МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

ПРОБЛЕМИ СТВОРЕННЯ, ВИПРОБУВАННЯ, ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЇ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

18

Житомир
2020

Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : збірник наукових праць. Вип. 18 / Житомирський військовий інститут імені С. П. Корольова. – Житомир : ЖВІ, 2020. – 136 с. – ISSN 2076-1546. https://doi.org/10.46972/2076-1546.2020.18.

Рекомендовано до друку рішенням вченої ради Житомирського військового інституту імені С. П. Корольова, протокол № 5 від 18.12.2020.

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

ISSN 2076-1546

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

Свідоцтво про державну реєстрацію КВ № 21859-11759 ПР від 21.12.2015.

ЗМІСТ

УДК 621.396.722 DOI: 10.46972/2076-1546.2020.18.01

С. П. Фриз, О. В. Кальватинський, Р. О. Авсієвич

МОДЕЛЬ СИСТЕМИ ВИЗНАЧЕННЯ ВИДУ ФАЗОВОЇ МАНІПУЛЯЦІЇ ТА СИМВОЛЬНОЇ ШВИДКОСТІ В РАДІОЛІНІЯХ КОСМІЧНИХ СИСТЕМ

У статті запропоновано модель універсальної автоматизованої системи визначення виду фазової маніпуляції та символьної швидкості для прийому наземними засобами потоку даних, що передаються в радіолініях низькоорбітальних космічних систем в умовах часткової апріорної невизначеності.

Актуальність проведення дослідження за обраною тематикою полягає в тому, що в останнє десятиліття фіксується значне збільшення кількості космічних систем, які експлуатуються на низьких навколоземних орбітах. Зазначене зумовлює збільшення різноманіття структур радіоліній космічних систем, що створює часткову апріорну невизначеність відносно параметрів радіосигналів, які транслюються цими системами. Водночас функціонування космічних систем на низьких навколоземних орбітах накладає обмеження на тривалість сеансу зв'язку, що в умовах часткової апріорної невизначеності параметрів радіосигналу ускладнює налаштування наземної демодулюючої апаратури.

У статті наведено можливий варіант побудови структурної схеми універсальної автоматизованої системи визначення виду фазової маніпуляції та символьної швидкості. Описано принцип роботи системи та обґрунтовано її працездатність шляхом математичного моделювання процесів.

Розглянута модель універсальної автоматизованої системи визначення виду фазової маніпуляції та символьної швидкості дозволяє в режимі часу, наближеному до реального, визначати: номінальне значення центральної несучої частоти радіосигналу, ширину спектра радіосигналу, символьну швидкість та один із трьох видів фазової маніпуляції (BPSK, QPSK, 8PSK).

За результатами проведених розрахунків встановлено, що досліджувана система може використовуватися під час прийому потоку даних від космічних систем, які експлуатуються на низьких навколоземних орбітах. Крім того, вона може застосовуватися для визначення основних параметрів радіосигналів й інших систем з радіолініями з фазовою маніпуляцією.

Подальші дослідження за обраною тематикою будуть спрямовані на вивчення можливості розширення кількості видів маніпуляцій, що можуть автоматично визначатися запропонованою системою.

Ключові слова: *радіолінія; радіосигнал; фазова маніпуляція; символьна швидкість; космічні системи; низька навколоземна орбіта; автоматизація.*

Постановка проблеми в загальному вигляді. Радіолінії космічних систем характеризуються такими параметрами: центральна несуча частота радіосигналу, ширина спектра радіосигналу, значення відношення рівня потужності радіосигналу до рівня потужності шумів, вид маніпуляції та значення символьної швидкості. Визначення зазначених параметрів радіолінії необхідне для проведення подальшої демодуляції

наземними засобами прийнятого потоку даних від космічних систем. Залежно від цільового призначення космічної системи використовуються радіочастоти в межах від 1,4 ГГц до 50 ГГц. Крім того, у космічних системах застосовується значне різноманіття фазової та амплітудно-фазової видів маніпуляції: BPSK, QPSK, OQPSK, DQPSK, 8PSK, 8QAM, 16QAM, 16APSK, 32QAM, 32APSK, 64QAM, 64APSK та інші. Також використовується широкий діапазон символьних швидкостей у межах від 2 кБод до 450 МБод. Водночас у сучасних космічних системах застосовують адаптивні режими роботи, що передбачають зміну параметрів радіолінії під час трансляції потоку даних, обумовлену необхідністю забезпечення сталого значення ймовірності виникнення бітової помилки під впливом різного роду завад. Усе це значно ускладнює виконання завдань із прийому інформації від космічних систем в умовах апріорної невизначеності параметрів радіоліній. Тому актуальною є потреба у створенні універсальних автоматизованих систем з визначення параметрів радіоліній.

Аналіз останніх досліджень і публікацій. Наукометричні бази містять велику кількість публікацій щодо використання різних методів пошуку номінальних значень центральних несучих частот радіосигналів на фоні шумів. Зазначеному сприяла розробка радіосистем із псевдовипадковим перестроюванням радіочастот, а також розробка програмно-обумовлених засобів передачі інформації. Зокрема, різні автори із цією метою пропонують використовувати метод автокореляційної функції [1, 2], метод аналізу переходів сигналу через нуль [2], дискретне перетворення Фур'є (ДПФ) [1], алгоритм Герцеля [1], параметричні та непараметричні методи спектрального оцінювання [1, 4], перетворення Вінгера – Вілла [3], вейвлет-перетворення [5, 6], віконні перетворення на основі ДПФ, метод періодограм, методи авторегресійних спектральних оцінювань, математичний апарат нечіткої логіки [1].

Водночас у відкритих публікаціях питанням автоматичного визначення виду маніпуляції та символьної швидкості приділялося значно менше уваги. Дане питання особливо гостро стоїть під час розробки наземних комплексів прийому даних в умовах часткової апріорної невизначеності структур радіоліній космічних систем, що експлуатуються на низьких навколоземних орбітах. Зазначене обумовлено тим, що подібні системи мають коротку тривалість сеансу зв'язку та використовують при цьому високі швидкості передачі даних. Крім того, є жорсткі вимоги щодо тривалості обробки прийнятих даних від подібних космічних систем. Враховуючи вказане, нижче розглянемо структурну схему й математичну модель універсальної автоматизованої системи визначення виду маніпуляції та символьної швидкості, що дозволятимуть здійснювати обробку даних від низькоорбітальних космічних систем з урахуванням наведених вимог.

Також за результатами аналізу робіт [8–10] з'ясовано, що в низькоорбітальних космічних системах широкого застосування набули радіолінії з такими видами маніпуляції: BPSK, QPSK, 8PSK та їх різновиди. З урахуванням цього розглянемо рішення для обробки радіосигналів тільки з наведеними видами фазової маніпуляції.

Формулювання завдання дослідження. Метою статті є розробка та дослідження структурної схеми й математичної моделі для автоматичного визначення виду фазової маніпуляції та символьної швидкості в прийнятому наземними засобами потоці даних від космічних систем, що експлуатуються на низькій навколоземній орбіті й використовують радіолінії з фазовою маніпуляцією.

Виклад основного матеріалу. Очевидно, що для визначення виду фазової маніпуляції доцільно використовувати схеми, що містять у своєму складі фазовий детектор (ФД) та систему фазового автоматичного підстроювання частоти (ФАПЧ). Також для визначення виду маніпуляції та символьної швидкості необхідно попередньо встановити номінальні значення несучої частоти та ширину спектра радіосигналу. В умовах необхідності здійснення обробки короткотривалих високошвидкісних радіосигналів у режимі часу, наближеному до реального, розв'язання вказаних задач доцільно здійснювати методом ДПФ. Для реалізації зазначених вимог можна використати схему на основі петлі рішень [11], зображену на рис. 1.

Структурна схема, наведена на рис. 1, дозволяє швидко визначати значення центральної несучої частоти та ширини спектра радіосигналу, а потім шляхом підбору вид фазової маніпуляції та значення символьної швидкості.

З рис. 1 видно, що запропонована структурна схема універсальної автоматичної системи визначення виду фазової маніпуляції та символьної швидкості на основі петлі рішень складається з таких елементів: системи ФАПЧ, системи прийняття рішення (СПР), модуля перетворення Фур'є та аналізу сигналів (МПФАС).

Система ФАПЧ у схемі зібрана на основі: двох змішувачів; цифрового генератора частот, керованого напругою (NCO – англ. *numerically controlled oscillator*); фільтрів низьких частот (ФНЧ), ФД та слідкувального фільтра (СФ).

Між системою ФАПЧ та МПФАС розміщується СПР, до складу якої входять модуль обчислення коефіцієнтів та модуль виявлення захоплення.

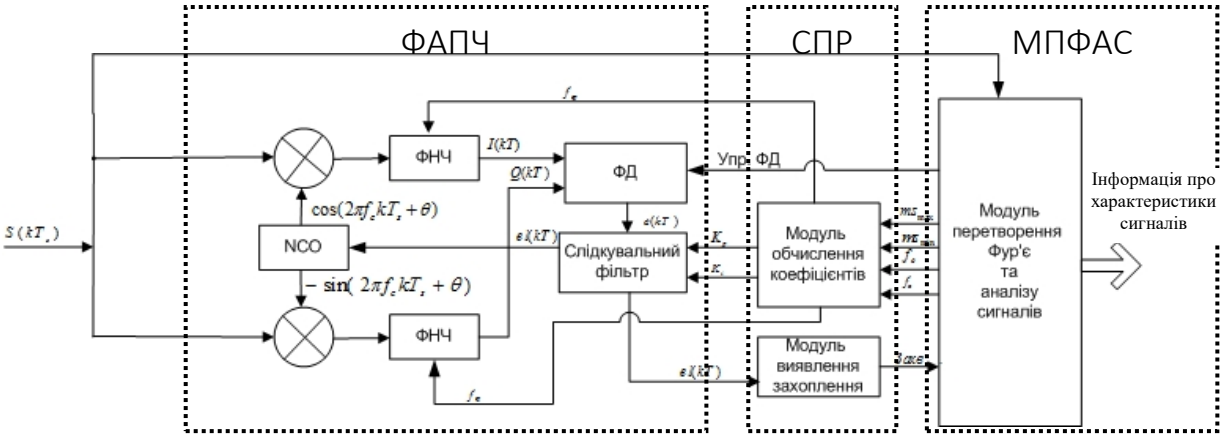


Рис. 1. Структурна схема універсальної автоматичної системи визначення виду фазової маніпуляції та символьної швидкості на основі петлі рішень

Принцип роботи схеми можна описати таким чином: на вхід схеми подаються відліки $S(kTs)$ з виходу аналого-цифрового перетворювача (АЦП). Одночасно вони надходять на входи системи ФАПЧ та МПФАС. У системі ФАПЧ змішувачі здійснюють перемноження вхідних відліків з ортогональними сигналами NCO, початкові параметри якого задає СФ, виходячи з розрахунків, проведених у системах МПФАС та СПР. На виході змішувачів формуються дві квадратурні складові вхідного сигналу. У подальшому квадратурні складові через ФНЧ подаються на вхід ФД, налаштування якого здійснюється на основі розрахунків, проведених МПФАС. З виходу ФД на СФ подається сигнал розузгодження, який у подальшому оцінюється модулем виявлення захоплення. Значення сигналу

розузгодження обирається з урахуванням виду маніпуляції та символьної швидкості. У разі, якщо сигнал розузгодження перевищує попередньо обраховане значення, СПР подає на МПФАС команду про необхідність зміни обрахованих параметрів, які після перерахунку знову подаються на СФ для зміни налаштування NCO.

МПФАС визначає центральну несучу частоту та ширину спектра радіосигналу, використовуючи метод ДПФ. Зазначені дані потрібні для коректного налаштування системи ФАПЧ, а також розрахунку значення сигналу розузгодження. Якщо сигнал розузгодження на виході ФД не перевищує попередньо розрахованого значення, то приймається рішення, що параметри радіосигналу визначено коректно, тоді СПР формує сигнал про видачу користувачу обчислених параметрів.

Зазначений процес можна описати алгоритмом, наведеним на рис. 2.

Рис. 2. Алгоритм роботи універсальної автоматизованої системи визначення виду фазової маніпуляції та символьної швидкості

Розглянемо математичну модель запропонованої універсальної автоматизованої системи визначення виду фазової маніпуляції та символьної швидкості.

Як зазначено вище, виявлення корисного сигналу здійснюється шляхом аналізу масиву даних обчислень перетворення Фур'є:

$$X(m)=\sum_{n=0}^{N-1} x(n)\cdot e^{-j2\pi nm/N}, \tag{1}$$

де $X(m)$ – m -й компонент ДПФ;

m – індекс ДПФ у частотній області;

$x(n)$ – послідовність вхідних відліків;

n – часовий індекс вхідних відліків;

N – кількість відліків вхідної послідовності та частотних відліків результату ДПФ.

Компонент $X(m)$ має комплексну форму, його описують виразом

$$X(m)=X_r(m)+jX_i(m). \tag{2}$$

Для виявлення корисного сигналу необхідна амплітуда сигналу, яку визначають за таким виразом:

$$Xam(m)=\sqrt{X_r(m)^2+X_i(m)^2}\ . \tag{3}$$

За відсутності корисного сигналу необхідно визначити рівень шумів у частотній смузі прийому як

$$Ams=\frac{\sum_{n=0}^{N-1} Xam(n)}{N-1}, \tag{4}$$

де *Ams* – рівень шумів у прийнятій смузі частот.

Визначення рівня шумів необхідно проводити перед сеансом прийому інформації. Пошук корисного сигналу зводиться до визначення максимального значення амплітуди сигналу $Xam(m)$.

Слід вважати, що корисний сигнал виявлено та рівень сигналу достатній для демодуляції, якщо виконується умова $Xam_{max}(m)>G$, де G – поріг амплітуди, а m відповідає центральній частоті спектра сигналу. Відомо, що для стійкого прийому інформації ймовірність похибки повинна бути не гірше ніж $P = 10^{-3}$. Для цього необхідно забезпечити відношення сигнал/шум на вході приймача $E_o/N_o > 6$ *dB* [12].

Визначивши максимальний рівень сигналу $Xam_{max}(m)$ та рівень шумів *Ams*, можна розрахувати відношення сигнал/шум E_o/N_o (dB) за таким виразом:

$$E_o/N_o = 20\times log_{10}\left(\frac{0{,}707\times Xam_{max}(m)}{Ams}\right). \tag{5}$$

Індекси ДПФ, за яких спектр сигналу спадає до рівня шуму (див. рис. 1), визначимо як ms_{min} та ms_{max}. Тоді ширину спектра сигналу можна розрахувати як

$$\Delta f = \left(ms_{\max} - ms_{\min}\right) \times f_{\partial}, \tag{6}$$

де Δf – ширина спектра сигналу;

f_{∂} – крок частотної сітки перетворення, який залежить від технічних характеристик АЦП і параметрів m та N у виразі (1).

Використовуючи отримані результати, необхідно знайти тривалість символу T_s, який розраховують числовим методом в апаратній реалізації приладу, що важливо для налагодження автоматичного підстроювання частоти, і визначають у разі розв'язання рівняння розподілення потужності для сигналів із фазовою маніпуляцією [16]:

$$P(f) = \frac{E_s}{2} \times \left(\left(\frac{\sin(\pi \times (f - f_c) \times T_s)}{\pi \times (f - f_c) \times T_s} \right)^2 + \left(\frac{\cos(\pi \times (f - f_c) \times T_s)}{\pi \times (f - f_c) \times T_s} \right)^2 \right). \tag{7}$$

Для дискретних систем вираз (7) з урахуванням умовних позначень виразів (1)–(6) набуває такого вигляду:

$$Xam_{вим}(m_{вим} f_{\partial}) = \frac{Xam_{\max}}{2} \left[\left(\frac{\sin(\pi \times (m_{вим} f_{\partial} - m_s f_{\partial}) \times T_s)}{\pi \times (m_{вим} f_{\partial} - m_s f_{\partial}) \times T_s} \right)^2 + \left(\frac{\cos(\pi \times (-m_{вим} f_{\partial} - m_s f_{\partial}) \times T_s)}{\pi \times (-m_{вим} f_{\partial} - m_s f_{\partial}) \times T_s} \right)^2 \right], \tag{8}$$

де $Xam_{вим}(m_{вим} f_{\partial})$ – рівень амплітуди сигналу для індексу $m_{вим} f_{\partial}$ швидкого ДПФ у частотній області;

$T_s = T_{symb}$ – тривалість символа для BPSK маніпуляції;

$T_s = T_{symb} / 2$ – тривалість символа для QPSK маніпуляції;

$T_s = T_{symb} / 3$ – тривалість символа для 8PSK маніпуляції;

m_s – індекс швидкого ДПФ центра спектра сигналу. Його визначають відповідно до виразу

$$m_s = \frac{(ms_{max} - ms_{min})}{2} + ms_{min}. \tag{9}$$

Для розв'язання рівняння (8) необхідно, щоб виконувалась умова

$$\begin{cases} m_{вим} > ms_{\min}; \\ m_{вим} < ms_{\max}; \\ m_{вим} \neq m_s. \end{cases} \tag{10}$$

Отже, у разі виконання умови (10) у рівнянні (8) лишається невідомою лише величина T_s.

Розв'язок рівняння (8) відносно T_s дозволяє визначити символьну швидкість передачі даних. Математичну модель, описану виразами (1)–(10), реалізовано в МПФАС, який

дозволяє розв'язувати рівняння (8) числовим методом і є центральним елементом розробленої системи визначення виду фазової маніпуляції на петлі керуючих рішень. Розв'язок (8) є вихідними даними для розрахунку параметрів системи ФАПЧ, яка, у свою чергу, є ключовим елементом для визначення виду фазової маніпуляції.

Детально розглянемо принцип визначення виду фазової маніпуляції та математичну модель універсальної автоматизованої системи визначення виду фазової маніпуляції. Вихідні дані АЦП $S(kTs)$ перемножуються з гармонічними коливаннями в NCO. Після фільтрації у ФНЧ квадратурні складові сигналу $I(kT)$ та $Q(kT)$ потрапляють на ФД. Залежно від очікуваного виду маніпуляції ФД описують відповідним математичним виразом [16].

У разі BPSK ФД реалізується як

$$e(kT) = sign(I(kT)) \times Q(kT), \tag{11}$$

QPSK – як

$$e(kT) = sign(I(kT)) \times Q(kT) - sign(Q(kT)) \times I(kT). \tag{12}$$

Сигнал похибки $e(kT)$ є вхідним сигналом для СФ. Вихідний сигнал фільтра $el(kT)$ задає величину частоти цифрового гетеродина NCO та описується таким виразом:

$$el(kT) = K_p \times e(kT) + K_i \times e(kT-1) + el(kT-1), \tag{13}$$

де K_p – пропорційна константа;

K_i – інтеграційна константа.

