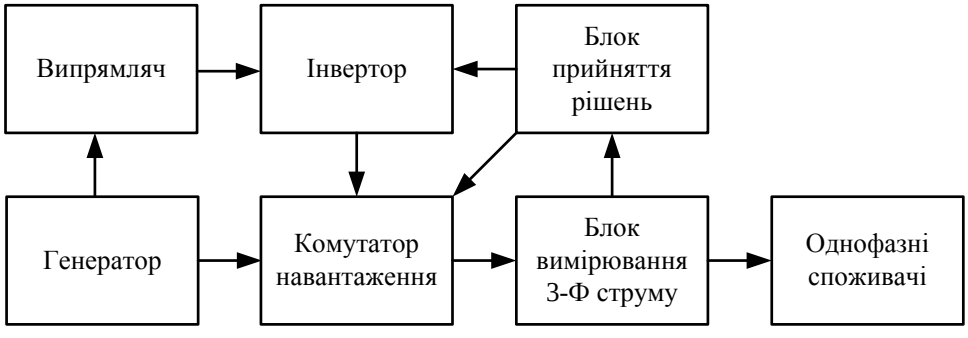


Рис. 3. Структурна схема системи перерозподілу потужності

Загальну принципову схему, що реалізує запропонований спосіб підвищення ефективності роботи трифазного генератора в умовах асиметричного навантаження, наведено на рис. 4.

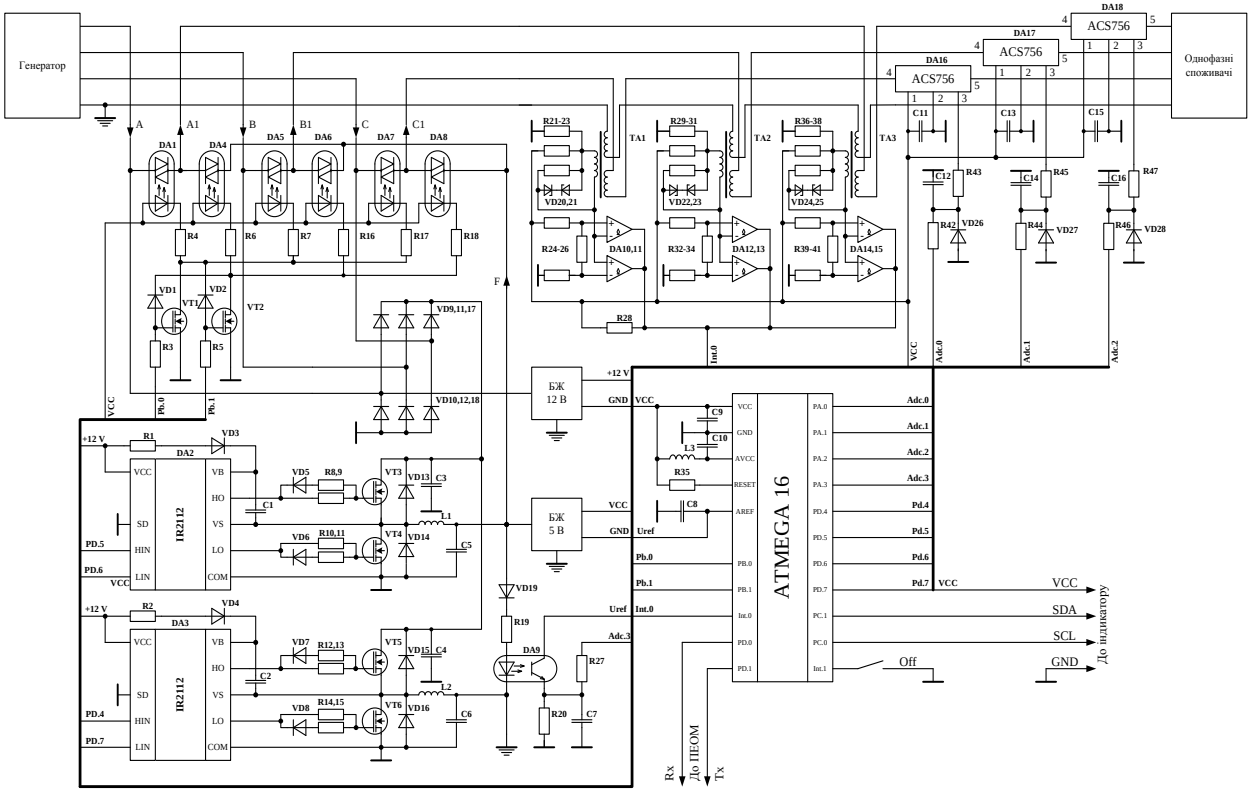


Рис. 4. Схема перерозподілу потужності однофазним споживачам

Напруга від генератора надходить на оптосимісторний комутатор (DA1, DA4-8) із шести інтегральних оптосимісторів, кожен із яких розраховано на напругу 800 В та робочий струм до 30 А. Кожен із них має забезпечувати комутацію всієї потужності для забезпечення перерозподілу в разі значної асиметрії навантаження. Для захисту від одночасного ввімкнення живлення від генератора та інвертора передбачено схему захисту, реалізовану на двох n-канальних польових транзисторах (VT1, VT2) та двох діодах (VD1, VD2).