Величини констант залежать від ширини спектра сигналу та від швидкості передачі даних. Якщо неправильно вибрані константи, то система ФАПЧ не буде здійснювати захоплення за несучу, відповідно, визначення виду маніпуляції не можливе. Згідно з [17], константи K_p та K_i визначають як

$$K_p = \frac{g_1}{K_0 \times K_d}; \tag{14}$$

$$K_i = \frac{g_2}{K_0 \times K_d}, \tag{15}$$

де K_0 – коефіцієнт передачі NCO;

K_d – коефіцієнт передачі ФД;

g_1 та g_2 – коефіцієнти стійкості системи зі зворотним зв'язком, які повинні відповідати такій умові [17]:

$$\begin{cases} g_2 \geq \dfrac{g_1^{\,2}}{4}; \\ g_2 < g_1. \end{cases} \tag{16}$$

Для дискретних систем ФАПЧ коефіцієнти g_1 та g_2 визначають за виразами [17]:

$$g_1 = 2 - \exp\left(-(\omega_p \times \xi \times T)\right) \times \cos\left(\omega_p \times T \times \sqrt{1-\xi^2}\right); \tag{17}$$

$$g_2 = \exp\left(-(2 \times \omega_p \times \xi \times T)\right) - 1 + g_1, \tag{18}$$

де $T = 1/F_d$ – період дискретизації;

F_d – частота дискретизації АЦП;

$\omega_p = 2 \times \pi \times f$ – резонансна частота контуру;

ξ – демпінг-фактор для стійкої роботи системи ФАПЧ слід вважати 0,5.

Правильно визначені коефіцієнти СФ надають можливість автоматизованій системі швидко та якісно здійснити захоплення вхідного сигналу, але виникає необхідність виявити ознаку захоплення системи ФАПЧ саме за корисний сигнал, яка є індикатором про визначення маніпуляції та надає команду модулю виявлення захоплення про початок роботи. Одним із факторів, який визначає здійснення захоплення за сигнал, є властивість квадратур мати однакову амплітуду в разі супроводу ФАПЧ за частотою та фазою. Тобто захоплення слід вважати здійсненим за умови

$$\sum_{k=0}^{L-1} \left([I(kT)] - [Q(kT)] \right) \le B, \tag{19}$$

де L – кількість відліків оцінки захоплення за сигнал;

B – поріг дисбалансу $I(kT)$ та $Q(kT)$ складових, за якого слід вважати, що захоплення здійснено.

Величина порога залежить від частоти дискретизації та виду маніпуляції.

Практичну реалізацію складових описаної вище системи доцільно реалізувати на базі програмованих логічних інтегральних схем, зокрема, використовуючи технологію вентильної матриці, яка програмується в умовах експлуатації. Апаратна основа в ході використання зазначеної технології наділяє прилад можливістю швидкої зміни алгоритмів обробки інформації з метою дослідження й оцінювання ефективності методів демодуляції та декодування прийнятої інформації.

Висновки. У результаті проведеної роботи проаналізовано можливість використання універсальної автоматизованої системи визначення виду фазової маніпуляції та символьної швидкості на основі схеми петлі рішень в наземних станціях прийому потоку даних від космічних систем. Встановлено, що запропонована схема може використовуватися для автоматичного визначення основних параметрів радіоліній космічних систем, що експлуатуються на низькій навколоземній орбіті. Зазначені результати підтверджено шляхом математичного моделювання для заданих значень відношення сигнал шум та ймовірності виникнення помилки. Застосування такої схеми дозволяє відразу після визначення виду фазової маніпуляції та символьної швидкості проводити демодуляцію й декодування бітового потоку цільової інформації, прийнятої з космічних систем на низькій навколоземній орбіті. Запропоновану в статті систему можливо використовувати для автоматичного визначення параметрів радіосигналів із фазовою маніпуляцією і в інших цифрових радіолініях.

СПИСОК ЛІТЕРАТУРИ

1. Современные зарубежные тактические устройства: портативные радиостанции. URL: https://trcvr.ru/2016/02/17/современные-зарубежные-тактические (дата обращения: 11.10.2020).
2. Айфичер Э. С. Цифровая обработка сигналов: практический поход. 2-е изд.; пер. с англ. Москва : Изд. дом «Вильямс», 2008. 992 с.
3. Лайонс Р. Цифровая обработка сигналов. 2-е изд.; пер с англ. Москва: ООО «БиномПресс», 2006. 656 с.
4. Kanaa A., Zuri Sha'ameri A. A robust parameter estimation of FHSS signals using time-frequency analysis in a non-cooperative environment // Physical Communication. 2018. № 26. P. 9–20.
5. Li T., Tang Y., Lv Y. Parameter estimation of FH signals based on STFT and music algorithm // Computer Application and System Modeling. 2010. P. 84–96.
6. Overdyk H. F. Detection and estimation of frequency hopping signals using wavelet transforms. Thesis for the degree of master of science in electrical engineering. Monterey, California. Naval Postgraduate School, 1997. 114 p.
7. Hosseini S. N., Razavi H. Joint detection and hop parameters estimation of slow FHSS/MFSK signals using DHWT-AC technique in Rayleigh block fading channels // Proceedings of the International MultiConference of Engineers and Computer Scientists. Hong Kong, 2009. P. 55–59.
8. Hamkins J., Marvin K. Simon. Autonomous Software-Defined Radio Receivers for Deep Space Applications. Jet Propulsion Laboratory California Institute of Technology, 2006. 431 p.
9. Prakasam P., Madheswaran M. Automatic modulation identification of QPSK and GMSK using wavelet transform for adaptive demodulator in SDR // Proceedings of the International Conference on Signal Processing Communications and Networking (ICSCN '07). Chennai, India, 2007. 507 p.
10. Azzouz E., Nandi A. K. Automatic Modulation Recognition of Communication Signals. Kluwer Academic Publishers. Boston : Mass, 1996. 447 p.
11. Фриз С. П., Кальватинський О. В. Математична модель автоматизованої системи визначення виду модуляції та символьної швидкості передачі даних для приймальних систем дистанційного зондування Землі // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ ДУТ, 2015. Вип. 11. С. 87–96.
12. Lopatka J., Pedzisa M. Automatic modulation classification using statistical moments and a fuzzy classifier // Proceedings of the 5th International Conference on Signal Processing (WCCC-ICSP'00). Beijing, China, 2000. Vol. 3. 1500 p.
13. TM Space Data Link Protocol. Recommendation for Space Data System Standards, CCSDS 130.1-G-2. Green Book. Washington, D.C. : CCSDS, November, 2012. 237 p.
14. Direct Access System User's Guide for the EOS–AM Spacecraft (ICD–107) / NASA Goddard Space Flight Center. Prepared by: Lockheed Martin Corporation, Lockheed Martin Missiles & Space, 1998. 55 p.
15. Каменев В. Е., Черкасов В. В., Чечин Г. В. Спутниковые сети связи : учеб. пособ. Москва : Альпина Паблишер, 2004. 536 с.
16. Радиоэлектронные системы. Основы построения и теория : справочник / Под ред. Я. Д. Ширмана. Изд 2-е, перераб. и доп. Москва : Радиотехника, 2007. 512 с.

17. Mohamed Khalid Nezami. RF Architectures and Digital Signal Processing Aspects of Digital Wireless Transceivers. Milcom, 2003. 513 p.
18. Floyd M. Gardner. Phaselock Techniques. 3rd Edition. Consulting Engineer. Palo Alto. California : A JOHN WILEY & SONS, INC., 2005. 450 p.

Подано 25.10.2020

REFERENCES

1. Sovremennye zarubezhnye takticheskie ustroistva: portativnye radiostantsii [Modern foreign tactical devices: portable radios]. (n.d.). Retrieved from https://trcvr.ru/2016/02/17/sovremennye-zarubezhnye-takticheskie [in Russian].
2. Aificher, E. S. (2008). *Tsifrovaia obrabotka signalov: prakticheskii pokhod [Digital Signal Processing: A Practical Approach].* 2nd ed.; trans. from English. Moscow [in Russian].
3. Laions, R. (2006). *Tsifrovaia obrabotka signalov [Digital signal processing].* 2nd ed.; trans. from English. Moscow [in Russian].
4. Kanaa, A., & Zuri Sha'ameri, A. (2018). A robust parameter estimation of FHSS signals using time-frequency analysis in a non-cooperative environment. *Physical Communication, 26*, 9–20.
5. Li, T., Tang, Y., & Lv, Y. (2010). Parameter estimation of FH signals based on STFT and music algorithm. *Computer Application and System Modeling*, 84–96.
6. Overdyk, H. F. (1997). *Detection and estimation of frequency hopping signals using wavelet transforms.* Thesis for the degree of master of science in electrical engineering. Monterey, California. Naval Postgraduate School.
7. Hosseini, S. N., & Razavi, H. (2009). Joint detection and hop parameters estimation of slow FHSS/MFSK signals using DHWT-AC technique in Rayleigh block fading channels. // In *Proceedings of the International MultiConference of Engineers and Computer Scientists.* (pp. 55–59). Hong Kong.
8. Hamkins, J., & Marvin, K. Simon. (2006). *Autonomous Software-Defined Radio Receivers for Deep Space Applications.* Jet Propulsion Laboratory California Institute of Technology.
9. Prakasam, P., & Madheswaran, M. (2007). Automatic modulation identification of QPSK and GMSK using wavelet transform for adaptive demodulator in SDR. *Proceedings of the International Conference on Signal Processing Communications and Networking (ICSCN '07).* Chennai, India.
10. Azzouz, E., Nandi, A. K. (1996). *Automatic Modulation Recognition of Communication Signals.* Kluwer Academic Publishers. Boston : Mass.
11. Fryz, S. P., Kalvatynskyi, O. V. (2015). Matematychna model avtomatyzovanoi systemy vyznachennia vydu moduliatsii ta symvolnoi shvydkosti peredachi danykh dlia pryimalnykh system dystantsiinoho zonduvannia Zemli [The mathematical model automated system to determine the modulation types and symbol rate, for consider receiving data of remote sensing]. *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], 11,* 87–96. Zhytomyr: ZhMI DUT [in Ukrainian].
12. Lopatka, J., & Pedzisa, M. (2000). Automatic modulation classification using statistical moments and a fuzzy classifier. In *Proceedings of the 5th International Conference on Signal Processing (WCCC-ICSP'00), Vol. 3,* (p. 1500). Beijing, China.

13. *TM Space Data Link Protocol. Recommendation for Space Data System Standards, CCSDS 130.1-G-2.* (November 2012). Green Book. Washington, D.C.: CCSDS.
14. *Direct Access System User's Guide for the EOS–AM Spacecraft (ICD–107)*. (1998). NASA Goddard Space Flight Center. Prepared.
15. Kamenev, V. E., Cherkasov, V. V., & Chechin, G. V. (2004). *Sputnikovye seti sviazi [Satellite communication networks]*. Moscow [in Russian].
16. Shirman, Ia. D. (Ed.). (2007). *Radioelektronnye sistemy. Osnovy postroeniia i teoriia [Electronic systems. Basics of construction and theory]*. 2nd ed. Moscow [in Russian].
17. Mohamed Khalid Nezami.(2003). *RF Architectures and Digital Signal Processing Aspects of Digital Wireless Transceivers.* Milcom.
18. Floyd, M. Gardner. (2005). *Phaselock Techniques.* 3rd ed. Consulting Engineer. Palo Alto. California : A JOHN WILEY & SONS, INC.

S. P. Fryz, O. V. Kalvatynskyi, R. O. Avsiievych

THE MODEL OF SYSTEM FOR DETERMINING THE TYPE OF PHASE MANIPULATION AND SYMBOL RATE IN THE RADIO LINES OF SPACE SYSTEMS

The article proposes a model of a universal automated system for determining the type of phase manipulation and symbol rate for receiving the flow of data by ground-based means transmitted in the radio lines of low-orbit space systems under a partial prior uncertainty.

The relevance of the study on the selected topic is that in the last decade there has been noted a significant increase in the number of space systems operating in low-Earth orbits. The afore-mentioned fact leads to an increase in the variety of radio line structures of space systems, which creates a partial prior uncertainty in relation to the parameters of radio signals transmitted by these systems. At the same time, the operation of space systems in low-Earth orbits imposes restrictions on the duration of the communication session, which makes it difficult to set up the ground-based demodulating equipment under conditions of a partial prior uncertainty of the radio signal parameters.

Considering the above, the article presents a possible option for designing a structure chart of a universal automated system for determining the type of phase manipulation and symbol rate. The principle of system operation is described and its operability is substantiated by mathematical modelling processes.

The considered model of the universal automated system for determining the type of phase manipulation and symbol rate enables to determine the nominal value of the central carrier frequency of the radio signal, radio spectrum width, symbol rate and one of three types of phase manipulation (BPSK, QPSK, 8PSK) in the time operation mode close to real one.

By the results of calculations being made, it is established that the system under study can be used while receiving data from space systems operating in low-Earth orbits. Also, the proposed system can be applied to determine the basic parameters of radio signals and other systems that use radio lines with phase manipulation.

Further research on the selected topic will be aimed at studying the possibility of expanding the number of types of manipulations that can be automatically determined by the proposed system.

Keywords: *radio line; radio signal; phase manipulation; symbol rate; space systems; low-Earth orbit; automation.*

УДК 004:047:004.912 DOI: 10.46972/2076-1546.2020.18.02

Д. Л. Федорчук, С. М. Марченков, О. М. Наумчак

ОЦІНЮВАННЯ ДИНАМІКИ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ ЗА ДАНИМИ ЕЛЕКТРОННИХ ЗАСОБІВ МАСОВОЇ КОМУНІКАЦІЇ

У статті розглянуто основні напрямки деструктивного інформаційно-психологічного впливу противника на населення України, керівників та особовий склад органів військового управління Збройних Сил України та інших силових структур. Досліджено питання аналізу поширення в мережі Інтернет інформаційних повідомлень (контенту) електронних засобів масової комунікації, що містять деструктивний інформаційно-психологічний вплив. Запропоновано модель соціальних мереж як засобу масової комунікації, що використовується для здійснення деструктивного інформаційно-психологічного впливу. Її основними складовими є користувач, його думки (погляди), вплив, довіра та репутація. Розглянуто процес впливу на користувача засобами соціальних мереж шляхом нововведення та його розповсюдження. Також надано показники, за допомогою яких можна охарактеризувати досліджуваний процес та оцінити вплив: "лайки", "дизлайки", "репости", "перегляди" та "коментарі". Описано процес відслідковування негативних впливів, що містяться в інформаційних повідомленнях, з точки зору деструктивного інформаційно-психологічного впливу. Проаналізовано систему показників динаміки поширення інформаційних повідомлень у мережі Інтернет. Обґрунтовано необхідність фіксації показників на визначені моменти часу. На основі аналізу основних показників рядів динаміки доведено доцільність використання додаткових показників: "кількість втягнень", "абсолютний приріст", "темп зростання", "темп приросту" – та наведено порядок їх розрахунку. Розроблено логічно-структурну схему розрахунку показників динаміки поширення інформаційних повідомлень засобами мережі Інтернет. Визначено, що для вирішення завдання автоматизації відслідковування та візуалізації динаміки поширення інформаційних повідомлень необхідне спеціалізоване програмне забезпечення, яке передбачатиме зчитування первинних показників із визначених публікацій електронних засобів масової комунікації та соціальних мереж, а також розраховуватиме запропоновані показники динаміки поширення інформаційних повідомлень у визначені моменти часу.

Ключові слова: *електронні засоби масової комунікації; інформаційні повідомлення; деструктивний інформаційно-психологічний вплив; система показників; динаміка поширення.*

Постановка проблеми в загальному вигляді. В умовах збройної агресії Російської Федерації (РФ) проти України питання, пов'язані із забезпеченням інформаційної безпеки (ІБ) держави у воєнній сфері, суттєво актуалізувалися. Основами (засадами) державної інформаційної політики з питань забезпечення ІБ визначено систему заходів, які у воєнній сфері спрямовані на [1–3]:

запобігання інформаційним загрозам (викликам, ризикам) шляхом запровадження превентивних заходів із забезпечення ІБ для попередження можливості їх виникнення ще на ранніх стадіях зародження;

виявлення ознак інформаційних загроз та деструктивних впливів, яке полягає в систематичному моніторингу, аналізі й контролі можливості появи реальних або потенційних інформаційних загроз;

впровадження своєчасних заходів з нейтралізації інформаційних загроз (викликів), прогнозування ризиків ІБ держави в інформаційній сфері;

вживання заходів з ліквідації (локалізації) загроз (викликів);

ліквідацію наслідків негативних інформаційно-психологічних впливів (ІПсВ).

Досвід протистояння агресії РФ проти України показує, що дані в мережі Інтернет (особливо з російських соціальних мереж (СМ)) напередодні та під час проведення антитерористичної операції широко використовувалися противником для здійснення деструктивного ІПсВ на населення України, керівників та особовий склад органів військового управління (ОВУ), особовий склад Збройних Сил (ЗС) та інших силових структур [4]. Основною метою зазначених ІПсВ була, є та буде в найближчому майбутньому дискредитація вищого військово-політичного керівництва держави; поширення серед місцевого населення паніки, страху й хаосу, зневіри в можливості своїх органів управління та силових структур. Аналіз наявних фактів підтверджує високу ефективність інформаційної зброї.

Аналіз останніх досліджень і публікацій. Застосування методів і способів ведення гібридних війн перетворило інформаційний простір на ключову арену протиборства держав для досягнення національних, економічних, політичних, військових цілей тощо [4]. Значуща роль відводиться поширенню негативного ІПсВ у текстових повідомленнях, які розміщуються в електронних засобах масової інформації (е-ЗМІ) та СМ [5]. На даний час відомо багато робіт, присвячених питанням розповсюдження інформації в мережах, розробленню моделей динамічних процесів у мережевих структурах та інформаційному управлінню, моніторингу [7]. Однією із складових моніторингу є аналіз поширення інформаційних повідомлень (контенту) (ІП), що містять деструктивний вплив, за даними Інтернету [5]. Дезінформація та маніпуляції вміло застосовуються в е-ЗМІ та розповсюджуються за допомогою СМ та інших комунікаційних каналів. Виявлення та оцінювання загроз від деструктивних психологічних впливів, що здійснюються противником з використанням можливостей глобальної мережі, залишається надзвичайно актуальним завданням [6]. Однією з його складових є аналіз поширення ІП (контенту), що містять деструктивний вплив, за інтернет-даними для оцінювання створюваного ними рівня загроз (ефективності з позиції противника). Крім того, виникає й інше актуальне завдання щодо супроводження контенту, який створюється та розповсюджується в мережі Інтернет у рамках організації інформаційної протидії, та оцінювання його ефективності [6].

Формулювання завдання дослідження. Виявлення та оцінювання рівня загроз від деструктивних ІПсВ, що здійснюються противником із використанням можливостей е-ЗМІ, залишається надзвичайно актуальним завданням. Крім відслідковування контенту, що містить деструктивний ІПсВ, для оцінювання створюваного ним рівня загрози, виникає й інше актуальне завдання щодо супроводження проукраїнського контенту (для оцінювання його ефективності).

Слід зазначити, що в даний час інформаційні потоки, які циркулюють в мережі Інтернет, настільки зросли, що окремі їх джерела фактично перетворилися та злилися в суцільне русло. А тому виконання зазначених вище завдань у “ручному режимі”, як це робиться нині,

є нераціональним. Отже, на сьогодні важливим завданням є автоматизація відслідковування та візуалізація динаміки поширення ІП за даними мережі Інтернет [8].

Виклад основного матеріалу. Ключовими елементами практично будь-якої моделі СМ є: користувач, погляд (думка), вплив / довіра, репутація. Оскільки управління є впливом на керовану систему (об'єкт управління) з метою забезпечення її потрібної поведінки, то предметом управління в СМ є погляди користувачів, їх репутація та довіра один до одного [9].

Нововведення (інформація) потрапляють у СМ через новаторів – користувачів змін, а потім поступово приймаються багатьма користувачами, які передають інформацію про нововведення один одному. Міжособистісні контакти користувачів та комунікаційні джерела (зокрема е-ЗМІ та СМ) розповсюджують інформацію про нововведення та впливають на лаштунки, диспозиції, уяву та в кінцевому підсумку на рішення користувачів щодо прийняття нововведення. Зрештою від прийняття інновацій для користувачів та соціальної системи виникають позитивні чи негативні наслідки (бажані чи небажані, прямі чи опосередковані, передбачувані чи непередбачувані) [9].

Отже, для того, щоб змінити поведінку користувачів (об'єктів управління або впливу) за допомогою комунікаційних каналів (до яких також належать е-ЗМІ та СМ), у соціальну систему вводиться нововведення – і розпочинається процес його прийняття користувачем. Одними з показників, що характеризують цей процес, є кількість "лайків", "дизлайків", "репостів", "переглядів" та "коментарів", відслідковуючи кількість яких та динаміку їх зміни можливо аналізувати стадії сприймання нововведення [9].

З погляду деструктивного ІПсВ процес відслідковування та візуалізації можна описати так:

противник визначається із нововведенням (ідея, погляд, думка, суспільна думка, вибір (зокрема шляхом голосування) тощо), яке повинно сприйняти населення України (окремого регіону), військово-політичне керівництво нашої держави (окремого регіону), особовий склад силових структур та правоохоронних органів для відповідної зміни поведінки в інтересах противника;

дане нововведення "зашивається" у відповідні ІП (статті, повідомлення, відеоролики, різноманітні графічні матеріали тощо), тобто розробляється відповідна продукція ІПсВ;

з використанням комунікаційних каналів (зокрема е-ЗМІ та СМ) даний контент поширюється в мережі Інтернет;

шляхом аналізу реакції користувачів на даний контент відбувається його коригування та дозування для досягнення потрібного ефекту з урахуванням цілей противника [9].

Сукупність деструктивних ІПсВ, що містяться в ІП, поширення яких здійснюється та стимулюється противником для відповідної зміни поведінки об'єктів впливу шляхом прийняття "зашитого" в них нововведення, становлять відповідні інформаційні загрози.

Отже, відслідковування та візуалізація динаміки поширення ІП (нововведень) за даними мережі Інтернет повинно забезпечувати процес фіксації зазначених показників на визначені моменти часу для їх подальшого аналізу [10]. Процес прийняття користувачем нововведення може характеризуватися такими показниками: кількість "лайків", "дизлайків", "репостів", "переглядів" та "коментарів".

Введемо позначення:

L – кількість "лайків";

D – кількість “дизлайків”;

R – кількість “репостів”;

V – кількість “переглядів”;

C – кількість “коментарів”.

Обчислення цих показників здійснюється за допомогою функціоналу відповідних СМ, вони є первинними для проведення подальшого аналізу. Одним із завдань автоматизації є забезпечення зчитування показників за відповідними URL-посиланнями на повідомлення (контент).

У результаті аналізу публікацій, що стосуються вибору та аналізу показників динаміки поширення ІП в мережі Інтернет, зроблено висновок про доцільність використання додаткового показника, а саме кількості “втягнень”. Під кількістю “втягнень” In будемо розуміти кількість користувачів, що здійснили будь-яку дію з публікацією (поставили “лайк” або “дизлайк”, прокоментували чи зробили “репост”). У такий спосіб кількість “втягнень” у найпростішому випадку може бути обчислена як

$$In = L + D + R + C. \tag{1}$$

Усі визначені вище показники змінюються з часом. Враховуючи те, що вивчення динаміки показників, які змінюються в часі, є одним з головних завдань математичної статистики, а також те, що дане завдання вирішується за допомогою аналізу рядів динаміки (часових рядів), проведено аналіз основних показників рядів динаміки [8, 9] з метою визначення серед них доцільних для аналізу динаміки поширення ІП за даними мережі Інтернет.

За результатами проведеного аналізу зроблено висновок про доцільність використання таких показників, як: абсолютний приріст Δy , темп зростання T_r та темп приросту T_{pr} [10].

Абсолютний приріст Δy характеризує збільшення (зменшення) рівня ряду за визначений проміжок часу, він визначається за виразом [8, 9]

$$\Delta y = y_i - y_{i-1}, \tag{2}$$

де y_i – поточний рівень ряду;

y_{i-1} – рівень ряду, що передує поточному.

Абсолютний приріст може бути додатним та від’ємним. Він вимірює абсолютну швидкість зростання чи зниження рівня.

Темп зростання T_r – це показник інтенсивності зміни рівня ряду, виражений у відсотках. Він визначається як [11]:

$$T_r = \frac{y_i}{y_{i-1}} \times 100\%. \tag{3}$$

Темп приросту T_{pr} показує відносне значення приросту та на скільки відсотків порівнюваний рівень більший чи менший рівня, прийнятого за базу порівняння. Він може

бути як додатним, так і від'ємним чи рівним нулю, виражається у відсотках та визначається за таким виразом [8, 9]:

$$T_{pr} = \frac{y_i}{y_{i-1}} \times 100\% - 100\% = T_r - 100\%. \quad (4)$$

Показники абсолютного приросту, темпу зростання та темпу приросту розраховуються для кожного із наведених вище первинних показників (L, D, R, V, C), а також для показника кількості "втягнень" In. На рис. 1 зображено розроблену структурно-логічну схему розрахунку показників динаміки поширення ІП за даними мережі Інтернет.

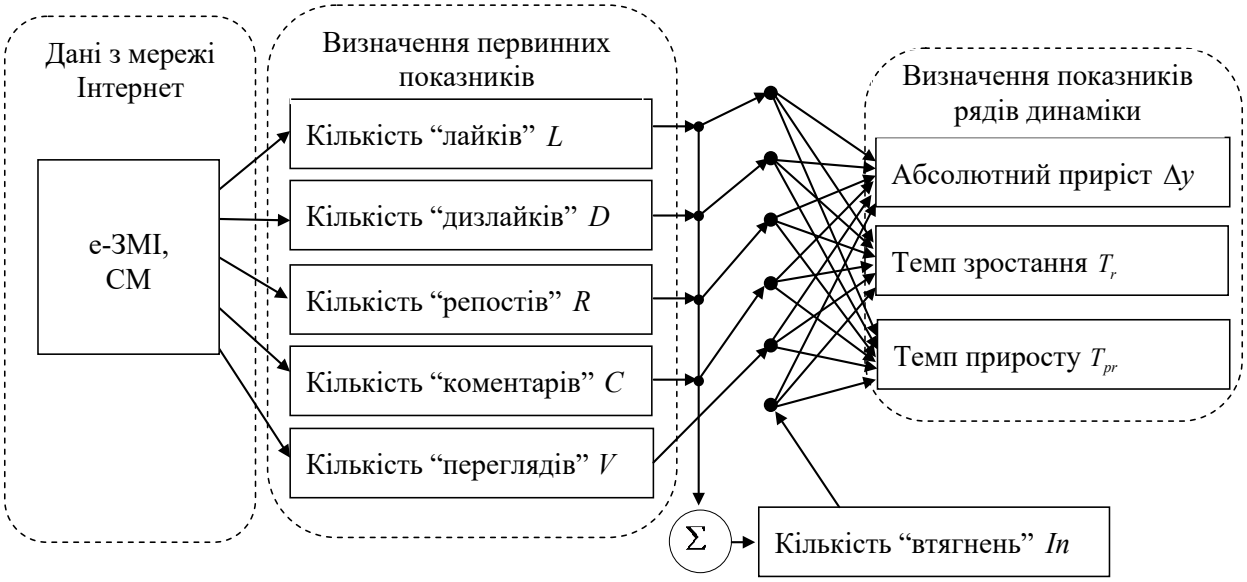


Рис. 1. Структурно-логічна схема розрахунку показників динаміки поширення ІП за даними мережі Інтернет

Вирішити завдання автоматизації відслідковування та візуалізації динаміки поширення ІП можна за рахунок розроблення спеціалізованого програмного забезпечення, яке реалізовуватиме зчитування первинних показників із визначених публікацій е-ЗМІ та СМ, а також розрахунок значень запропонованих показників динаміки поширення ІП (див. рис. 1) на відповідні моменти часу.

Висновки. Отже, питання відслідковування динаміки поширення ІП, за допомогою яких здійснюється деструктивний ІПсВ на особовий склад ЗС України та посадових осіб ОВУ, залишається актуальним для оцінювання рівня загроз ІБ у воєнній сфері. Крім того, зазначене питання актуальне для оцінювання ефективності контенту, що створюється та розповсюджується з використанням відкритих інформаційних джерел мережі Інтернет з метою інформаційної протидії.

Автоматизація зазначеного дозволить підвищити ефективність щодо: супроводження визначених ІП, розміщених на відкритих ресурсах мережі Інтернет; аналізу показників динаміки їх поширення, поєднаних у систему. Зазначена система складається з первинних показників та показників рядів динаміки.

Інформація щодо узятих на супроводження ІП та значень показників динаміки їх поширення повинна зберігатися у базі даних, що дозволить проводити ретроспективний аналіз відповідних повідомлень та показників динаміки їх поширення з метою:

виявлення взаємозв'язків між різними повідомленнями, що належать до різних напрямів реалізації інформаційних загроз;

проведення аналізу підготовчих заходів противника під час здійснення деструктивного ІПсВ на цільові об'єкти (цільову аудиторію) та проведення інформаційних операцій (зазначений аналіз дозволить удосконалити механізми своєчасного виявлення підготовчих заходів противника із застосуванням е-ЗМІ у ході гібридної війни проти України);

проведення аналізу ефективності та своєчасності поширення контенту, що протидіє ворожому.

Перспективним напрямом подальших досліджень є: підвищення рівня автоматизації аналізу контенту, зокрема текстової інформації шляхом розроблення та впровадження методів автоматичного семантичного аналізу текстів і визначення їх змісту; розроблення та впровадження надійних методів і алгоритмів автоматичного реферування текстових документів; використання автоматичного перекладу з іноземної мови для моніторингу іншомовних ресурсів у мережі Інтернет.

СПИСОК ЛІТЕРАТУРИ

1. Про національну безпеку України : Закон України від 15.12.2005 № 31, ст. 241 // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 10.11.2020).

2. Доктрина інформаційної безпеки України, затв. Указом Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017/ (дата звернення: 20.06.2019).

3. Про стан виконання рішень Ради національної безпеки і оборони України та додаткові заходи щодо забезпечення обороноздатності держави : рішення Ради національної безпеки і оборони України від 06.05.2015, затв. Указом Президента України від 26.05.2015 № 285/2015. URL: https://zakon.rada.gov.ua/laws/show/n0007525-15 (дата звернення: 20.06.2019).

4. Гіда О. Ф. Соціальні мережі як засіб деструктивних впливів через інформаційний простір // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 3 (31). С. 268–272.

5. Кондратьев М. А., Ивановский Р. И., Цыбалова Л. М. Применение агентного подхода к имитационному моделированию процесса распространения заболевания // Научно-технические ведомости СПб ГПУ. 2010. № 2. С. 189–194.

6. Грищук Р. В., Канкін І. О., Охрімчук В. В. Технологічні аспекти інформаційного протиборства на сучасному етапі // Захист інформації. 2015. Т. 17, № 1. С. 80–86.

7. Додонов А. Г., Ланде Д. В., Прищепа В. В., Путятин В. Г. Конкурентна розвідка в комп'ютерних мережах. Київ : ІПРІ НАН України, 2013. С. 20–45.

8. Ланде Д. В., Кондратенко Я. А. Особливості побудови систем розподіленого контент-моніторингу глобальних інформаційних мереж // Information Technology and Security. 2017. Vol. 5, Iss. 1 (8). P. 5–11.

9. Губанов Д. А., Новиков Д. А., Чхарташвили А. Г. Социальные сети: модели информационного влияния, противоборства и управления : монографія. Москва : Изд-во физматлитературы, 2010. 228 с.
10. Рудий С. 5 метрик Facebook, які дійсно корисні. URL: http://www.cossa.ru/155/36815 (дата звернення: 20.06.2019).
11. Теорія ймовірностей та математична статистика : навч. посіб. / О. І. Кушлик-Дивульська, Н. В. Поліщук, Б. П. Орел, П. І. Штабалюк. Київ : НТУУ «КПІ», 2014. 212 с.

Подано 10.11.2020

REFERENCES

1. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 15.12.2005 № 31, st. 241 [On National Security of Ukraine: Law of Ukraine from 15.12.2005 № 31, article 241]. *Vidomosti Verkhovnoi Rady Ukrainy [Information of the Verkhovna Rada of Ukraine]*. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].
2. Doktryna informatsiinoi bezpeky Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 25.02.2017 № 47/2017 [Doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine from 25.02.2017 № 47/2017]. Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017/ [in Ukrainian].
3. Pro stan vykonannia rishen Rady natsionalnoi bezpeky i oborony Ukrainy ta dodatkovi zakhody shchodo zabezpechennia oboronozdatnosti derzhavy : rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 06.05.2015, zatv. Ukazom Prezydenta Ukrainy vid 26.05.2015 № 285/2015 [On the status of implementation of decisions of the National Security and Defense Council of Ukraine and additional measures to ensure the defense capabilities of the state: the decision of the National Security and Defense Council of Ukraine from 06.05.2015, approved by the Decree of the President of Ukraine from 26.05.2015 № 285/2015.]. Retrieved from https://zakon.rada.gov.ua/laws/show/n0007525-15 [in Ukrainian].
4. Hida, O. F. (2013). Sotsialni merezhi yak zasib destruktyvnykh vplyviv cherez informatsiinyi prostir [Social networks as a means of destructive influences through the information space]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka) [Fight against organized crime and corruption (theory and practice)], 3* (31), 268–272 [in Ukrainian].
5. Kondrat'ev, M. A., Ivanovskii, R. I., & Tsybalova, L. M. (2010). Primenenie agentnogo podkhoda k imitatsionnomu modelirovaniiu protsessa rasprostraneniia zabolevaniia [Application of the agent-based approach to the simulation of the disease spreading process]. *Nauchno-tekhnicheskie vedomosti SPb GPU [Scientific and technical bulletin of the St. Petersburg State Pedagogical University], 2,* 189–194. Saint Petersburg [in Russian].
6. Hryshchuk, R. V., Kankin, I. O., & Okhrimchuk, V. V. (2015). Tekhnolohichni aspekty informatsiinoho protyborstva na suchasnomu etapi [Technological aspects of information confrontation at the present stage]. *Zakhyst informatsii [Information protection], Vol. 17,* № 1, 80–86 [in Ukrainian].
7. Dodonov, A. H., Lande, D. V., Pryshchepa, V. V., & Putiatyn ,V. H. (2013). *Konkurentna rozvidka v komp'iuternykh merezhakh [Competitive intelligence in computer networks]*. Kyiv: NAS of Ukraine [in Ukrainian].

8. Lande, D. V., & Kondratenko, Ya. A. (2017). Osoblyvosti pobudovy system rozpodilenoho kontent-monitorynhu hlobalnykh informatsiinykh merezh [Features of construction of distributed content monitoring systems of global information networks]. *Information Technology and Security, Vol. 5,* Iss. 1 (8), 5–11 [in Ukrainian].
9. Gubanov, D. A., Novikov, D. A., & Chkhartashvili, A. G. (2010). *Sotsial'nye seti: modeli informatsionnogo vliianiia, protivoborstva i upravleniia [Social networks: models of information influence, confrontation and control]*. Moscow [in Russian].
10. Rudyi, S. (n.d.). *5 metryk Facebook, yaki diisno korysni [5 Facebook metrics that are really useful]*. Retrieved from http://www.cossa.ru/155/36815 [in Ukrainian].
11. Kushlyk-Dyvulska, O. I., Polishchuk, N. V.,. Orel, B. P, & Shtabaliuk, P. I. (2014). *Teoriia ymovirnostei ta matematychna statystyka [Probability theory and mathematical statistics]*. Kyiv: NTU of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" [in Ukrainian].

Подано 12.11.2020

D. L. Fedorchuk, S. M. Marchenkov, O. M. Naumchak

ASSESSING THE DYNAMICS OF DISSEMINATION OF INFORMATION MESSAGES ACCORDING TO THE DATA OF ELECTRONIC MASS MEDIA

The main directions of destructive information and psychological influence of the enemy on the population of Ukraine, leaders and personnel of the military administration, the Armed Forces of Ukraine and other law enforcement agencies, issues of the analysis of the dissemination of information messages (content) of the electronic media which contain the destructive information and psychological impact are considered. The model of social networks as a means of mass communication, which is used for the realization of destructive information and psychological influence is considered. The main components of the model are the user, his thoughts (views), influence, trust and reputation. The process of influencing to the user by means of social networks through innovation and its dissemination is considered. Indicators that can be used to characterize the process and to evaluate the impact: "likes", "dislikes", "reposts", "views", and "comments" are also provided. The process of tracking the destructive influences contained in information messages from the point of view of destructive informational and psychological influence is described. The system of indicators of dynamics of distribution of information messages on the Internet is analyzed. The necessity of fixing on certain points of time and use of additional indicators: "number of drawings", "absolute growth", "growth rate", "growth rate" is grounded and the order of their calculation is given. The logical and structural scheme of calculating the dynamics of information message dissemination by means of the Internet has been developed. It is determined that to solve the problem of automation of tracking and visualization of the dynamics of information dissemination requires specialized software that will read the primary indicators from certain publications of electronic communications and social networks and calculate the proposed indicators of the dynamics of information message propagation.

Keywords: *electronic media of mass communication, informational messages, destructive informational and psychological influence, system of indicators, dynamics of dissemination.*

УДК 621.396 DOI: 10.46972/2076-1546.2020.18.03

О. М. Кубрак, В. О. Чолпанов, І. М. Дюков

ОЦІНКА ЙМОВІРНОСТЕЙ БІТОВОЇ ПОМИЛКИ СИСТЕМ ЗВ'ЯЗКУ З ФАЗОВОЮ МОДУЛЯЦІЄЮ ШИРОКОСМУГОВИХ СИГНАЛІВ

На сьогоднішній день бездротовий зв'язок є однією з найперспективніших сфер у галузі комунікацій. Сучасні системи і засоби радіозв'язку функціонують у складній радіоелектронній обстановці. Розвиток бездротових мереж наступного покоління залежить як від передавального, так і від приймального обладнання, яке має забезпечувати високу швидкість передачі даних, необхідну для підтримки надійного рівня перешкодозахищеності. Основними факторами, що впливають на якість радіозв'язку, є: природні й навмисні завади, що діють у каналі поширення радіохвиль; багатопроменеве поширення; обмеження пропускної здатності та необхідність асинхронного доступу. Один із можливих методів часткового вирішення зазначених вище проблем – використання систем зв'язку з розширеним спектром.