Також вхідна напруга надходить на випрямляч, побудований за схемою Ларіонова на діодах *VD9-12,17,18* (*DSI30-08AS*), обраних із запасом за потужністю для зменшення їх нагріву та розрахованих на роботу зі струмами до 30 А, що витримують зворотну напругу до 800 В.

Для забезпечення максимальної ефективності перетворення в режимі перерозподілу потужності було обрано синхронну структуру інвертора. За основу для побудови взято дослідження [4]. Як керувальний елемент (генератор синфазних ШІМ сигналів) було взято 8-бітний ОМК фірми *ATMEL – ATMEGA* 16 через його доступність, наявність двоканального двопорогового 16-бітного таймера та 8-канального10-бітного аналогово-цифрового перетворювача (АЦП). Для керування потужними вихідними N-канальними *MOSFET* транзисторами (*FQD2N80*) схему доповнено інтегральним драйвером *IR2112*.

Рівень вихідної напруги інвертора контролюється через оптотранзистор DA9, що застосовано для гальванічної розв’язки. Живлення оптотранзистора здійснюється від вбудованого в ОМК опорного джерела живлення для більшої точності результату роботи АЦП. Напруга знімається з навантаження оптотранзистора R20 вбудованим в ОМК АЦП

та перераховується в значення напруги табличним методом (експериментально зняті значення відповідності напруг записано в таблицю).

Для контролю споживаного струму (потужності) в кожній із фаз встановлено спеціалізований датчик *ACS756* (на схемі DA16 – DA18), дані від якого надходять на входи ADC.0 – ADC.3 вбудованого в ОМК 10-бітного АЦП.

Для захисту особового складу від ураження струмом у схемі передбачено контроль диференційного струму, реалізований на диференціальних трансформаторах TA1–TA3 та компараторах DA10–DA15. Сигнал спрацювання будь-якого компаратора формує низький рівень на вході переривання INT0.

Крім того, для спрощення аналізу потужностей споживачів кожної із фаз та режиму роботи пристрій перерозподілу потужності доповнено виносним пультом з 16×2 дисплеєм, під'єднаним через канальний ущільнювач *PCF8574T*.

Для коректної роботи пристрою під керуванням ОМК слід організувати його роботу за таким алгоритмом (рис. 5).

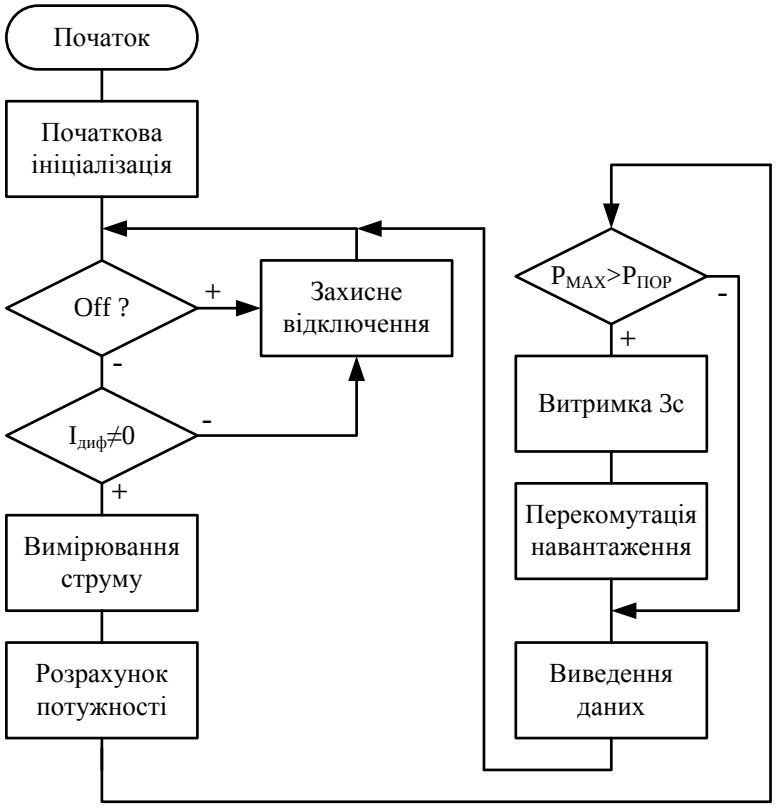


Рис. 5. Алгоритм роботи пристрою перерозподілу потужності

Робота починається з початкових налаштувань ОМК. Перед увімкненням навантаження проводиться аналіз дозволу роботи та відсутності диференційного струму.