У статті досліджено ефективність різних типів фазової модуляції, які використовуються для систем прямого розширення спектра (Direct Sequence Spread Spectrum). За канал поширення радіохвиль обрано ідеалізований канал з адитивним білим гаусівським шумом (Additive White Gaussian noise). Було помічено, що системи радіозв'язку з прямим розширенням спектра із двійковою фазовою модуляцією (Binary phase shift keying) досягає кращих показників значень імовірності бітової помилки (Bit error rate) порівняно з іншими. Дослідження проводилися в середовищі динамічного міждисциплінарного моделювання складних технічних систем – Simulink (основному інструменті для модельно-орієнтованого проєктування), основним інтерфейсом якого є графічний інструмент для побудови діаграм і гнучкий набір бібліотек функціональних блоків.

Ключові слова: *системи зв'язку з розширеним спектром; фазова модуляція; імовірність бітової помилки; перешкодозахищеність; адитивний білий гаусівський шум (Additive White Gaussian noise); Direct Sequence Spread Spectrum.*

Постановка проблеми в загальному вигляді. Сигнали з розширеним спектром з роками стають усе більш популярними для використання в системах зв'язку завдяки своїй перешкодозахищеності. Найпоширенішого застосування набули три різновиди розширення спектра, описані в Рекомендації ITU-R SM.1055 [1] та в [2, 3], а саме: з прямою послідовністю; зі стрибкоподібною зміною частоти; з поєднанням зазначених вище методів з використанням розширювальної прямої послідовності та стрибкоподібної зміни частоти (Direct Spread/Frequency Hopping). Системи радіозв'язку (СРЗ) на основі широкосмугових сигналів (ШСС) для передачі інформації відрізняються тим, що їх ефективна ширина спектра набагато більша за швидкість передачі інформації в бітах за секунду, тому коефіцієнт розширення спектра для сигналу з розширеним спектром набагато більший за одиницю. Другою важливою особливістю, що враховується для проєктування систем зв'язку з використанням сигналів з розширеним спектром, є вплив у каналі розповсюдження різних типів радіоперешкод. Вказані умови розпосюдження

призводять до інформаційних втрат, що зумовлює необхідність оцінювання перешкодостійкості сигналів із розширеним спектром.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження і розвиток методів радіоподавлення СРЗ з ШСС зробили українські та закордонні вчені: Змієвський В. В., Ємельянов С. Л., Перунов Ю. М., Варакін Л. Є., Купріянов О. І., Сахаров А. В., Борисов В. І., Зінчук В. М., Лимарев А. Е., Torrieri D. J., Burel G., Poisel R. A., Wang H. тощо. У [4] Роберт А. Шольц розглядав розвиток систем зв'язку з розширеним спектром, які є стійкими до сигналів перешкод. Він зазначав, що перешкодостійкість прямого розширення спектра (Direct Sequence Spread Spectrum – DSSS) майже вдвічі перевищує за цією характеристикою розширення спектра з використанням стрибкоподібної зміни частот, однак більший розподіл смуги досягається завдяки технології стрибкоподібної зміни частоти [5]. Якість обслуговування, що надається системою бездротового зв'язку, може бути значно підвищена за допомогою правильного вибору схеми модуляції [6]. Поєднання розширеного спектра сигналу та фазової модуляції (ФМ) може забезпечити дуже надійний канал передачі даних [7], [8]. Wang H. у своїй роботі [8] стверджував, що DSSS-система з М-розширювальними кодами, отриманими шляхом зміщення однієї і тієї ж PN-послідовності, може збільшити ефективність передачі систем розширеного спектра, а також подолати обмеження швидкості передачі даних. Разом з тим потребує додаткового дослідження питання оцінювання завадостійкості систем зв’язку з розширеним спектром.

Формулювання завдання дослідження. Метою статті є проведення оцінювання ефективності перешкодозахищеності СРЗ із ШСС шляхом розроблення її програмної моделі з різними типами ФМ та визначення ймовірностей бітової помилки (Bit error rate – BER) в разі впливу в каналі розповсюдження адитивного білого гаусівського шуму (Additive White Gaussian noise – AWGN), а також аналіз отриманих результатів.

Виклад основного матеріалу. Як видно з рис. 1, на якому зображено варіант реалізації структурної схеми передавача з DSSS, у системі відбувається двоступенева модуляція. Сигнал даних $x(t)$ може бути як аналоговим, так і цифровим. У більшості випадків сигнал даних подається в цифровому вигляді, тому він безпосередньо перемножується з кодовим сигналом $g(t)$. З метою спрощення аналізу розглянемо бінарну ФМ (Binary phase shift keying – BPSK).

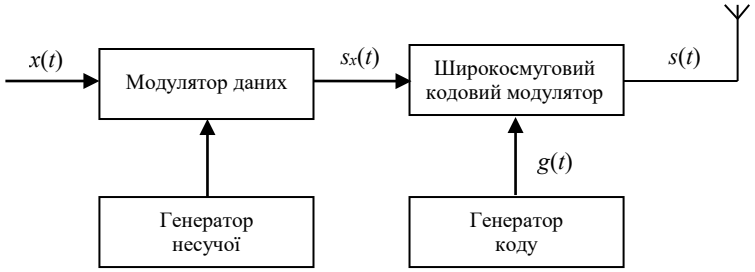


Рис. 1. Структурна схема передавача системи з розширенням спектра за методом DSSS

Як правило, потік інформаційних біт для методу BPSK подається у вигляді біполярної послідовності імпульсів з рівнями +1 і -1. Тоді сам процес модуляції реалізується шляхом простого перемноження даних і сигналу несучого коливання:

$$s_x(t) = \sqrt{2P}x(t)\cos(\omega_0 t). \quad (1)$$

У результаті такої операції відбувається миттєва зміна фази модульованого коливання на π радіан відносно несучого коливання відповідно до інформаційних даних.

Якщо розширювальна послідовність також подається у форматі «без нулів», то результуючий сигнал можна записати як

$$s(t) = \sqrt{2P}x(t)g(t)\cos(\omega_0 t). \quad (2)$$

У приймачі (рис. 2) формується синхронізований у часі псевдовипадковий сигнал $g(t)$, який забезпечує зворотну процедуру – стискання спектра і є точною копією сигналу псевдовипадкової послідовності на передавальному боці. Отриманий вузькосмуговий PSK сигнал демодулюється.

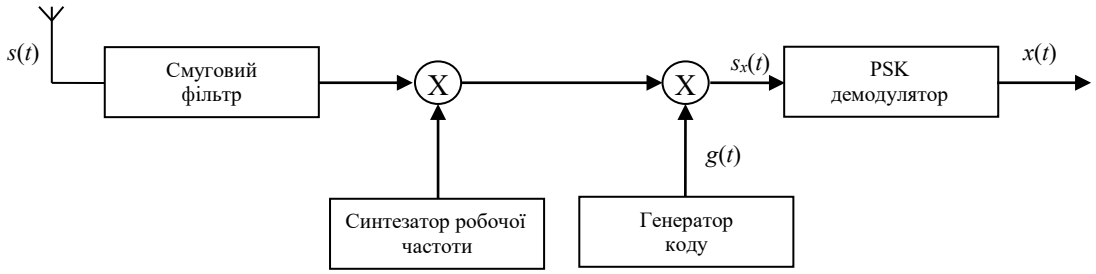


Рис. 2. Структурна схема приймача системи з прямим розширенням спектра

Тобто можна стверджувати, що демодуляція сигналу для DSSS-BPSK систем відбувається також за два етапи. Перший – це стискання спектра прийнятого сигналу, який виконується шляхом визначення кореляції прийнятого сигналу із синхронізованою копією розширювальної послідовності. Другий етап реалізується за допомогою звичайного демодулятора виду радіочастотної модуляції.

Перешкодостійкість ШСС визначають за широко відомим співвідношенням, що зв'язує відношення сигнал-шум на виході приймача q^2 з відношенням сигнал-шум на вході приймача ρ^2 [9]:

$$q^2 = 2B\rho^2, \quad (3)$$

де $\rho^2 = P_c/P_n$ (P_c, P_n – потужності ШСС і перешкоди);

$q^2 = 2E/N_n$, де E – енергія ШСС; N_n – спектральна щільність потужності перешкоди в смузі ШСС. Відповідно, $E = P_cT$, а $N_n = P_n/F$;

B – база ШСС.

Відношення сигнал-шум на виході q^2 визначає робочі характеристики прийому ШСС, а відношення сигнал-шум на вході ρ^2 – енергетику сигналу й перешкоди. Як видно зі співвідношення (3), прийом ШСС узгодженим фільтром або корелятором супроводжується посиленням сигналу (або зменшенням впливу перешкоди) у $2B$ рази. Саме тому величину

$$K_{ШСС} = q^2/\rho^2 \quad (4)$$

називають коефіцієнтом посилення ШСС у разі обробки або просто її посилення [9]. З (3), (4) випливає, що коефіцієнт посилення обробки $K_{ШСС} = 2B$.

Відомо, що вплив адитивної перешкоди в СРЗ із ШСС зводиться до збільшення спектральної щільності потужності шуму на виході змішувача приймача. Вираз для оцінювання $P_{пом}$ у разі впливу загороджувальної шумоподібної перешкоди (типу «білий шум») на приймач має такий вигляд [10]:

$$P_{пом} = \frac{1}{2} erfc \sqrt{\frac{K_c P_c}{\eta P_n}}, \tag{5}$$

де K_c – коефіцієнт розширення спектра сигналу $(K_c = W_c / F_c)$, W_c – ширина смуги частот ШСС, Гц; F_c – ширина смуги частот інформаційного символа, Гц;

P_c – потужність сигналу на вході приймача СРЗ із ШСС, Вт;

P_n – потужність перешкоди на вході приймача СРЗ із ШСС, Вт;

η – параметр перешкоди $(\eta = sin\, c^2[(f_n - f)\tau_{імп}])$;

$f_п$ – несуча частота сигналу перешкоди, Гц;

f_c – несуча частота ШСС, Гц;

$\tau_{імп}$ – тривалість імпульсу кодової послідовності, с;

$erfc(x)$ – додатковий інтеграл помилок $\left(erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt \right)$.

Отже, одним з основних призначень СРЗ із ШСС є забезпечення надійного прийому інформації в разі впливу потужних перешкод, коли відношення сигнал-шум на вході приймача ρ^2 може бути набагато менше одиниці. Необхідно ще раз відзначити, що наведені співвідношення справедливі для перешкоди у вигляді гаусівського випадкового процесу з рівномірною спектральною щільністю потужності (білий шум).

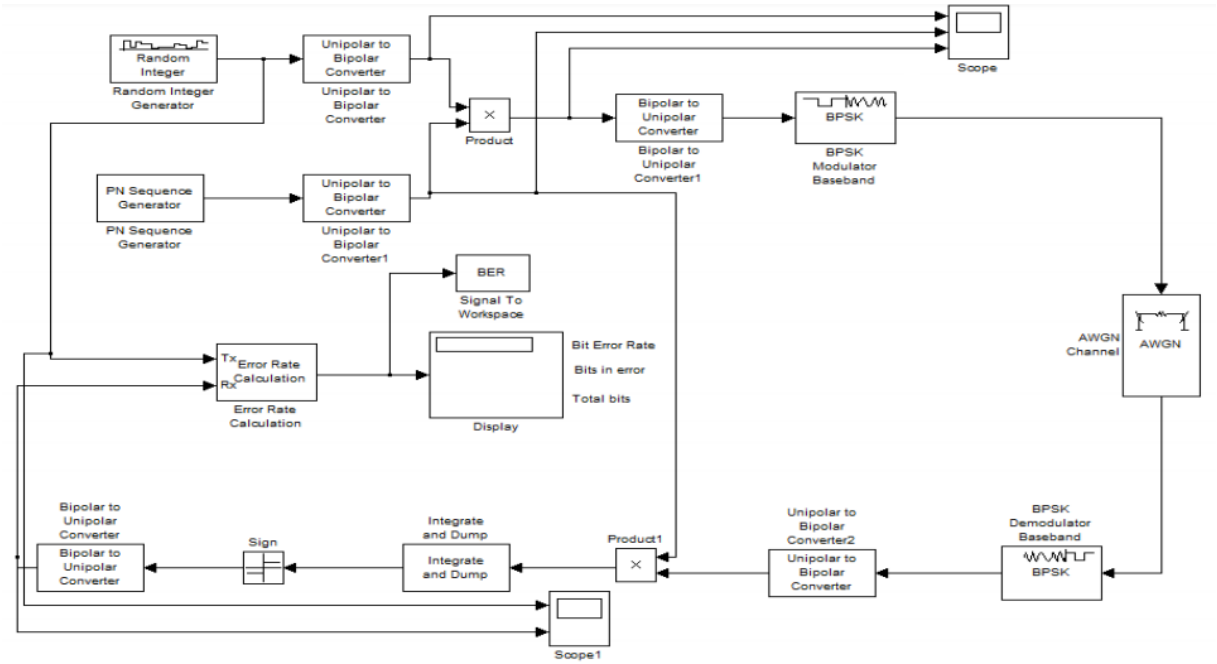


Рис. 3. Модель системи зв'язку з використанням DSSS у програмному середовищі MATLAB Simulink

Зображена на рис. 3 модель СРЗ із ШСС розроблена для системи з використанням сигналу з прямим розширенням спектра й каналом AWGN в програмному середовищі MATLAB Simulink (основному інструменті для модельно-орієнтованого проєктування) із використанням відповідних підсистемних блоків.

Джерело даних – це генератор випадкових цілих чисел (random Integer generator), який генерує випадкові рівномірно-розподілені двійкові цілі числа (0 і 1) з тривалістю біта 1 мс та швидкістю передачі даних 1 Кб/с (рис. 4). Блок генератора послідовності PN (PN-Sequence generator), який використовується з підбібліотеки генераторів послідовностей джерел зв'язку, генерує послідовність псевдовипадкових двійкових чисел, як показано на рис. 5. Передані дані надходять із PN-послідовністю до суматора за модулем 2 для отримання результуючого сигналу, який наведено на рис. 6. BPSK-модулятор перетворює отриману послідовність на біполярну зі зворотною фазою (0 або 180), як зображено на рис. 7. На рис. 8 показано переданий у каналі з AWGN сигнал у разі відношення сигнал-шум, що дорівнює 10 дБ. Якщо в приймачі використовується правильний розширювальний PN-код, то отримані дані від BPSK-демодулятора є такими, як продемонстровано на рис. 9, де отримана послідовність еквівалентна переданій.

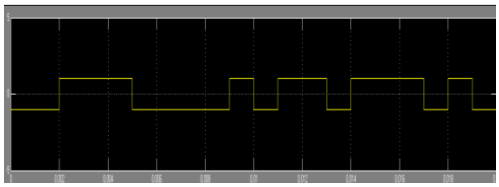


Рис. 4. Корисний сигнал

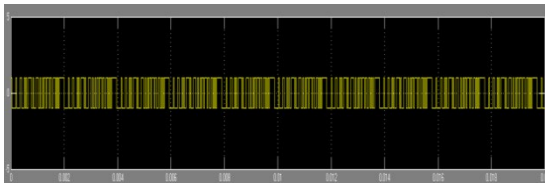


Рис. 5. Генерована послідовність псевдовипадкових двійкових чисел

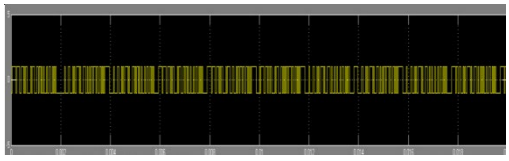


Рис. 6. Результат перемноження корисного сигналу та розширюючого коду

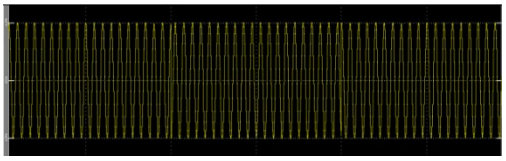


Рис. 7. Сигнал з виходу BPSK-модулятора

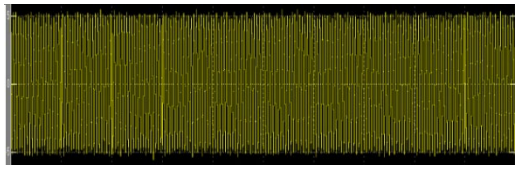


Рис. 8. Сигнал на вході BPSK-демодулятора

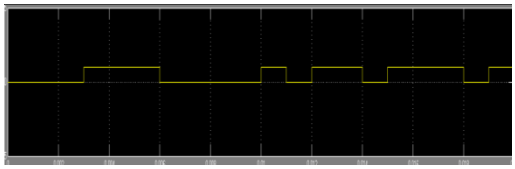


Рис. 9. Отримані дані, які відповідають переданому корисному сигналу

За допомогою моделі системи з DSSS у програмному середовищі MATLAB Simulink (рис. 3) було проведено оцінювання системи щодо такого параметра, як імовірність помилки на біт інформації (табл. 1, рис. 10). Було виявлено, що в разі роботи системи протягом 10 мс та загальної сумарної кількості переданих бітів, що становила 1000, BER виявився 0,008 для значення відношення сигнал-шум 5 дБ.

Таблиця 1

Порівняння залежності BER від $\frac{E_b}{N_0}$ для різних схем модуляції DSSS

$\frac{E_b}{N_0}$, (дБ)	Тип ФМ, що застосовується до ШСС				
	DSSS-BPSK	DSSS-QPSK	DSSS-8PSK	DSSS-16PSK	DSSS-QAM
1	2	3	4	5	6
-5	0,1934	0,3008	0,4279	0,6706	0,3723
-4	0,1774	0,2494	0,3796	0,591	0,3434
-3	0,1611	0,2182	0,3351	0,6084	0,3114
-2	0,1323	0,1826	0,2831	0,5664	0,2944
-1	0,1119	0,1505	0,2419	0,5185	0,2481
0	0,073	0,1202	0,1841	0,4603	0,2153
1	0,062	0,081	0,1228	0,4123	0,181
2	0,05	0,053	0,083	0,3745	0,13
3	0,03	0,031	0,051	0,33	0,112
4	0,018	0,005	0,028	0,2724	0,082
5	0,008	0,003	0,016	0,2262	0,054
6	0,003	0,002	0,08	0,1818	0,04
7	0	0,001	0,004	0,0117	0,02
8	0	0	0,001	0,078	0,001
9	0	0	0	0,046	0,004
10	0	0	0	0,022	0
11	0	0	0	0,014	0
12	0	0	0	0,008	0

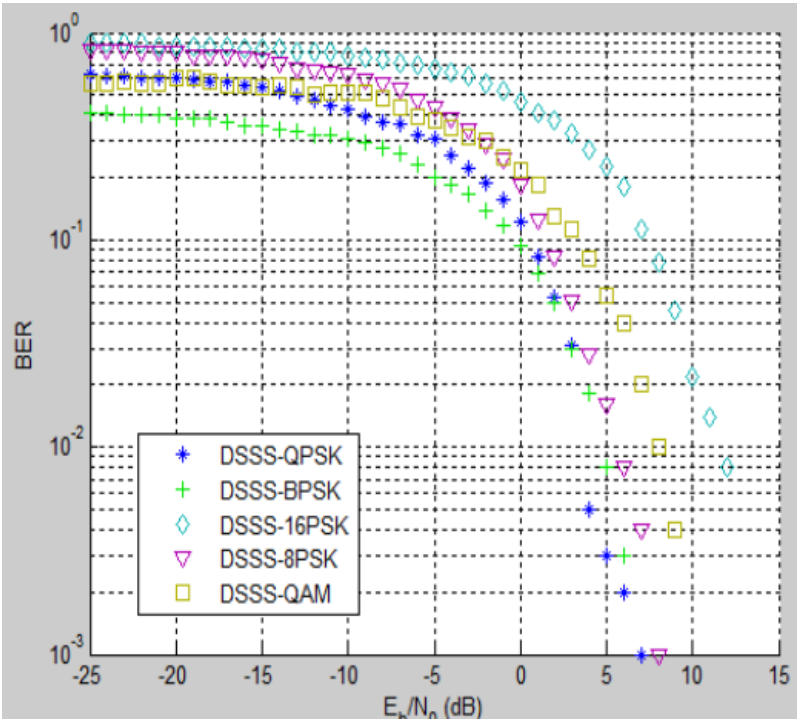


Рис. 10. Графік залежності BER від Eb/N0 для різних схем модуляції DSSS

Висновки. Бездротові системи зв'язку вразливі до впливу навмисних та ненавмисних перешкод, таких як втрати на шляху розповсюдження, радіоперешкоди тощо. Ці фактори обмежують дальність дії та надійність таких систем. Канал розповсюдження з AWGN – це модель каналу, у якій погіршення зв'язку є результатом лінійного додавання до корисного сигналу широкосмугового або білого шуму з постійною спектральною щільністю.

Встановлено, що система з DSSS-BPSK, у разі впливу в каналі розповсюдження AWGN, ефективніша щодо BER порівняно з іншими типами цифрових методів модуляції, такими як: QPSK, 8PSK, 16PSK та QAM, – як показано на графіку (рис. 10). На зображенні видно, що для досягнення BER = 10^{-3} необхідне значення $\frac{E_b}{N_0} = 6$, тоді як система з DSSS-QPSK, DSSS-4PSK, DSSS-16PSK та DSSS-QAM потребує вищих значень $\frac{E_b}{N_0}$ для досягнення того самого значення BER.

Результати моделювання показали, що для заданої швидкості передачі даних та за умови впливу AWGN на канал розповсюдження DSSS-BPSK виявилась більш стійкою до негативного впливу білого шуму. Майбутні дослідження будуть спрямовані на оцінювання ефективності системи зв'язку із ШСС у разі впливу різних типів перешкод.

СПИСОК ЛІТЕРАТУРИ

1. Recommendation ITU-R SM. 1055 the use of spread spectrum technique. URL: https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1055-0-199407-I!!PDF-E.pdf (last accessed: 25.08.2020).
2. Григорьев В. А., Лагутенхо О. И., Распаев Ю. А. Сети и системы радиодоступа. Москва : Эко-Трендз, 2005. 384 с.
3. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В. Широкополосные беспроводные сети передачи информации. Москва : Техносфера, 2005. 592 с.
4. Robert A. Scholtz. The Origins of Spread Spectrum Communications // IEEE transactions on Communications. Nov. 1982. Vol. 30, № 05. P. 822–852.
5. Donald Schilling, Laurence B. Milstein, Marvin Kullback, Frank Miller. Spread spectrum for commercial applications // IEEE communication magazine. April 1991. Vol. 29, Iss. 4. P. 66–79.
6. Manoj Barnela and Dr. Suresh Kumar. Digital Modulation Schemes Employed in Wireless Communication: A Literature review // International Journal of Engineering, Applied and Management Sciences Paradigms. April 2014. Vol. 14, Iss. 01. P. 1–9.
7. Kai Yang Narayan Prasad and Xiaodong Wang. A Message-Passing Approach to Distributed Resource Allocation in Uplink DFT-SpreadOFDMA Systems // IEEE transactions on Communications. April 2011. Vol. 59, № 4. P. 1099–1113.
8. Wang Ding, Zhao Yi-Xuas. Multi-subchannel spread spectrum for anti-jam communications // IEEE industrial conference on industrial control and electronics engineering. 2012. P. 161–165. ISBN: 978-1-4673-1450-3.
9. Феер К. Беспроводная цифровая связь. / Пер. з англ. Москва : Радио и связь, 2000. 519 с.
10. Скляр В. Цифровая связь. Теоретические основы и практическое применение. (2-е изд.). Прентис Холл, Нью-Джерси, 2001. 1104 с.

Подано 24.09.2020

REFERENCES

1. Recommendation ITU-R SM. 1055 the use of spread spectrum technique. (n.d.). Retrieved from https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1055-0-199407-I!!PDF-E.pdf.
2. Grigor'ev, B. A., Lagutenkho, O. I., & Raspaev, Iu. A. (2005). *Seti i sistemy radiodostupa [Radio access networks and systems]*. Moscow: Eko-Trendz [in Russian].
3. Vishnevskii, V. M., Liakhov, A. I., Portnoi, S. L., & Shakhnovich, I. V. (2005). *Shirokopolosnye besprovodnye seti peredachi informatsii [Broadband wireless information transmission networks]*. Moscow: Tekhnosfera [in Russian].
4. Robert A. Scholtz. (1982). The Origins of Spread Spectrum Communications. *IEEE transactions on Communications, Vol. 30,* № 05, 822–852.
5. Donald Schilling, Laurence B. Milstein, Marvin Kullback, Frank Miller. (1991). Spread spectrum for commercial applications. *IEEE communication magazine, Vol. 29,* Iss. 4, 66–79.
6. Manoj Barnela & Dr. Suresh Kumar. (2014). Digital Modulation Schemes Employed in Wireless Communication: A Literature review. I*nternational Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 14,* Iss. 01, 1–9.
7. Kai Yang Narayan Prasad & Xiaodong Wang. (2011). A Message-Passing Approach to Distributed Resource Allocation in Uplink DFT-SpreadOFDMA Systems. *IEEE transactions on Communications, Vol. 59,* № 4, 1099–1113.
8. Wang Ding, Zhao Yi-Xuas. (2012). Multi-subchannel spread spectrum for anti-jam communications. *IEEE industrial conference on industrial control and electronics engineering,* 161–165. ISBN: 978-1-4673-1450-3.
9. Feer, K. (2000). *Besprovodnaia tsifrovaia sviaz' [Wireless digital communication]*. Trans. from English. Moscow [in Russian].
10. Skliar, V. (2001). Tsifrovaia sviaz'. *Teoreticheskie osnovy i prakticheskoe primenenie [Digital Communications: fundamentals and applications]*. 2nd ed. Prentice Hall, New Jersey [in Russian].

O. M. Kubrak, V. O. Cholpanov, I. M. Dyukov

ESTIMATION OF BIT ERROR PROBABILITIES OF COMMUNICATION SYSTEMS WITH FM BROADBAND SIGNALS

Today, wireless communication is one of the most promising areas in the field of communications. Modern radio communication systems and facilities operate in a complex electronic environment. The development of next-generation wireless networks depends on both transmitting and receiving equipment, which must provide the high data rates needed to maintain a reliable level of interference protection. The main factors influencing the quality of radio communication are natural and intentional interference in the radio wave propagation channel, multi-beam propagation, bandwidth limitation and the need for asynchronous access. One of the possible methods of partial solution of the above problems is the use of extended spectrum communication systems.

The article investigates the effectiveness of different types of phase modulation used for Direct Sequence Spread Spectrum systems. An idealized channel with additive white Gaussian noise was chosen as the radio wave propagation channel. It has been observed that Binary

phase shift keying radio systems achieve better Bit error rate values than other systems. The research was conducted in the environment of dynamic interdisciplinary modeling of complex technical systems - Simulink (the main tool for model-oriented design), whose main interface is a graphical tool for charting and a flexible set of libraries of functional blocks.

The simulation results showed that for a given data rate and under the influence of AWGN on the propagation channel, DSSS-BPSK was more resistant to the negative effects of white noise. Future research will focus on evaluating the effectiveness of the SSS communication system in the event of different types of interference.

Keywords: *extended spectrum communication systems; phase modulation; bit error probability; noise immunity; Binary phase shift keying, Additive White Gaussian noise; Direct Sequence Spread Spectrum.*

УДК 623.618:629.05:004.03 DOI: 10.46972/2076-1546.2020.18.04

Ю. А. Ніцук, О. М. Семчак, І. В. Шаріпова

ШЛЯХИ ЗМЕНШЕННЯ ПОХИБОК РОЗРАХУНКІВ ЕОМ АВТОНОМНОГО РУХОМОГО ОБ'ЄКТА ДЛЯ АЛГОРИТМІВ SLAM НАВІГАЦІЇ

У статті розглянуто питання щодо проведення оцінювання складності алгоритмів EKF-SLAM та побудови карти місцевості відповідно до опорних точок з погляду його алгоритмічно-програмної реалізації. Це дає можливість визначати шляхи подальшого розвитку та адаптації відомих математичних співвідношень алгоритмів EKF-SLAM та DP-SLAM для зменшення похибок розрахунків координат бортовими ЕОМ автономного рухомого об'єкта для реалізації алгоритмів.

Оцінювання стану автономного мобільного пристрою здійснюють шляхом фільтрації частинок. Генерується безліч гіпотез, що є кінцевим числом, які передбачають місце розташування робота. Кожен значущий елемент карти, тобто орієнтир, у кожній частинці може бути оцінений із використанням розширених фільтрів Калмана, обумовлених позицією частинок робота. А коефіцієнт ваги частинок розраховується для визначення ймовірності попадання певної частинки в остаточний набір, який буде окреслювати не лише реальне місце розташування автономного рухомого об'єкта на карті, але й положення всіх виявлених орієнтирів.

Запропонований у роботі шлях модифікації відомих математичних співвідношень фільтрів Калмана щодо їх адаптації до особливостей алгоритмічної та програмної реалізації в бортових ЕОМ забезпечує економію пам'яті бортової ЕОМ і зменшення необхідного обчислювального ресурсу. Зауважено, що алгоритми реалізації SLAM навігації, змінені запропонованим шляхом, використовують меншу кількість частинок, ніж методи, що ґрунтуються тільки на частотному фільтрі. Помилка початкового обчислення координат орієнтирів зводиться до мінімуму і не накопичується з часом у математичному сенсі.

Ключові слова: *автономний рухомий об'єкт; Simultaneous Localization And Mapping; показники якості; прогнозування параметрів; експертна оцінка; короткострокове прогнозування; фільтр Калмана.*

Постановка проблеми в загальному вигляді. Точне знання положення робота є фундаментальною проблемою мобільної робототехніки. Адже саме з розв'язання задачі локалізації починається процес навігації. Однак на точність локалізації впливають випадкові й систематичні помилки в показаннях датчиків. Тому завдання синтезу високоточних алгоритмів обробки інформації датчиків мобільного автономного рухомого об'єкта для визначення його поточного положення в просторі є актуальним науково-прикладним завданням [1, 2].

Наявні системи інерціальної та супутникової навігації з об'єктивних причин не в повній мірі забезпечують необхідну точність визначення координат положення в просторі автономного рухомого об'єкта (АРО). У той же час розвиток технологій локальної навігації на основі візуального зворотного зв'язку в комплексі із застосуванням систем технічного поля зору дозволяє з високою точністю провести оцінювання не лише координат АРО, але й навколишніх об'єктів, розташованих у полі його зору [2, 3].

Аналіз останніх досліджень і публікацій. Визначення свого місця розташування робот може виконувати як на підставі апріорно наявної карти простору (місцевості), так і на підставі своїх спостережень. В ідеальному випадку є можливість завантажити роботу карту навколишнього простору, однак на практиці це малоймовірно, тому постає актуальне завдання: навчити робота будувати карту місцевості й одночасно визначати своє положення та траєкторію руху. Галузь знань, що описує методи вирішення даного завдання, отримала назву SLAM (Simultaneous Localization And Mapping) [4].

Задача SLAM поділяється на кілька підзадач: обчислення поточного становища робота на основі даних із датчиків або на основі GPS; знаходження нових точок інтересу; асоціація нових і старих даних; зберігання карти місцевості.

У ході реалізації відомих алгоритмів проведення арифметичних операцій унаслідок округлень результату обчислень, обумовлених поданням двійкових чисел у форматі з плаваючою комою, уже при складанні систем рівнянь та обчисленні поліномів 4-го ступеня починають накопичуватися помилки комп'ютерних розрахунків, які призводять до виродження матриць і унеможливлюють отримання результату обчислень [6–8]. Ці помилки пов'язані з обмеженою довжиною розрядної сітки ЕОМ (що зазвичай дорівнює 32 або 64 біти). Для вирішення зазначеної проблеми запропоновано метод подання чисел як масивів [7, 8].

Для вивчення особливостей алгоритмічної та програмної реалізації становить інтерес аналіз математичних співвідношень реалізації варіантів фільтра Калмана, висвітлений у [9]. Саме в згаданій роботі проведено вивчення можливостей використання різноманітних варіантів відомих фільтрів Калмана для оцінювання стану апріорі відомої динамічної системи. За своїм змістом це завдання схоже із завданням навігації АРО.

Формулювання завдання дослідження. Основними функціональними можливостями, які повинен мати АРО, є вирішення різноманітних прикладних задач зі збору інформації та виконання складних технологічних операцій у різнорідному середовищі, на відкритій місцевості або в складних міських умовах. Одне з ключових завдань пов'язане з необхідністю точного визначення координат точки свого положення та побудовою карти місцевості. Воно може бути вирішене критичним аналізом математичних співвідношень відомих алгоритмів EKF-SLAM навігації щодо їх алгоритмічної та програмної реалізації [14].

Виклад основного матеріалу. Алгоритм Extended Kalman Filter SLAM (EKF-SLAM) – метод, який ґрунтується на розширеному фільтрі Калмана для розв'язання задачі SLAM [15–17].

Фільтр Калмана – ефективний рекурсивний фільтр, що оцінює вектор стану динамічної системи, використовуючи низку неповних і зашумлених вимірювань. У теорії статистичного оцінювання розширений фільтр Калмана (EKF) – це нелінійна версія фільтра Калмана, що лінеаризується на позначці поточного середнього значення і коваріації. У разі добре визначених моделей переходу розширений фільтр Калмана фактично було визнано стандартом у теорії оцінювання нелінійних станів, навігаційних систем і GPS.

Використання фільтрів Калмана має на меті дооцінку вектора стану апріорі відомої динамічної системи, тобто для розрахунку поточного стану системи необхідно знати поточний

вимір, а також попередній стан самого фільтра [9, 18]. Для випадку навігації АРО це означає розв'язання задачі визначення місцезнаходження, що залежить від двох змінних:

$X_к$ – оцінка вектора поточного розташування АРО у момент часу *к;*

$P_к$ – коваріаційна матриця помилок (міра точності оцінювання поточного розташування АРО) у момент часу ***к***.

У [9, 12] зазначено, що розширений фільтр Калмана (EKF) дуже схожий на простий фільтр Калмана за винятком того, що він може бути використаний у нелінійних процесах. EKF – це один з найбільш поширених методів розв'язання задачі SLAM. Він дозволяє не лише уточнювати оцінку положення АРО на карті, але й положення всіх виявлених орієнтирів. Зазвичай процес оцінки стану системи в контексті SLAM розбивають на три етапи:

1) оновлення оцінки стану системи на основі одометричних даних;

2) оновлення оцінки стану системи на основі повторно виявлених орієнтирів;

3) додавання нових орієнтирів у систему.

У розширеному фільтрі Калмана моделі переходу та спостереження не повинні бути обов'язково лінійними функціями стану, натомість вони можуть бути нелінійними диференційованими функціями.

Функція еволюції процесу / системи в разі використання фільтра Калмана в завданнях навігації може використовуватися для обчислення передбачуваного стану з попередньої оцінки, тобто для визначення поточного та подальшого місця розташування на наступному кроці. Аналогічно функція вимірювань, що зв'язує істинний вектор стану і вектор проведених вимірювань, може використовуватися для обчислення передбачуваного вимірювання з передбаченого стану.

Проте ці функції не можуть застосовуватися до коваріації безпосередньо, натомість обчислюється матриця часткових похідних (матриця Якобі).

На кожному такті обчислень поточного місця розташування матриця Якобі обчислюється для поточних передбачених станів системи, тобто поточного місцезнаходження АРО. Ці матриці можуть використовуватися в рівняннях фільтра Калмана. Процес, власне, лінеаризує нелінійну функцію навколо поточної оцінки місця розташування АРО.

Оскільки фільтр Калмана є різновидом рекурсивних фільтрів, то для обчислення оцінки стану системи на поточний такт роботи йому необхідна оцінка стану на попередньому й вимірювання на поточному тактах.

У [9–11] зауважено, що попри всю свою привабливість EKF має низку недоліків, серед яких можна виокремити обмеження на кількість орієнтирів у системі. У [9] вказано, що ситуація обумовлена тим, що матриця P має розмірність mxm, де m – кількість виявлених орієнтирів. На кожному етапі оновлення матриці P має бути оновлений кожен її елемент, у зв'язку з чим істотно підвищується складність алгоритму визначення поточного місцезнаходження. У [9, 11] зроблено висновок, що EKF найбільше підходить до ситуації, коли середовище має не дуже велику кількість (декілька сотень) легко помітних орієнтирів.

Кожна ітерація фільтра Калмана ділиться на дві фази: екстраполяція (прогноз) і корекція. Зазвичай вони чергуються: екстраполяція проводиться за результатами корекції до наступного спостереження, а корекція – разом із доступними на наступному кроці спостереженнями [4, 5].

Під час екстраполяції фільтр отримує попередню оцінку стану системи на поточний крок за підсумковою оцінкою стану з попереднього кроку. Цю попередню оцінку також називають апріорною оцінкою стану, оскільки для її отримання не використовуються спостереження відповідного кроку.

Математичний опис оцінки стану динамічної системи на основі розширеного фільтра Калмана детально розглянуто в [9, 11].

Стан АРО в довільний момент часу описується за допомогою оцінки вектора його поточного місця розташування X_p і коваріаційної матриці P_p, що мають такий вигляд:

$$X_p = \left[x_p y_p \varphi_p \right]^T; \tag{1}$$

$$P_p = \begin{bmatrix} \sigma^2_{x_p x_p} & \sigma^2_{x_p y_p} & \sigma^2_{x_p \varphi_p} \\ \sigma^2_{x_p y_p} & \sigma^2_{y_p y_p} & \sigma^2_{y_p \varphi_p} \\ \sigma^2_{x_p \varphi_p} & \sigma^2_{y_p \varphi_p} & \sigma^2_{\varphi_p \varphi_p} \end{bmatrix}, \tag{2}$$

де x_p – оцінка координати АРО за віссю абсцис;

y_p – оцінка координати АРО за віссю ординат;

φ_p – оцінка кутової орієнтації АРО. Для відомих рухомих об’єктів аналогом цих значень є значення напрямку поздовжньої осі машини.