Після ввімкнення навантаження відбувається вимірювання струмів споживання в кожній із фаз та їх подальший перерахунок у значення потужності. Якщо виміряні потужності не перевищують вказаного порога (вводиться завчасно для кожного генератора з його технічного опису), то віддається команда на роботу в першому режимі (без перерозподілу).

Якщо ж вимірювання виявили перевищення споживаної потужності на будь-якій із фаз, то починається відлік часу в три секунди (час на завершення перехідних комутаційних процесів) до переходу в другий режим роботи (комутація однофазних споживачів на роботу від інвертора).

Незалежно від способу живлення споживачів виводиться інформація про поточну споживану потужність на дисплей та ПЕОМ.

Для простоти написання програмного коду було використано середовище графічного програмування *Algorithm Builder for AVR 5.44.*

Головна програма починається з налаштування векторів переривань, встановлення режимів роботи портів, обнулення змінних, ініціалізації дозволу переривань та налаштування режимів роботи таймерів (рис. 6, А), під час якого відбувається встановлення коефіцієнта попереднього поділу частоти та режиму роботи до збігу з порогом. Ініціалізація змінних проводить їх обнулення та формує дозвіл переривань.

За перериванням від таймера розраховується чергове значення *sin(x)* із подальшим зчитуванням і видачею у відповідний порт ОМК з урахуванням поточного півперіоду.

Формування вибірок значення синуса відбувається шляхом зміни часу спрацювання одного із виходів ШІМ таймера № 1 (рис. 6, Е), переконфігурація якого проходить за законом синуса кожні чотири такти підпрограмою. 32 значення позитивної півхвилі *sin(x)* збережено в блоці (рис. 6, Є).

Контроль параметрів струму та напруги виконується за перериванням від таймера № 2 (рис. 6, Л). Кожне спрацювання таймера переналаштовує АЦП та викликає блок обробки переривань (рис. 6, Б). За кожним спрацюванням зберігаються відповідні дані.

Параметри амплітуди вихідного сигналу інвертора контролюються кожні пів секунди. У разі виявлення відхилення вихідної напруги підпрограмою (рис. 6, С) проводиться корекція коефіцієнта домноження часового еквівалента значення синуса (*Ku*). Якщо відхилення напруги незначне, то корекція не проводиться. Для домноження використовується окрема підпрограма (рис. 6, Д).

Якщо корекція напруги неможлива та є значне відхилення, яке не компенсується зміною коефіцієнта домноження значення синуса, то відбувається перехід до підпрограми зупинки роботи (рис. 6, І). Цей фрагмент коду також відповідає за відключення навантаження в разі виникнення диференційного струму.

Перед початком роботи та після виникнення нештатних ситуацій слід ініціювати запуск роботи від генератора, для чого передбачено переривання від входу *int1* (рис. 6, З).

Після проведення вимірювання струму у всіх трьох фазах проводиться перерахунок значення потужності підпрограмою (рис. 6, Н), після роботи якої виконується сортування за допомогою іншої підпрограми (рис. 6, М).

Після визначення P_{max} порівнюються відхилення потужностей (рис. 6, О). Якщо відхилення потужності було виявлено, то запускається таймер № 0, що відраховує 3 с. У разі зникнення відхилення в цьому проміжку виконується повторний запуск.

За спрацюванням таймера № 0 проводиться перекомутація навантаження на роботу від інвертора (рис. 6, К).

Корекція вихідної напруги в разі виявлення відхилення підпрограмою (рис. 6, С) відбувається шляхом домноження на коригувальний коефіцієнт підпрограмою (рис. 6, Д).