Коефіцієнти коваріаційної матриці P_p відображають міру залежності числового значення координат АРО один від одного. Діагональні елементи описують середньоквадратичну похибку оцінки числового значення координати за відповідною віссю [4, 9, 11]. На початку роботи системи навігації для цих змінних у програмній реалізації мають бути присвоєні значення за замовчуванням, що характеризують ситуацію невідомого положення АРО відносно орієнтирів положення. Якою б точною не була інформаційно-вимірювальна система АРО, у [9] запропоновано спеціально задати значення помилки оцінки початкового положення, відмінне від нуля. Така пропозиція обумовлена математичним припущенням того, що за реалізації фільтра на бортовій ЕОМ нульові значення на діагональних елементах можуть призвести до помилки в ході обчислення зворотної матриці [9, 19].

Координати виявлених орієнтирів за умови, що вони є нерухомими об’єктами, описуються у вигляді вектора оцінки координат орієнтирів X_0, і коваріаційної матриці P_0, що мають такий вигляд:

$$X_0 = \left[x\, y_1 \ldots x_n\, y_n \right]^T; \tag{3}$$

$$P_0 = \begin{bmatrix} \sigma^2_{(x_1 x_1)} & \sigma^2_{(x_1 x_1)} & \cdots & \sigma^2_{(x_1 x_n)} & \sigma^2_{(x_1 x_n)} \\ \sigma^2_{(x_1 y_1)} & \sigma^2_{(y_1 y_1)} & \cdots & \sigma^2_{(y_1 x_n)} & \sigma^2_{(y_1 x_n)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma^2_{(x_1 x_n)} & \sigma^2_{(y_1 x_n)} & \cdots & \sigma^2_{(x_p x_p)} & \sigma^2_{(x_n y_n)} \\ \sigma^2_{(x_1 y_n)} & \sigma^2_{(y_1 y_n)} & \cdots & \sigma^2_{(x_n y_n)} & \sigma^2_{(y_n y_n)} \end{bmatrix}, \tag{4}$$

де n – кількість орієнтирів, виявлених АРО;

x_i – оцінка координати *i*-го орієнтира за віссю абсцис;

y_i – оцінка координати *i*-го орієнтира за віссю ординат.

Матриця P_0 за своєю суттю відображає міру залежності оцінки числового значення координат місцевих орієнтирів за віссю абсцис та віссю ординат один від одного.

Поточне місцезнаходження АРО визначається вектором *X*, що відображає оцінку координат АРО і орієнтирів на поточному кроці ітераційних розрахунків, а також коваріаційною матрицею *P*, що мають такий вигляд:

$$X = \begin{bmatrix} X_p^T & X_0^T \end{bmatrix}^T ; \tag{5}$$

$$P = \begin{bmatrix} P_p & P_{p0} \\ P_{p0}^T & P_0 \end{bmatrix}, \tag{6}$$

де P_{p0} – коваріаційна матриця розмірністю *3xn*, що відображає залежність між оцінкою координат АРО і оцінками положення орієнтирів.

На початку руху АРО в програмній реалізації фільтра передбачаються такі числові значення координат місця розташування за замовчуванням:

$$X = X_p = 0, P = P_p.$$

У коваріаційній матриці P_p значення діагональних елементів встановлюються відмінними від нуля [9, 19], це реалізує помилку оцінки початкових координат старту руху АРО [9].

Розвитком фільтра Калмана для випадку навігації АРО є алгоритм Distributed Particle SLAM (DP-SLAM) [16, 17]. Це один з підходів до вирішенні завдань SLAM, який використовує числові значення змінних показників далекоміра і фільтр частинок для зберігання гіпотез про поточне значення координат АРО і конфігурації навколишнього середовища в сенсі значень координат орієнтирів.

Фільтр частинок (послідовний метод Монте-Карло) – рекурсивний алгоритм, що дозволяє на основі поточної карти обчислити найбільш імовірне положення робота за допомогою деякого набору (хмари) частинок, що займають простір станів.

Основна ідея методу фільтрації частинок полягає в поданні апостеріорного розподілу положення робота за допомогою кінцевого числа семплів, замість параметричного вигляду (наприклад, експоненційної функції в разі нормального розподілу). Таке уявлення є наближеним, але завдяки непараметричному вигляду дозволяє описати набагато складніші розподіли.

Під час руху робота відбувається збір даних з далекоміра та одометричних датчиків, а також побудова миттєвої карти простору з точок з імовірнісною характеристикою ваги (зважених частинок) [16, 17]. Чим більша вага частинки, тим вона значущіша. У міру переміщення є шанс зустріти ту ж частинку з деякою помилкою. З визначенням належності нової частинки до вже наявної її вага збільшується. Отже, повна карта складається з частинок з найбільшою вагою.

Модель простору станів складається з марковського процесу та масиву результатів процесу вимірів (поточних координат). Фільтр частинок зберігає зважену нормалізовану множину вибірки станів (поточних значень координат), нормалізує ваги для нової множини станів.

Хмара частинок, тобто множина координат, розрахованих відносно різних орієнтирів, характеризує невизначеність поточного місця розташування АРО. Чим більша кількість частинок-орієнтирів, тим більша ймовірність коректного визначення поточного місця розташування АРО. Одна частинка у фільтрі частинок містить положення і кутову орієнтацію робота. Імовірність частинок розраховується на основі різниці реальних свідчень далекоміра і показань, які повинні були б бути в даній частинці [4, 12].

DP-SLAM полягає в тому, що у фільтрі підтримується безліч гіпотез про поточний стан робота [16, 17]. У початковий момент генерується випадковий набір гіпотез. У ході роботи алгоритму деякі з них будуть відсіюватися через невідповідність вторинним ознакам системи, які можуть бути виміряні більш точно. У результаті після завершення циклу сканування вибирається найбільш вірогідна з тих гіпотез, що залишилися у фільтрі, вона і буде шуканою картою, на якій до того ж буде відзначена траєкторія руху виконавця.

Карта зберігається у вигляді зв'язного графа ієрархічної системи [15], що називають деревом, у вузлах якого знаходяться частинки. Завдання зберігання частинок карти спрощується введенням так званих частинок «батьків» і «нащадків». Кожен вузол може мати тільки одного з «батьків» і кілька «нащадків», завдяки чому в ході асоціації даних не потрібно проходити граф повністю. Пошук проводиться лише за «батьківськими» частинками до «нащадків».

DP-mapping зберігає тільки одну копію сітки зайнятості (карти). Ідея реалізації дерева успадкування частинок досить проста. Його коренем є початкова частинка, з якої походять всі інші. Кожна частинка містить покажчик на свого «батька», має унікальний ідентифікатор (ID) і зберігає список осередків карти, які вона оновила.

На рис. 1 концептуально показано «родовід» частинок й оновлення карт, листям – «дерева предків», що вказують на карти. Кожна червона крапка в дереві родоводу є вибірковою позицією робота, а чорні лінії навколо червоної крапки – нові спостереження, пов'язані з поточною позицією робота. Сіра лінія показує частину карти, успадковану від попередньої частинки.

Варто звернути увагу на те, що всі карти в цьому прикладі узгоджуються з початковим виглядом. Дві ліві карти узгоджуються зі спостереженнями, зробленими лівим ребром кореня, у той час як дві праві карти – зі спостереженнями, зробленими правим ребром кореня. Зберігання та повторне копіювання цих розділів карти щоразу, коли частинка повторно відбирається, марна трата пам'яті й часу. Замість цього використовується єдина сітка зайнятості, яка зберігає дерево спостережень на кожному квадраті.

На рис 2 показано, як кожна частинка вставляє свої спостереження в глобальну сітку. Вони зберігаються у вигляді збалансованого дерева, індексованого за унікальним ідентифікатором, присвоєним кожній частинці.

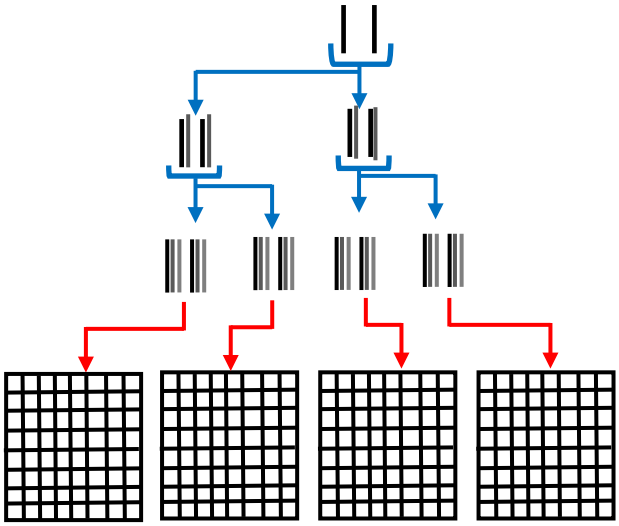


Рис. 1. Деревовидна система зберігання «гіпотетичних» карт

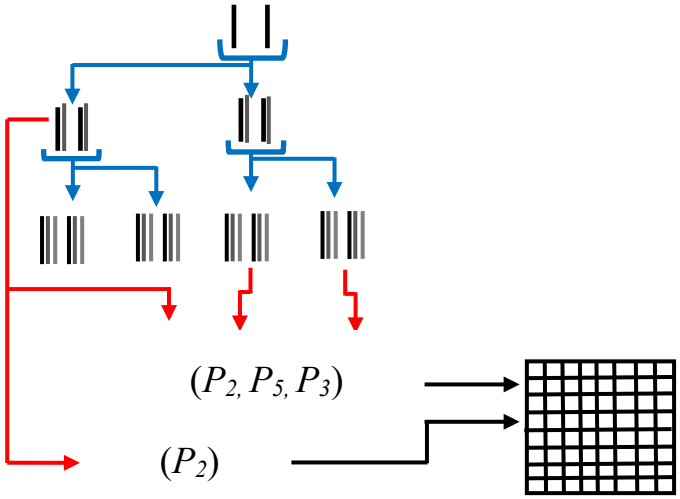


Рис. 2. Побудова карти за допомогою частинок

Звідси випливає, що перевагою алгоритму є низька складність:

$$O(ADlgP),$$

де A – кількість звернень частинки до карти в ході локалізації;

D – глибина вкладеності графа;

P – кількість частинок.

DP-SLAM має можливість швидко працювати з великими обсягами даних, але за умови $ADlgP > M$ знадобляться великі обчислювальні дані (де M – розмір карти).

Недоліком алгоритму є те, що для отримання коректного результату вимірювань необхідна велика кількість частинок.

На наступному кроці кожен орієнтир на карті оцінюється за допомогою розширеного фільтра Калмана. Усі EKF орієнтирів обумовлені шляхами робота, причому кожна частинка у фільтрі має власний набір EKF.

Якщо орієнтир виявлений уперше, то необхідно реалізувати такі кроки в алгоритмі програмної реалізації:

виконати ініціалізацію позиції орієнтира на основі вимірів і поточної позиції частинки;

знайти матрицю Якобі;

сформувати EKF для даного орієнтира;

в іншому разі:

отримати очікувані вимірювання і матрицю Якобі;

обчислити коваріацію вимірювань;

розрахувати посилення Калмана;

обчислити помилку між фактичним і прогнозованим наглядом;

оновити середнє значення й коваріацію EKF.

У результаті виконання даного кроку алгоритму кожна частинка матиме *N* орієнтирів, поданих за допомогою EKF.

Етап повторної вибірки є важливим аспектом, який чинить основний вплив на продуктивність фільтра частинок. Під час повторної вибірки частинки з низькою вагою зазвичай замінюються зразками з вищою вагою. З одного боку, необхідна повторна вибірка, оскільки використовується тільки кінцева кількість частинок. З іншого – етап повторної вибірки може видалити хороші зразки з набору, зумовлюючи виснаження частинок. Відповідно, важливо знайти критерій, коли виконувати етап повторної вибірки. У роботі [18] введено так зване «ефективне число» частинок, щоб оцінити, наскільки добре поточний набір частинок описує справжній апостеріор.

У запропонованому алгоритмі передбачено, що щоразу, коли вага частинки падає нижче заданого значення, то буде проводитися повторна вибірка. Цей підхід значно знижує ризик заміни хороших частинок, оскільки кількість операцій повторної вибірки скорочується, бо вони виконуються тільки за необхідності.

Повторна вибірка виконується відповідно до так званої «вибірки з низькою дисперсією», розглянутої в роботах [16–18].

Висновки. Отже, під час модифікації відомих математичних співвідношень фільтрів Калмана щодо їх адаптації до особливостей алгоритмічної та програмної реалізації в бортових ЕОМ забезпечується економія пам’яті апаратури та зменшення необхідного обчислювального ресурсу.

Найбільш доцільним шляхом зменшення похибок розрахунків координат бортовими ЕОМ автономного рухомого об’єкта для реалізації алгоритмів EKF-SLAM навігації є розроблення алгоритму, що поєднує позитивні властивості розглянутих алгоритмів SLAM навігації.

Удосконалені алгоритми EKF-SLAM навігації використовують меншу кількість частинок, ніж методи, що ґрунтуються тільки на частотному фільтрі. А помилка початкового обчислення координат орієнтирів зводиться до мінімуму і не накопичується з часом у математичному сенсі. З використанням методу подання чисел як масивів зводиться до мінімуму помилка початкового обчислення координат орієнтирів у сенсі подання чисел на рівні мікроархітектури програмних кодів базових арифметичних операцій.

Оцінювання поточного значення координат АРО в разі створення вдосконаленого алгоритму фільтрації досягається шляхом фільтрації частинок. Кожен елемент карти

в кожній частинці може бути оцінений з використанням розширених фільтрів Калмана, обумовлених позицією частинок робота. Коефіцієнт ваги частинок розраховується для визначення ймовірності попадання певної частинки в остаточний набір, який становитиме реальне місце розташування.

Запропонований шлях зменшення похибок розрахунків координат бортовими ЕОМ АРО для реалізації алгоритмів EKF-SLAM навігації використовує меншу кількість частинок зі зведенням до мінімуму ймовірності помилки поточного обчислення координат, що не накопичується з часом.

СПИСОК ЛІТЕРАТУРИ

1. Захаров А. А., Тужилкин А. Ю., Веденин А. С. Алгоритм определения положения и ориентации трехмерных объектов по видеоизображениям на основе вероятностного подхода // Фундаментальные исследования. 2014. № 11-8. С. 1683–1687.

2. Menache A. Understanding motion capture for computer animation. The Morgan Kaufmann Series In Computer Graphics. 2011. 254 p.

3. Tobon R. The Mocap Book: A Practical Guide to the Art of Motion Capture. Forisforce. 2010. 258 p.

4. SLAM – что это такое. URL: https://icleborobot.by/slam-chto-eto-v-navigatsii.html (дата обращения: 15.12.2018).

5. Nguyen V., Harati A., Siegwart R. Lightweight SLAM algorithm using orthogonal planes for indoor mobile robotics // Intelligent Robots and Systems. 2007. P. 658–663. DOI: http://doi.org/10.1109/iros.2007.4399512

6. Левченко А. А., Войтенков Р. М. Анализ предельных точностей вычислений в информационных системах с представлением чисел с плавающей запятой // Збірка тез доп. 3-го наук.-техн. семінару “Перспективні шляхи розвитку інформаційних систем прицілювання та самонаведення високоточного озброєння РВіА”. Львів : АСВ, 2012. С. 119.

7. Levchenko A. Arithmetic operation for binari numbers represettated as arrays // Modern engineering and innovative technologies / International periodic scientific journal. Karlsruhe, Germany. 2019. № 9, Part 1. P. 51–59.

8. Левченко А. О., Войтенков Р. М. Метод подання чисел для програмних засобів гарантоздатних інформаційних технологій систем підтримки прийняття рішень для керування станом ОВТ // Збірник тез доповідей 19-ї наук.-практ. конф. (“Проблеми створення, розвитку та застосування інформаційних систем спеціального призначення”, 19 квітн. 2012, м. Житомир). Житомир : ЖВІ НАУ, 2012. С. 142–143.

9. Кучерский Р. В., Манько С. В. Алгоритмы локальной навигации и картографии для бортовой системы управления автономного мобильного робота // Известия ЮФУ. Технические Науки. 2012. № 3 (128). С. 13–22.

10. Semchak O., Levchenko A. Disadvanteges of computer implementation of SLAM-metods of local navigation autonovus mobile objects // SWorld journal : International periodic scientific journal. Sofia, Bulgaria. 2019. № 2, Part 2. P. 108–115.

11. Aulinas J. The SLAM Problem: A Survey // Proceedings of the 2008 Conference on Artificial Intelligence Research & Development. 2008. P. 363–71. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.163.6439 (last accessed: 15.07.2020).

12. Любкевич К. О., Гунченко Ю. О. Локалізація мобільного робота на місцевості. // Збірник матеріалів XIV Всеукр. конф. студентів і молодих науковців (“Інформатика, інформаційні системи та технології”). Одеса, 2017. С. 188.
13. Methods and technologies of monitoring of the position of a mobile object in space: Proceedings / Nechyporenko O. V. et. al. // Kompiuterne modeliuvannia ta optymizatsiia skladnykh system (KMOSS-2018). Dnipro : Balans-klub, 2018. P. 193–195.
14. Levchenko A. Features of implementation of information technology for provision of numerical value of parameters // Modern engineering and innovative technologies // International periodic scientific journal. Karlsruhe, Germany. 2019. № 10, Part 1. P. 36–42.
15. Robot Mapping And Ekf Slam. URL: https://slideplayer.com/slide/5983202/ (last accessed: 10.01.2018).
16. Eliazar Austin I., Ronald Parr. DP-SLAM 2.0 // ICRA ’04: IEEE International Conference on Robotics and Automation. 2004. Vol. 2. P. 1314–1320.
17. Austin Eliazarand, Ronald Parr. DP-SLAM. URL: https://users.cs.duke.edu/~parr/dpslam/ – (last accessed: 10.02.2018).
18. Doucet A., Freitas N., Murphy K. P., Russell S. J. Rao-Blackwellised particle filtering for dynamic Bayesian net works // Proc. of the 16th Conf.48 on Uncertainty in Artificial Intelligence. San-Francisco: Morgan Kaufmann Publisers Inc, 2000. P. 176–183.
19. Левченко А. О., Войтенков Р. М. Витоки втрати працездатності систем діагностики ОВТ другого роду з представленням чисел з плаваючою комою // Сб. науч. труд. Sword. 2014. Вип. № 4 (37), Том 5. С. 27–35.