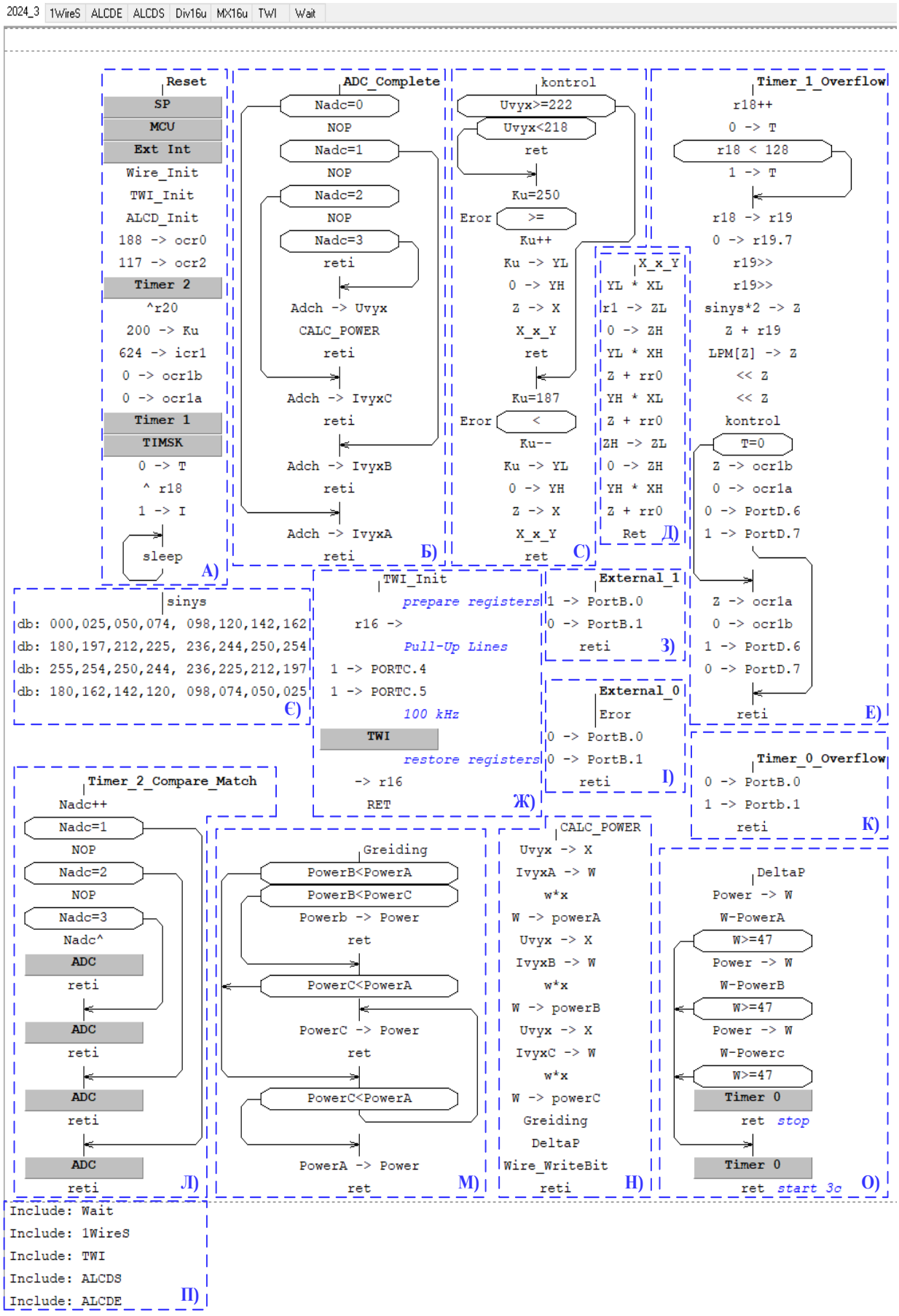


Рис. 6. Фрагменти коду програми

Для виведення даних використовується графічний дисплей 16 × 2 (підключеним через канальний ущільнювач *PCF8574T*), ініціалізація якого виконується підпрограмою (рис. 6, Ж). Також для роботи з ПЕОМ застосовуються додаткові бібліотеки, які під'єднуються до основного проєкту в блоці (рис. 6, П).

Для перевірки функціонування системи перерозподілу потужності було проведено моделювання із використанням дослідного пристрою, у складі якого були ввідна розподільна коробка, комутатор навантаження, канал вимірювання струмів кожної фази, канал вимірювання диференційного струму та напруги на виході генератора, інвертор та макетна плата з вбудованим мікроконтролером ATMEGA16.

Перевірка правильності функціонування та відлагодження розробленого дослідного зразка системи перерозподілу потужності проводилася в наметовому містечку з роботою від трифазного дизельного генератора FGD6500E3 загальною потужністю 6,5 кВт та допустимим навантаженням на 1 фазу 2,8 кВт.

У ході експлуатації дослідного зразка розподілювача потужності було перевірено його роботу з різними навантаженнями. У табл. 1 споживану потужність фази А наведено в стовпчику P_A, потужності фаз В та С – у P_B та P_C відповідно, сумарну потужність фаз – у P_Σ, вихідну напругу інвертора – у $U_{ВИХ}$, наявність диференційного струму – у $I_{ДИФ}$.