Подано 06.11.2020

REFERENCES

1. Zakharov, A. A., Tuzhylkyn, A. Yu., & Vedenyn, A. S. (2014). Alhorytm opredelenyia polozhenyia y oryentatsyy trekhmernykh ob"ektov po vydeoyzobrazhenyiam na osnove veroiatnostnoho podkhoda [Algorithm for determining the position and orientation of three-dimensional objects from video images based on a probabilistic approach]. *Fundamentalnye yssledovanyia [Basic research], 11-8,* 1683–1687 [in Russian].
2. Menache, A. (2011). Understanding motion capture for computer animation. The Morgan Kaufmann Series In Computer Graphics.
3. Tobon, R. (2010). The Mocap Book: A Practical Guide to the Art of Motion Capture. Forisforce.
4. SLAM – chto eto takoe. (n.d.). Retrieved from https://icleborobot.by/slam-chto-eto-v-navigatsii.html [in Russian].
5. Nguyen V., Harati, A., & Siegwart, R. (2007). Lightweight SLAM algorithm using orthogonal planes for indoor mobile robotics. *Intelligent Robots and Systems,* 658–663. http://doi.org/10.1109/iros.2007.4399512
6. Levchenko, A. A., & Voitenkov, R. M. (2012). Analyz predelnykh tochnostei vychyslenyi v ynformatsyonnykh systemakh s predstavlenyem chysel s plavaiushchei zapiatoi [Analysis of the limiting accuracy of calculations in information systems with the representation of floating point numbers]. In *Zbirka tez dop. 3-ho nauk.-tekhn. seminaru [Collection of abstracts of papers 3rd scientific-technical seminar]*. (“Perspektyvni shliakhy rozvytku informatsiinykh system

prytsiliuvannia ta samonavedennia vysokotochnoho ozbroiennia RViA" ["Prospective ways of development of information systems for aiming and homing high-precision weapons"]). (p. 119). Lviv: NAA [in Russian].

7. Levchenko, A. (2019). Arithmetic operation for binari numbers represettated as arrays. *Modern engineering and innovative technologies. International periodic scientific journal, 9* (1), 51–59. Karlsruhe, Germany.

8. Levchenko, A. O., & Voitenkov, R. M. (2012). Metod podannia chysel dlia prohramnykh zasobiv harantozdatnykh informatsiinykh tekhnolohii system pidtrymky pryiniattia rishen dlia keruvannia stanom OVT [The method of representing numbers for software tools of guaranteeing information technologies of decision support systems for the management of weapons and military equipment]. In *Zbirnyk tez dopovidei 19-i nauk.-prakt. konf. [Collection of abstracts of the 19th scientific-practical conference]* ("Problemy stvorennia, rozvytku ta zastosuvannia informatsiinykh system spetsialnoho pryznachennia" ["Problems of creation, development and application of special purpose information systems"]). Zhytomyr, April 19, 2012. (pp. 142–143). Zhytomyr : ZhMI NAU [in Ukrainian].

9. Kucherskyi, R. V., & Manko, S. V. (2012). Alhorytmy lokalnoi navyhatsyy y kartohrafyy dlia bortovoi systemy upravlenyia avtonomnoho mobylnoho robota [Local navigation and mapping algorithms for the on-board control system of an autonomous mobile robot]. *Yzvestyia YuFU. Tekhnycheskye Nauky [Izvestia UFU. Technical science], 3* (128), 13–22 [in Russian].

10. Semchak, O., & Levchenko, A. (2019). Disadvanteges of computer implementation of SLAM-metods of local navigation autonovus mobile objects. *SWorld journal. International periodic scientific journal, 2* (2), 108–115. Sofia, Bulgaria.

11. Aulinas J. (2008). The SLAM Problem: A Survey. In *Proceedings of the 2008 Conference on Artificial Intelligence Research & Development*. (p. 363–371). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.163.6439

12. Liubkevych, K. O., & Hunchenko, Yu. O. (2017). Lokalizatsiia mobilnoho robota na mistsevosti [Localization of mobile robot in the field]. In *Zbirnyk materialiv XIV Vseukr. konf. studentiv i molodykh naukovtsiv [Collection of materials XIV All-Ukrainian. conf. students and young scientists]* ("Informatyka, informatsiini systemy ta tekhnolohii" ["Informatics, information systems and technologies"]). (p. 188). Odesa [in Ukrainian].

13. Nechyporenko, O. V. et. al. (2018). Methods and technologies of monitoring of the position of a mobile object in space. *Kompiuterne modeliuvannia ta optymizatsiia skladnykh system* (KMOSS-2018) *[Computer modeling and optimization of complex systems (CMOCS-2018)]*. (pp. 193–195). Dnipro: Balans-klub.

14. Levchenko, A. (2019). Features of implementation of information technology for provision of numerical value of parameters. *Modern engineering and innovative technologies. International periodic scientific journal, 10* (1), 36–42. Karlsruhe, Germany.

15. Robot Mapping And Ekf Slam. (n.d.). Retrieved from https://slideplayer.com/slide/5983202/

16. Eliazar Austin, I., & Ronald Parr. (2004). DP-SLAM 2.0. *ICRA '04: IEEE International Conference on Robotics and Automation, Vol. 2,* 1314–1320.

17. Austin Eliazarand, Ronald Parr. (n.d.). DP-SLAM. Retrieved from https://users.cs.duke.edu/~parr/dpslam

18. Doucet, A., Freitas, N., Murphy, K. P., & Russell, S. J. (2000). Rao-Blackwellised particle filtering for dynamic Bayesian net works. In *Proc. of the 16th Conf.48 on Uncertainty in Artificial Intelligence.* (pp. 176–183). San-Francisco: Morgan Kaufmann Publisers Inc.

19. Levchenko, A. O., & Voitenkov, R. M. (2014). Vytoky vtraty pratsezdatnosti system diahnostyky OVT druhoho rodu z predstavlenniam chysel z plavaiuchoiu komoiu [Sources of disability of weapons diagnostics systems and military equipment of the second kind with the representation of floating point numbers]. *Sb. nauch. trud. Sword [Collection of scientific papers Sword], Vol. 4* (37), Iss. 5, 27–35 [in Ukrainian].

Yu. A. Nitsuk, O. M. Semchak, I. V. Sharipova

WAYS OF DIMINISHING OF ERRORS OF CALCULATIONS OF COMPUTER OF AUTONOMOUS MOBILE OBJECT ARE FOR ALGORITHMS OF SLAM OF NAVIGATION

A question is in-process considered, in relation to the lead through of estimation of complication of algorithms of EKF-SLAM and construction of map of locality in accordance with supporting points, from point of his algorithmically programmatic realization. It enables to determine the ways of subsequent development and adaptation of the known mathematical correlations of algorithms of EKF-SLAM and DP-SLAM for diminishing of errors of calculations of co-ordinates airborne COMPUTERS of autonomous mobile object for realization of algorithms.

The estimation of the state of off-line mobile unit is arrived at by filtration of particles. The great number of hypotheses which are an eventual number is generated, which show by itself the predictable place of location of robot. Every meaningful element of map, that orienteer, in every particle can be appraised with the use of the extended filters of Kalmana, particles of robot conditioned position.

And the coefficient of weight of particles settles accounts for determination of probability of hit of certain part in a final set, which will present not only the real place of location of autonomous mobile object on a map but also position of found out all orienteers.

The way of modification of the known mathematical correlations of filters of Kalmana offered in-process from point of their adaptation to the features of algorithmic and programmatic realization in airborne COMPUTERS provides economy of memory of airborne COMPUTER and diminishing of necessary calculable resource

It is noticed that the algorithms of realization of SLAM of navigation are changed the offered way use less of particles, than methods, based only on a frequency filter. The error of initial calculation of co-ordinates of orienteer is taken to the minimum and does not accumulate in course of time in mathematical sense.

Keywords: *autonomous mobile object; Simultaneous Localization And Mapping; indexes of quality; prognostication of parameters; expert estimation; short-term prognostication; filter of Kalmana.*

ISSN 2076-1546

УДК 623.624.2 DOI: 10.46972/2076-1546.2020.18.05

Р. М. Олійник, С. В. Цілина, Ю. М. Живець, О. В. Єрмоленко

СИСТЕМИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ З БЕЗПІЛОТНИМИ АПАРАТАМИ МУЛЬТИРОТОРНОГО ТИПУ В РАЙОНАХ ВЕДЕННЯ БОЙОВИХ ДІЙ

В умовах сучасного ведення війни інформаційна складова має вирішальне значення для обох сторін конфлікту. Донецька і Луганська області стали своєрідним плацдармом для випробувань і застосування в дії безпілотних літальних апаратів різних габаритів та функціонального призначення, найпоширенішими серед яких є невеликі розвідувальні безпілотні літальні апарати. Десятки ворожих апаратів збирають інформацію про місце дислокації українських військових.

На сьогоднішній день жодна держава не готова протистояти спланованим атакам безпілотних літальних апаратів. Традиційні види озброєння протиповітряної оборони розраховані на великі й віддалені цілі, у той час як сучасна лінійка безпілотників складається з нано-, мікро- і мініапаратів, що літають на малих висотах.

Проведено порівняльний аналіз сучасних засобів протидії безпілотним літальним апаратам та зроблено висновки щодо можливості їх застосування у Збройних Силах України. Розглянуто новітні засоби знищення безпілотних літальних апаратів провідних країн світу. Висвітлено питання щодо можливості блокування роботи ворожих дронів у зонах (районах) ведення бойових дій. Запропоновано шляхи підвищення ефективності боротьби з малорозмірними безпілотними літальними апаратами.

Пріоритетами в реалізації програм розробки сучасних вітчизняних засобів знищення безпілотних літальних апаратів можна вважати використання засобів їх перехоплення або знищення за допомогою систем електронної протидії.

Актуальність дослідження полягає в аналізі основних наявних методів боротьби з безпілотними літальними апаратами, розробці перспективних підходів та ознайомленні із сучасними досягненнями й напрямками розвитку засобів боротьби з дронами, що застосовуються противником.

Ключові слова: *мобільні засоби радіоелектронної боротьби; засоби знищення безпілотних літальних апаратів; розвідувальні безпілотні літальні апарати мультироторного типу; дрон.*

Постановка проблеми в загальному вигляді. У районі проведення операції Об’єднаних сил (ООС) на сході України проводяться польоти безпілотних літальних апаратів (БпЛА) для розвідки в інтересах артилерійських підрозділів як незаконних збройних формувань, так і підрозділів Збройних сил (ЗС) РФ. Підтверджено факти, коли після обльоту БпЛА через нетривалий час здійснювалися обстріли позицій підрозділів ЗС України з артилерійського та танкового озброєння.

БпЛА стали невід’ємною частиною бойових дій у воєнних конфліктах у всьому світі. В умовах збройного протистояння на Донбасі, зокрема із застосуванням дороговартісних, професійно виготовлених розвідувальних і ударних безпілотників, значною проблемою

в умовах безпосереднього зіткнення з противником є їх дешеві зразки. Справа в тому, що навіть коптер побутового рівня здатний доставити на передову мініатюрний вибуховий або запалювальний пристрій, виконувати розвідувальні функції та виступати в ролі корегувальника вогню.

Досвід ведення бойових дій показав, що знищити малогабаритний квадрокоптер зі стрілецької зброї не завжди вдається, а витрачати зенітні снаряди або дорогі ракети на копійчаний виріб недоцільно. Однак, враховуючи той факт, що навіть дешеві ворожі квадрокоптери доставляють противнику цінну розвідувальну інформацію, необхідність їх знищення або блокування роботи є одним із пріоритетних завдань.

БпЛА можливо «майже нейтралізувати», якщо під час польоту порушити роботу його бортових датчиків, забити канали зв'язку, передачі даних і контролю, заглушити сигнали системи GPS, унаслідок чого він стає «сліпим і безпорадним». Знищити його по-справжньому можна тільки фізично, уразивши ракетою, снарядом з гармати або променем лазерної гармати. Інформаційне заглушення за допомогою систем радіоелектронної боротьби (РЕБ) буде застосовуватися для будь-яких без винятку безпілотників.

Для вибору засобів фізичного знищення потрібно мати справу з критеріями вартість-ефективність.

Чи не єдиним способом для нашої армії знешкодити такі пристрої є знищення їх за допомогою стрілецької зброї або зенітних установок. Однак для нейтралізації невеликого безпілотника такі методи неефективні й вимагають значних ресурсів. Тому проти міні-БпЛА доцільно використовувати засоби РЕБ.

Аналіз останніх досліджень і публікацій. Щорічно розробники з усього світу представляють нові системи знешкодження БпЛА. Першими над проєктуванням портативного пристрою РЕБ проти безпілотників задумалися американці. Компанія Battelle в 2015 році розробила унікальну антидронову гвинтівку. Зброя здатна «збивати» безпілотники на відстані до 400 м. Пристрій створює радіоперешкоди, після чого БпЛА зазвичай застосовує протокол безпеки і виконує одну із запрограмованих дій: зависає в повітрі, здійснює посадку або повертається назад. У будь-якому разі оператор втрачає контроль над дроном і змушений перервати місію. Хоча перша антидронова гвинтівка використовувалася переважно для контролю повітряного простору під час масових громадських заходів, військові схвалили можливість адаптації портативної гвинтівки для реальних бойових умов.

За останні роки українська промисловість створила декілька зразків мобільних засобів РЕБ із ворожими БпЛА. На рис. 1 наведено один зі зразків антидронової гвинтівки [1]. Вона має направлену дію, блокує сигнали телеметрії, GPS-навігації та керування на дистанції від одного до шести кілометрів. Сподіваємося, що вже в найближчий час війська ЗС України будуть використовувати радіоелектронні гвинтівки в боротьбі з БпЛА противника.

До деякої міри аналогом українських розробок є російська антидронова гвинтівка «Ступор» (див. рис. 2), створена московським ТОВ «Локационная мастерская "ЛОКМАС"» [2].

Досить ефективним є варіант «spoofing attack» – перехват керування. Достатньо вдалою розробкою в цьому напрямку є білоруський комплекс «Гроза-С» (див. рис. 3), який базується

на автомобільному шасі [3]. На мачтах розміщено основні антенні блоки, а додаткову антену – під півсферичним обтічником. У комплексі є також засоби оптико-електронного спостереження. Стверджується, що він здатний посадити навіть захищений БпЛА.

Рис. 1. Українська антидронова гвинтівка

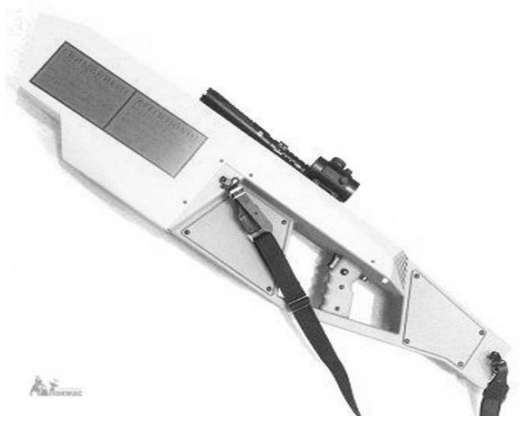


Рис. 2. Російська антидронова гвинтівка «Ступор»

Рис. 3. Комплекс «Гроза-С» (Білорусь)

Рис. 4. Комплекс РЕБ Vigilant Falcon (США)

Рис. 5. Радіолокаційна система Harrier (США)

Рис. 6. Комплекс EDM4S (Литва)

Окремо також слід зазначити ще одне технологічне рішення вітчизняної розробки, яке відповідає сучасним трендам. Так, приватна українська компанія «CONUS RESEARCH & MFG COMPANY» створила антидронову гвинтівку JAMMERGUN 3, яка

подавляє навігаційне управління, а також блокує передачу будь-якої інформації на панель управління міні-БпЛА. Фактично вона аналогічна таким системам як DroneGun Tactical та DroneDefender (США), «Rex-1» та «Ступор» (РФ), «Гроза-Р» (Білорусь).

JAMMERGUN 3 має у своєму складі антени типу «хвильовий канал», підключені до основного блоку живлення за допомогою RF-кабелів. Гвинтівка розміщується в рюкзаку з карманами для додаткового пристрою, що забезпечує зручність використання. Рюкзак інтегрований із системою охолодження й захищений від води та бруду. Для зручності на держак можна встановити коліматорний приціл – це значно покращить точність наведення на ціль.

Радіус подавлення сигналів БпЛА становить 0,1–0,6 км, а час безперервної роботи – 30 хв. Вага системи – 10 кг.

На рис. 4. показано установку Vigilant Falcon компанії SRC, яка ефективно виконує функції виявлення і перехвату керування БпЛА. На рис. 5 – базовий модуль радіолокаційної системи Harrier від компанії De Tect, який забезпечує виявлення БпЛА на відстані до 16 км, визначає траєкторію, швидкість руху й селекцію об’єктів [4].

Усі сучасні радари працюють у комплексі з оптико-електронними станціями. Це Harrier компанії De Tect (США), HAMMR компанії Northrop Grumman (США), радари LTAR і VIGILANT FALCON компанії SRC (США), радар SQUIRE компанії Thales (Франція), які дозволяють виявляти БпЛА, що працюють у режимі радіомовчання. Коли дрон здійснює обмін даними зі станцією керування, то питань його ідентифікації засобами РЕБ уже не існує [5].

Як показали події на сході України та в Сирії, БпЛА навіть побутового рівня здатні ефективно знищувати склади боєприпасів. На основі негативного досвіду бойових дій у Сирії Росія вже сформувала підрозділи з боротьби з БпЛА в Західному і Центральному військових округах, а також на військових базах у Киргизії та Таджикистані [6].

Одним із нововведень в електронній війні проти БпЛА є спрямований вплив на ціль потужним НВЧ-випромінюванням, яке здатне спалити будь-яке радіоелектронне обладнання, знищити пам’ять, програмне забезпечення та перетворити тим самим безпілотник у просту «залізяку». Прикладом такого озброєння є мікрохвильова гармата Phaser компанії Raytheon.

Дрони-перехоплювачі, лазерні гармати, НВЧ-гармати, радіоелектронні гвинтівки – усе це свідчить про те, що конструктори всього світу почали активну розробку засобів боротьби з БпЛА.

Досвід, отриманий під час виконання визначальних відомчих випробувань дослідного зразка комплексу протидії БпЛА EDM4S виробництва компанії «NT Service» (Литва), є основним змістом публікації.

Формулювання завдання дослідження. Дослідження полягає в аналізі основних наявних методів боротьби з безпілотними літальними апаратами, розробці перспективних підходів та ознайомленні із сучасними досягненнями й напрямками розвитку засобів боротьби з дронами, що застосовуються противником.

Виклад основного матеріалу. Ідею створення невеликого й ефективного пристрою проти БпЛА підхопили турецькі розробники. Компанією «Aselsan» була створена антидронова система IHASAVAR. Це комплект із портативного рюкзака й антидронового

глушника-гвинтівки, призначений для захисту військових баз, важливих об'єктів, місць проведення зустрічей і демонстрацій тощо. Завдяки високопотужній спрямованій антені, система IHASAVAR має високу ефективність у боротьбі з БпЛА. Пристрій використовує частоти від 400 МГц до 3000 МГц і від 5700 МГц до 5900 МГц. Електричне поле відповідає стандартам Міжнародної комісії з радіаційного захисту, тому пристрій безпечний для людини. Час безперервної роботи системи – півтори години.