Таблиця 1

Результати перевірки роботи системи перерозподілу потужності

№ досліду	P_A (кВт)	P_B (кВт)	P_C (кВт)	P_Σ (кВт)	$U_{ВИХ}$ (В)	$I_{ДИФ}$ (мА)	Режим
1	0,98	0,93	0,97	2,88	221	< 1	Робота від генератора
2	0,00	0,07	0,43	0,5	223	< 1	Робота від генератора
3	1,73	0,92	0,41	3,06	221	< 1	Робота від генератора
4	2,35	1,56	0,93	4,84	222	< 1	Робота через інвертор
5	0,00	0,00	0,00	0,00	223	≈ 40	Аварійне відключення

Досліди 1 та 2 було проведено за незначного розбалансу та відсутності диференційного струму. Система перерозподілу потужності відповідно до заданого алгоритму скомутувала навантаження на роботу безпосередньо від генератора.

Досліди 3 та 4 проводилися за наявності розбалансу та відсутності диференційного струму. У досліді 3 максимальне навантаження на фазу не перевищувало програмно встановленого порога в 2 кВт.

Для визначення ефективності роботи в режимі перерозподілу потужності через інвертор було окремо оцінено коефіцієнт корисної дії (ККД) інвертора за різної потужності (табл. 2). Аналіз проводився на основі вимірювання постійного струму й напруги на вході та змінного струму й напруги (діючих значень) на виході.

Як видно з аналізу ККД інвертора, його ефективність знижується в разі збільшення генерованої потужності. Середній ККД становить близько 93%. Зниження також може бути пов'язане з неточністю вимірювань через місця включення приладів.

Таблиця 2

Аналіз ККД реалізованого інвертора з ШІМ-синусом

$I_{вх}$, А	$U_{вх}$, В	$P_{вх}$, Вт	$I_{вих}$, А	$U_{вих}$, В	$P_{вих}$, Вт	ККД, %
0,31	317	98	0,41	221	91,41	93,28
1,51	316	478	2,03	220	445,74	93,25
3,24	315	1021	4,30	221	951,06	93,15
5,65	313	1768	7,45	221	1645,48	93,07
7,32	312	2283	9,61	221	2124,33	93,05
8,94	312	2789	11,79	220	2594,05	93,01
13,17	310	4083	17,31	219	3791,88	92,87
17,41	308	5362	22,81	218	4973,26	92,75

Як бачимо, на ККД пристрою схеми перерозподілу потужності також впливає ККД випрямляча (близько 99%). Окрім того, слід враховувати втрати потужності (до 1%) на комутаторі навантаження. Тобто загальний ККД у разі роботи з рівномірним навантаженням становить близько 99%, а за розбалансу потужності – 92%.

Висновки. У ході практичної експлуатації було проведено перевірку роботи пристрою за відсутності розбалансу потужності та за умови, що потужність навантаження в каналах менше 2 кВт (тобто робота пристрою без перерозподілу потужності). ККД розподільчого пристрою становить 99%. Обмеження в 2 кВт пов’язані з генератором, що використовувався разом із системою перерозподілу.

Також було перевірено роботу пристрою за розбалансу потужності (Рф > 2 кВт), у такому разі ефективність системи перерозподілу знижувалась до 92%. З урахуванням цього за асиметричного навантаження вдалося отримати від 5,5 кВт генератора FGD6500E3 5,06 кВт вихідної потужності.

Слід відмітити також можливість під’єднання до ПЕОМ, що дозволяє зібрати статистичний розподіл навантаження для його подальшого перерозподілу між каналами.

Подальше вдосконалення пристрою можливе через реалізацію функції підмішування потужності.

Дослідження, проведені з використанням пристрою, показали ефективність застосування ОМК для створення системи перерозподілу потужності.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Попова І. О., Квітка С. О., Вовк О. Ю. Дослідження несиметричного режиму на роботу динамічного індуктивного навантаження // Праці Таврійського держ. агротехнологіч. ун-ту : наукове фахове видання. Запоріжжя : ТДАТУ, 2023. Вип. 23, Т. 1. С. 179–187. https://doi.org/10.31388/2078-0877-2023-23-1-179-187

2. ДСТУ EN 50160:2023 Характеристики напруги електропостачання в електричних мережах загальної призначеності (EN 50160:2022, IDT). Київ, 2023. С. 5–44.

3. Шевченко В. П., Бєлікова Л. Я. Трансформатори : навч. посіб. для студентів ВНЗ. Одеса : Одеськ. нац.. політехнічн. ун-т, 2001. 128 с. URL: http://elib.chdtu.edu.ua/e-books/4872 (дата звернення: 25.10.2024).

4. Інвертор на базі мікроконтролера AVR / І. Білюк, О. Савченко, Р. Філоненко та ін. // Scientific Collection «InterConf». 2024. С. 326–329.
5. Кириленко О. В. Заходи та засоби перетворення енергетики України на інтелектуальну екологічно безпечну систему // Вісник НАН України. 2022. № 3. С. 18–23. https://doi.org/10.15407/visn2022.03.018
6. Вплив відновлюваних джерел енергії на роботу електроенергетичної системи / О. М. Довгалюк, О. П. Лазуренко, Ш. Н. Саїдов, І. С. Яковенко // Енергоефективність та енергетична безпека електроенергетичних систем (EEES-2018) : матеріали II Всеукр. наук.-техн. конф. 2018. С. 52–54.
7. Качан Ю. Г., Шрам О. А. Щодо структури енергоефективної електромережі промислового підприємства з джерелами розосередженої генерації // Вісник ВПІ. Серп. 2024. Вип. 4. С. 54–59. https://doi.org/10.31649/1997-9266-2024-175-4-54-59
8. Лисенко А. І. Вибір інвертора для сонячних панелей. Порівняння моделей різних виробників // Сучасні проблеми електроенерготехніки та автоматики : Міжнар. наук.-техн. журнал. URL: http://jour.fea.kpi.ua/article/view/131593/127784 (дата звернення: 27.10.2024).

Стаття надійшла до редакції 20.12.2024.

REFERENCES

1. Popova, I. O., Kvitka, S. O., & Vovk, O. Yu. (2023). Doslidzhennia nesymetrychnoho rezhymu na robotu dynamichnoho induktyvnoho navantazhennia [Research of the Asymmetrical Mode of Operation of a Dynamic Inductive Load]. *Pratsi Tavriiskoho derzhavnoho ahrotekhnolohichnoho universytetu: naukove fakhove vydannia [Proceedings of the Tavria State Agrotechnological University: scientific professional publication], Iss. 23,* Vol. 1, 179–187. Zaporizhzhia. https://doi.org/10.31388/2078-0877-2023-23-1-179-187 [in Ukrainian].
2. DSTU EN 50160:2023 Kharakterystyky napruhy elektropostachannia v elektrychnykh merezhakh zahalnoi pryznachenosti [Characteristics of the Voltage of the Power Supply in General Purpose Electrical Networks]. (EN 50160:2022, IDT). Kyiv [in Ukrainian].
3. Shevchenko, V. P., & Bielikova, L. Ya. (2001). *Transformatory [Transformers]*. Odesa. Retrieved from http://elib.chdtu.edu.ua/e-books/4872 [in Ukrainian].
4. Bilyuk, I., Savchenko, O., & Filonenko, R., et al. (2024). Invertor na bazi mikrokontrolera AVR [Inverter based on AVR microcontroller]. In *Scientific Collection «InterConf»*. (pp. 326–329) [in Ukrainian].
5. Kyrylenko, O. V. (2022). Zakhody ta zasoby peretvorennia enerhetyky Ukrainy na intelektualnu ekolohichno bezpechnu systemu [Measures and Means of Transforming the Energy Sector of Ukraine into an Intelligent Environmentally Safe System]. *Visnyk NAN Ukrainy [Bulletin of the NAS of Ukraine], 3,* 18–23. https://doi.org/10.15407/visn2022.03.018 [in Ukrainian].
6. Dovhaliuk, O. M., Lazurenko, O. P., Saidov, Sh. N., & Yakovenko, I. S. (2018). Vplyv vidnovliuvanykh dzherel enerhii na robotu elektroenerhetychnoi systemy [The Impact of Renewable Energy Sources on the Operation of the Electric Power System]. In *Enerhoefektyvnist ta enerhetychna bezpeka elektroenerhetychnykh system (EEES-2018): materialy II Vseukr.*

nauk.-tekhn. konf. [Energy Efficiency and Energy Safety of Electric Power Systems (EEES-2018): materials of the II All-Ukrainian Scientific and Technical Conference]. (pp. 52–54) [in Ukrainian].
7. Kachan, Yu. H., & Shram, O. A. (August, 2024). Shchodo struktury enerhoefektyvnoi elektromerezhi promyslovoho pidpryiemstva z dzherelamy rozoseredzhenoi heneratsii [Regarding the Structure of an Energy-Efficient Power Grid of an Industrial Enterprise with Distributed Generation Sources]. *Visnyk VPI [Bulletin of the VPI]*, *4*, 54–59. https://doi.org/10.31649/1997-9266-2024-175-4-54-59 [in Ukrainian].
8. Lysenko, A. I. (n.d.). Vybir invertora dlia soniachnykh panelei. Porivniannia modelei riznykh vyrobnykiv [Choosing an Inverter for Solar Panels. Comparison of Models from Different Manufacturers]. *Suchasni problemy elektroenerhotekhniky ta avtomatyky: Mizhnarodnyi nauk.-tekhn. zhurnal [Modern Problems of Electrical Engineering and Automation: International Scientific and Technical Journal]*. Retrieved from http://jour.fea.kpi.ua/article/view/131593/127784 [in Ukrainian].

Y. L. Bondarenko, M. D. Petruk, D. E. Stupak, I. A. Ishchenko

THE METHOD OF INCREASING THE EFFICIENCY OF A THREE-PHASE GENERATOR THROUGH ADAPTIVE REDISTRIBUTION OF POWER BETWEEN SINGLE-PHASE CONSUMERS

The article describes a method of increasing the efficiency of the three-phase generator by applying a system of redistribution of its power between single-phase consumers. Possible approaches and methods for solving the problem of asymmetry of load of power supplies are analyzed. The structural scheme of the power supply system of single-phase consumers is proposed, which realizes a uniform load of phases in the event of load asymmetry. The order of operation of the scheme in different modes of operation of the power redistribution system between consumers is substantiated and on its basis the functioning algorithm is proposed. The substantiation of the circuit solution of the adaptive power redistribution system between single-phase consumers under the control of a single-chip microcontroller is provided and a version of its circuit diagram is developed. The requirements are formulated and on their basis the option of constructing an inverter is designed, which corresponds to the features of the proposed structural scheme according to the level of input voltage. The functioning of the program code of the single-chip microcontroller according to the proposed algorithm has been developed and investigated. The results of practical verification of the functioning of the proposed power supply system are presented, which demonstrated an increase in the efficiency of a three-phase generator by applying a system of redistribution of its power between single-phase consumers. According to the results of the experiment, the directions of further research on the improvement of the proposed scheme are formulated.

Keywords: *three-phase generator; efficiency; load asymmetry; adaptation; single-chip microcontroller; redistribution of power; pulse width modulation; differential protection; power redistribution algorithm.*

Ахтирцева Владислава Сергіївна – доктор філософії, заступник начальника науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0002-0624-2284
Наукові інтереси:
– соціальна інженерія;
– методи імітаційного моделювання;
– OSINT.

Бикова Лариса Григорівна – ад'юнкт науково-організаційного відділу Військової академії (м. Одеса). ORCID: 0000-0001-7360-0240
Наукові інтереси:
– прикладна механіка в озброєнні та військовій техніці;
– моделювання та параметризація.

Бондаренко Юрій Леонідович – кандидат технічних наук, начальник кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0003-0395-4275
Наукові інтереси:
– оптимізація функціонування складних технічних систем;
– інформаційні технології багатокритерійної оптимізації систем та об'єктів;
– створення нових та удосконалення наявних систем електрозабезпечення.

Весельська Аміна Романівна – слухач Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0003-7704-1804
Наукові інтереси:
– психологічні операції.

Гребенюк Олег Олегович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0002-3097-3992
Наукові інтереси:
– системи радіомоніторингу.

Грищук Ольга Михайлівна – аспірантка Національного авіаційного університету. ORCID: 0000-0001-6957-4748
Наукові інтереси:
– кібербезпека та захист інформації.

Заєць Юрій Олексійович – заступник начальника факультету Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0000-6763-7813
Наукові інтереси:
– автоматизовані системи управління.

Зімчук Ігор Валерійович – кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0003-9372-5720
Наукові інтереси:
– синтез алгоритмів оцінювання та управління для автоматизованих технічних систем.

Ісмаілова Неллі Петрівна – доктор технічних наук, професор, професор кафедри Військової академії (м. Одеса). ORCID: 0000-0003-0181-4420

Наукові інтереси:
– прикладна механіка в озброєнні та військовій техніці;
– геометричне моделювання технічних форм та автоматизація їх проєктування.

Іщенко Іван Анатолійович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0007-7150-1653
Наукові інтереси:
– застосування мікропроцесорних пристроїв у системах електропостачання;
– застосування мікропроцесорів для модернізацій озброєння та військової техніки;
– дослідження шляхів оптимізації систем альтернативного живлення;
– математичне моделювання складних технічних систем.

Ковба Микола Вікторович – заступник начальника кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного. ORCID: 0000-0003-1816-1016
Наукові інтереси:
– проєктування та виготовлення мобільних робототехнічних систем.

Корченко Олександр Григорович – член-кореспондент НАН України, лауреат Державної премії України в галузі науки і техніки, заслужений діяч науки і техніки України, доктор технічних наук, професор, перший проректор Державного університету інформаційно-комунікаційних технологій. ORCID: 0000-0003-3376-0631
Наукові інтереси:
– кібербезпека та захист інформації;
– інформаційні технології.

Лобода Вероніка Вікторівна – старший науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0002-3535-0233
Наукові інтереси:
– інформаційні технології;
– стратегічні комунікації.

Мікрюков Іван Станіславович – ад'юнкт науково-організаційного відділу Військової академії (м. Одеса). ORCID: 0009-0001-4303-4038
Наукові інтереси:
– прикладна механіка в озброєнні та військовій техніці;
– моделювання та параметризація.

Мірошніченко Сергій Іванович – викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0007-2076-041X
Наукові інтереси:
– автоматизовані системи управління;
– інформаційні системи.

Охрімчук Володимир Васильович – кандидат технічних наук, професор кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0001-7518-9993
Наукові інтереси:

– кібербезпека;
– мережеві технології;
– інформаційні технології.

Охрімчук Інна Антонівна – викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0009-2314-1723
Наукові інтереси:
– інформаційні технології;
– автоматизоване оброблення інформації;
– комп'ютерна графіка.

Петрук Микола Дмитрович – кандидат технічних наук, доцент, професор кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0004-3115-1255
Наукові інтереси:
– удосконалення роботи автономних джерел електроживлення;
– пошук шляхів застосування сучасної елементної бази для розробки радіоелектронної апаратури.

Пількевич Ігор Анатолійович – заслужений працівник освіти України, доктор технічних наук, професор, професор кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0001-5064-3272
Наукові інтереси:
– математичне моделювання складних систем та процесів;
– боротьба в електромагнітному середовищі;
– кіберзахист.

Пулеко Ігор Васильович – кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова. ORCID 0000-0001-8875-017X
Наукові інтереси:
– моделювання та обробка інформації в складних технічних системах;
– інформаційні технології в управлінні групами розподілених динамічних об'єктів;
– штучний інтелект в технічних системах;
– інтернет речей.

Рикун Віталій Леонідович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0006-3264-9201
Наукові інтереси:
– математичне моделювання складних технічних систем;
– дослідження електромеханічних систем.

Свистунович Іван Володимирович – викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0004-6832-6397
Наукові інтереси:
– математичне моделювання складних технічних систем;
– дослідження систем електропостачання та релейного захисту.

Ступак Дмитро Євгенійович – кандидат педагогічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0000-0001-7638-3982

Наукові інтереси:
– теорія і методика професійної освіти у вищій школі;
– професійна компетентність фахівця;
– дослідження шляхів підвищення ефективності систем електропостачання.

Тарасенко Владислав Олександрович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0005-6267-9455
Наукові інтереси:
– інформаційні технології радіозв'язку.

Тимчук Сергій Віталійович – кандидат технічних наук, доцент кафедри Житомирського військового інституту імені С. П. Корольова. ORCID 0000-0002-4096-9946
Наукові інтереси:
– комплекси та засоби радіоелектронної розвідки.

Трутнєв Сергій Геннадійович – старший викладач кафедри Військової академії (м. Одеса). ORCID: 0000-0002-6107-7920
Наукові інтереси:
– методологія визначення похибок в системах імітаційного моделювання;
– математичні операції з цифрами, поданими у двійковому коді;
– підвищення точності в обчисленні чисел з плаваючою комою.

Чумакевич Віктор Олександрович – кандидат технічних наук, доцент, викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID 0000-0002-5773-393X
Наукові інтереси:
– функціонально-стійкі системи з керуванням, яке відновлюється;
– моделювання та спостереження геотехнічних процесів;
– математичне моделювання складних технічних систем.

Шапар Тетяна Миколаївна – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0008-0497-7675
Наукові інтереси:
– синтез алгоритмів оцінювання та управління для автоматизованих технічних систем.

Шестак Ігор Михайлович – викладач кафедри Житомирського військового інституту імені С. П. Корольова. ORCID: 0009-0007-0640-2210
Наукові інтереси:
– математичне моделювання складних технічних систем;
– дослідження систем електропостачання та релейного захисту.

Н А У К О В Е В И Д А Н Н Я

ПРОБЛЕМИ СТВОРЕННЯ, ВИПРОБУВАННЯ, ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЇ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Збірник наукових праць

Випуск 27 (І)

Видавничий оригінал виготовлений
у науково-організаційному відділенні ЖВІ

Редактор: **Л. М. Марищук**
Комп'ютерна верстка та макетування **Л. М. Марищук**
Дизайн і макет обкладинки **О. Ю. Тофанчук**

Свідоцтво про реєстрацію серія ДК № 7355 від 9 червня 2021 року.
Підписано до друку 27.12.2024. Формат 60 × 84 / 8.
Ум. друк. арк. 16,28. Тираж 50 прим. Зам. 1013 опер.

Друкарня ЖВІ

10004, м. Житомир, просп. Миру, 22