Знешкодження міні-БпЛА або дронів відбувається шляхом постановки перешкод на частотах дистанційного керування, супутників GPS або ГЛОНАСС, каналів передачі даних, телеметрії. У такий спосіб рушниця повністю «відрізає» безпілотник від оператора. Пристрій усуває необхідність відстеження сенсорних систем і дозволяє відразу знешкодити БпЛА.

Серед індивідуальних засобів знищення БпЛА можна виокремити DroneDefender, яка стала першою у світі гвинтівкою для нейтралізації безпілотників. Це засіб РЕБ, який у змозі генерувати сигнал на частотах систем супутникової навігації, а також на частотах неліцензованого діапазону IMS. Нею можна «вражати» БпЛА на відстані до 400 м. Після впливу на дрони за допомогою радіоперешкод вони зазвичай задіюють свій протокол безпеки. Найчастіше це передбачає кілька можливих сценаріїв розвитку подій: зависання безпілотника над поточною позицією (до подальшого падіння після розрядки акумуляторних батарей); посадка на землю або повернення апарата в точку старту. При цьому в будь-якому разі виконання ним завдання буде перервано.

Українські розробники теж не стоять осторонь. Фахівці ХК «Укрспецтехніка» представили першу вітчизняну радіоелектронну рушницю. З дальністю дії до 2 км і часом автономної роботи 8 годин ця зброя може бути використана як у зоні бойових дій, так і для супроводу військових колон. Кругові антени пристрою надають можливість постановки над об'єктом купола перешкод радіусом до 5 км. Однак поки етап випробувань за методиками військових ще не відбувся. Не виключено, що ці випробування будуть проходити одночасно для українських і турецьких розробок.

Найбільш простий і логічний спосіб позбутися від ворожого БпЛА – знищити його. Будь-яка літаюча техніка може бути збита. Головною проблемою в цій справі є виявлення цілі та проведення успішної атаки на неї. При цьому для нейтралізації може використовуватися найрізноманітніше озброєння.

Знищення БпЛА пов'язано з низкою складнощів у справі його виявлення і ураження, тому розглянемо наступний метод протидії – подавлення радіоелектронних систем. Деякі сучасні безпілотники мають можливість автономного виконання тих чи інших завдань, проте майже вся подібна техніка керується оператором, а команди передаються радіоканалом. Отже, заглушення каналу управління засобами РЕБ здатне як мінімум перешкодити виконанню завдання.

На озброєнні армій країн світу знаходиться велика кількість різноманітних систем РЕБ. Для успішного подавлення роботи ворожого БпЛА необхідно встановити частоти, на яких ведеться управління ним, після чого «забити» їх перешкодами. Далеко не всі сучасні безпілотники комплектуються автоматикою, здатною взяти на себе управління в разі втрати сигналу від оператора. Крім того, втрата зв'язку з оператором призведе до неможливості передачі такої розвідувальної інформації, як відеосигнал з камери дрона.

На випадок обриву каналу зв'язку з оператором деякі БпЛА мають відповідний автономний режим роботи. У разі втрати сигналу від пульта автоматика повертає

безпілотник у заданий район, де той може здійснити посадку. За таких умов система управління ігнорує всі сигнали, а переміщення в зазначену зону здійснюється за допомогою супутникової навігації. Використовуючи систему GPS, літальний апарат може визначити власне положення в просторі, напрямок і дальність до оператора або аеродрому і повернутися до нього. Щоб не допустити «евакуації» безпілотника, засоби РЕБ повинні заглушати не тільки канал управління, але й сигнали навігаційної системи. У результаті успішного «забиття» всіх цих сигналів противник з високою ймовірністю втратить свою техніку.

Під час проведення визначальних відомчих випробувань на базі Житомирського військового інституту імені С. П. Корольова за участю Головного управління оперативного забезпечення ЗС України та Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки були проведені дослідження зразка комплексу протидії БпЛА EDM4S (виробництва компанії «NT Service») (див. рис. 6).

Зразок є радіоелектронним засобом і складається з двох компонентів:

системи електронної протидії – EDM4S (код НАТО 5865-470009942);

приладу виявлення БпЛА – WINGMAN (код НАТО 5865-226297918).

Система електронної протидії EDM4S та прилад виявлення БпЛА WINGMAN уже прийнято на озброєння в Литві, Латвії, Фінляндії, Молдові. Зразок призначений для виявлення та протидії безпілотників мультироторного типу. Він дозволяє виявляти та протидіяти БпЛА, перешкоджаючи сигналам телеметрії та передачі даних, керування і навігації.

Система електронної протидії EDM4S є портативним, повністю автономним приладом. Його вага – 5,5 кг. Тривалість безперервної роботи під час радіоелектронного подавлення – не менше 45 хв. Ефективна дальність радіоелектронного подавлення (за відсутності атмосферних опадів, електромагнітних завад та в умовах прямої видимості) становить не меншу 3 км. Робочі діапазони: 1,5 ГГц (GPS); 1,5 ГГц (GLONASS); 2,4 ГГц; 5,8 ГГц. Ступінь захисту приладу згідно з ГОСТ14254-96 – IP54. Додатково можливе комплектування коліматорним та оптичним прицілами (рис. 7).

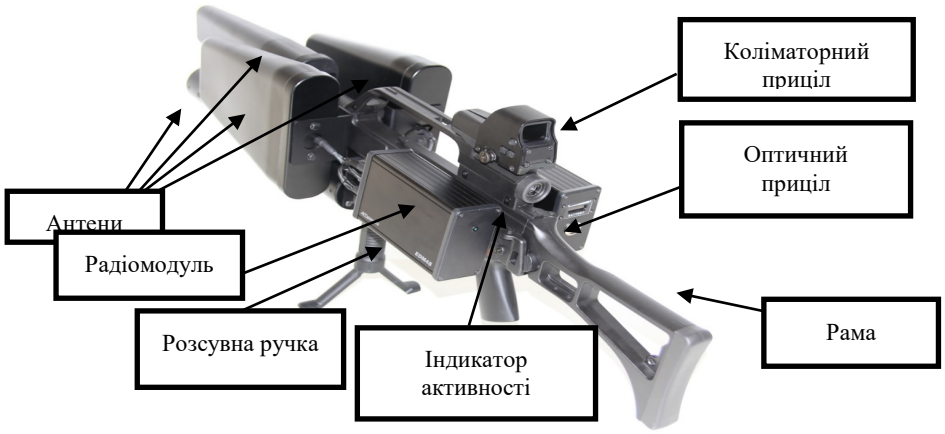


Рис. 7. Склад системи електронної протидії EDM4S

Прилад виявлення БпЛА WINGMAN є також портативним, повністю автономним. Час безперервної роботи в ході радіоелектронного подавлення – не менше 5 год. Ефективна дальність виявлення БпЛА мультироторного типу (за відсутності атмосферних

опадів, електромагнітних завад та в умовах прямої видимості) – не менше 3 км. Ступінь захисту (відповідно до ГОСТ14254-96) – IP67.

Цей комплекс для боротьби з БпЛА та дронами має направлену дію, блокує всі їх види, перекриває сигнали телеметрії, GPS-навігації та управління. Основний принцип цієї «гармати» – подавлення систем управління апарата електромагнітним випромінюванням. Майже вся подібна техніка керується оператором, а команди передаються радіоканалом. Отже, заглушення каналу управління засобами РЕБ у змозі як мінімум заважати виконанню завдання, а як максимум – знищити апарат після втрати керування.

Щоб не допустити «евакуації» БпЛА, засоби РЕБ повинні подавляти не тільки канал управління, а також сигнали навігаційної системи, якими користуються дрони.

У пристрій вмонтований блок, що в радіусі двох кілометрів заглушує сигнали супутникової навігації ГЛОНАСС й аналогічних закордонних систем. Також пристрій у змозі блокувати на відстані одного кілометра сигнали GSM, 3G, LTE та ставити перешкоди на частотах 900 МГц; 2,4 ГГц; 5,2–5,8 ГГц. При цьому дрон фізично не знищується, але втрачає зв’язок із пультом управління та приземляється.

За результатами кліматичних, електричних та механічних випробувань обидва прилади отримали позитивні оцінки.

Результати підконтрольної експлуатації комплексу EDM4S показали високу ефективність застосування в бойових умовах (на глибині ротних та взводних опорних пунктів першого рубежу оборони). Було зірвано виконання завдання для восьми БпЛА мультироторного типу противника як вдень, так і вночі, зокрема й БпЛА ударної дії.

Застосування комплексу здійснювалося як поза зоною візуального контролю БпЛА, так і під час візуального спостереження за БпЛА противника. Підтверджено, що під час його дії БпЛА противника стає некерованим, зупиняється, виконує зниження та приземлення в напрямку вітру. Після перших позитивних результатів застосування засобу спостерігалося різке скорочення виконання польотів ворожими БпЛА мультироторного типу.

Програма та методики визначальних відомчих випробувань дослідного зразка комплексу протидії БпЛА EDM4S виробництва компанії «NT Servic» була виконана в повному обсязі. Зразок випробування витримав. Побічного випромінювання на комплексі EDM4S операторам комплексу РЕБ з БпЛА «Буковель-АД» не спостерігалося.

У той же час подібний виріб має і низку недоліків. Так, у нього дуже обмежена дальність дії (лише в зоні прямого бачення цілі); низька «швидкострільність»: на нейтралізацію одного дрона може знадобиться декілька хвилин, за які він може виконати своє призначення, а в разі ударного варіанта це може бути критичним.

Зразок визнаний безпечним для використання в ЗС України та рекомендований для постачання на озброєння.

Висновки. У статті проаналізовано відомі способи протидії БпЛА противника. Не можна не відзначити, що всі вони припускають використання наявних систем та озброєнь. Отже, знищення або захоплення техніки противника з різною ймовірністю можливі вже за нинішнього розвитку озброєння та військової техніки. Підвищення ймовірності виконання подібних завдань залежатиме від характеристик нових систем і БпЛА, яким вони будуть протидіяти. Так чи інакше вже зараз зрозуміло, що подібні засоби протидії безпілотникам

можуть застосовуватися в разі потреби. Слід очікувати, що в майбутньому вони будуть тільки вдосконалюватися, підлаштовуючись під новинки в галузі створення БпЛА.

Незважаючи на те, що новітні технології протидії БпЛА постійно вдосконалюються, проте вже чітко визначено послідовність стадій цього процесу: виявити, розпізнати і знищити. Перші два елементи в цьому ланцюжку на даний момент здебільшого відпрацьовані за рахунок удосконалення наявних технологій. Результати проведення ООС (антитерористичної операції) на сході України свідчать, що БпЛА вдосконалюються як типова зброя диверсійно-терористичних війн. Сучасні воєнні конфлікти ведуться мобільними легкоозброєними підрозділами, які прагнуть завдати максимальної шкоди. Тому знаряддя протидії БпЛА повинні бути мобільними й компактними.

У цілому зауважимо, що застосування такої мобільної зброї цілком виправдане, наприклад, як засіб прикриття для взводного або ротного опорного пункту.

Однак найбільш радикальним засобом РЕБ з мультикоптерами та дронами експерти визнають подавлення їх бортової електроніки потужним мікрохвильовим випромінюванням, яке випалює електронні плати в приладах управління.

Пріоритетами в реалізації програм розробки сучасних вітчизняних засобів знищення БпЛА можна вважати використання засобів їх перехоплення або знищення за допомогою систем електронної протидії.

Отже, на сьогодні можна констатувати, що за останні кілька років в Україні відбулися суттєві зміни у сфері розробки та виробництва комплексів радіоелектронної протидії БпЛА. Створено низку різноманітних засобів, які дозволяють значно обмежити можливості використання російських безпілотників у повітряному просторі на сході нашої держави, що кардинальним чином впливатиме на хід подальших бойових дій.

Українським виробникам вдалося створити засоби, деякі з яких уже застосовуються за призначенням і можуть успішно конкурувати з аналогічними засобами на міжнародних ринках озброєння та військової техніки.

СПИСОК ЛІТЕРАТУРИ

1. Убийца беспилотников. На что способна украинская антидроновая винтовка. URL: https://www.dsnews.ua/politics/ubiytsa-bespilotnikov-na-chto-sposobna-ukrainskaya-antidronovaya-21022019220000 (дата обращения: 24.04.2020).
2. Переносной комплекс подавления БпЛА STUPOR. URL: https://topwar.ru/114758-perenosnoy-kompleks-podavleniya-bpla-stupor.html9 (дата обращения: 20.04.2020).
3. Системы борьбы с БпЛА «Гроза-С» и «Гроза-Р» (Беларусь). URL: https://topwar.ru/110000-sistemy-borby-s-bpla-groza-s-i-groza-r-belarus.html13 (дата обращения: 10.06.2020).
4. БпЛА и способы борьбы с ними. URL: https://swg54.livejournal.com/2619944.html (дата обращения: 24.04.2020).
5. Ловушка для дрона: как вывести из строя беспилотник. URL: https://rostec.ru/news/lovushka-dlya-drona-kak-vyvesti-iz-stroya-bespilotnik/ (дата обращения: 15.05.2020).
6. «Нелетальное противодействие»: как Россия совершенствует методы борьбы с БпЛА URL: https://russian.rt.com/russia/article/548902-borba-bespilotniki-voiska (дата обращения: 17.06.2020).

7. Застосування досвіду АТО для підготовки фахівців зв'язку РТЗ та ІС : навч. посіб. / А. М. Алімпієв, О. І. Кушнір, К. С. Васюта [та ін.]; М-во оборони України, Харків. ун-т Повітряних Сил ім. І. Кожедуба. Харків : ХУПС, 2016. 326 с. : іл., табл.
8. Лоринов А. Беспилотная воздушная разведка. Москва : Воениздат, 1997. 224 с.
9. Догерти М. Дж. Дроны. Первый иллюстрированый гид по беспилотникам. Москва : Эксмо, 2016. 224 с.

Подано 24.07.2020

REFERENCES

1. Ubiitsa bespilotnikov. Na chto sposobna ukrainskaia antidronovaia vintovka [The drone killer. What is the Ukrainian anti-drone rifle capable of]. (n.d.). Retrieved from https://www.dsnews.ua/politics/ubiytsa-bespilotnikov-na-chto-sposobna-ukrainskaya-antidronovaya-21022019220000 [in Russian].
2. Perenosnoi kompleks podavleniia BpLA STUPOR [STUPOR portable UAV suppression system]. Retrieved from https://topwar.ru/114758-perenosnoy-kompleks-podavleniya-bpla-stupor.html9 [in Russian].
3. Sistemy bor'by s BpLA «Groza-S» i «Groza-R» (Belarus') [Anti-UAV systems "Groza-S" and "Groza-R" (Belarus)]. (n.d.). Retrieved from https://topwar.ru/110000-sistemy-borby-s-bpla-groza-s-i-groza-r-belarus.html13 [in Russian].
4. BpLA i sposoby bor'by s nimi [UAVs and ways to combat them]. (n.d.). Retrieved from https://swg54.livejournal.com/2619944.html [in Russian].
5. Lovushka dlia drona: kak vyvesti iz stroia bespilotnik [Drone trap: how to disable a drone]. (n.d.). Retrieved from https://rostec.ru/news/lovushka-dlya-drona-kak-vyvesti-iz-stroya-bespilotnik/ [in Russian].
6. «Neletal'noe protivodeistvie»: kak Rossiia sovershenstvuet metody bor'by s BpLA ["Non-lethal counteraction": how Russia is improving methods of combating UAVs]. (n.d.). Retrieved from https://russian.rt.com/russia/article/548902-borba-bespilotniki-voiska [in Russian].
7. Alimpiiev, A. M., Kushnir, O. I., Vasiuta, K. S. et al. (2016). *Zastosuvannia dosvidu ATO dlia pidgotovki fakhivtsiv zv'iazku RTZ ta IS [Application of anti-terrorist operation experience for training of RTZ and IS communication specialists]*. Kharkiv: NAFU [in Ukrainian].
8. Lorinov, A. (1997). *Bespilotnaia vozdushnaia razvedka [Unmanned aerial reconnaissance]*. Moscow: Voenizdat [in Russian].
9. Dogerti, M. Dzh. (2016). *Drony. Pervyi illiustrirovanyi gid po bespilotnikam [Drones. The first illustrated drone guide]*.Moscow: Eksmo [in Russian].

R. M. Oliinyk, S. V. Tsilyna, O. V. Yermolenko, Y. M. Zhyvets

SYSTEMS OF RADIO-ELECTRONIC FIGHT AGAINST PILOTLESS VEHICLES MULTIROTOR TYPE IN DISTRICTS OF CONDUCT BATTLE ACTIONS

In modern warfare, the information component is crucial for both sides of the conflict. Donetsk and Luhansk regions have become a kind of bridgehead for testing and application in the operation of unmanned aerial vehicles of various dimensions and functional purposes, the most common of which are small reconnaissance unmanned aerial vehicles. Dozens of enemy vehicles are gathering information about the location of the Ukrainian military.

To date, no state is ready to withstand planned attacks by unmanned aerial vehicles. Traditional air defense weapons are designed for large and long-range targets, while the modern line of drones consists of nano-, micro- and mini-devices flying at low altitudes.

A comparative analysis of modern means of counteracting unmanned aerial vehicles and conclusions about the possibility of their use in the Armed Forces of Ukraine. The newest means of destruction of unmanned aerial vehicles of the leading countries of the world are considered. The issue of the possibility of blocking the work of enemy drones is covered in zones (areas) of hostilities. Ways to increase the effectiveness of small - scale unmanned aerial vehicles are proposed.

Priorities in the implementation of programs for the development of modern domestic means of destruction of unmanned aerial vehicles can be considered the use of means of interception or destruction by electronic countermeasures.

The relevance of the study lies in the analysis of the main available methods of control with unmanned aerial vehicles, development of perspective approaches and acquaintance with modern achievements and directions of development of means of struggle against drones applied by the enemy.

Keywords: *mobile facilities of radio electronic fight, facilities of elimination of pilotless aircrafts, reconnaissance unmanned aerial vehicle of multirotor type, drone.*

ISSN 2076-1546

УДК 629.7.067.8 DOI: 10.46972/2076-1546.2020.18.06

О. М. Перегуда, А. В. Родіонов, С. П. Самойлик

ПІДХІД ДО ПІДВИЩЕННЯ ЖИВУЧОСТІ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА І КЛАСУ В ОСОБЛИВИХ ВИПАДКАХ У ПОЛЬОТІ

У статті запропоновано підхід до підвищення живучості безпілотних літальних апаратів І класу в особливих випадках у польоті, який передбачає розроблення бортової інформаційної системи ідентифікації особливих випадків у польоті та синтезу керуючого впливу на літальний апарат за умови виникнення небезпечних факторів. У результаті аналізу основних тенденцій розвитку бортових систем управління безпілотними літальними апаратами виявлено, що провідними країнами світу приділяється значна увага до підвищення рівня їх інтелектуалізації. Це необхідно для забезпечення виконання складних завдань, які покладаються на сучасні безпілотні літальні апарати у військовій та цивільній сферах. Основними напрямками таких досліджень є виявлення проблематики групового застосування безпілотних літальних апаратів та розширення можливостей бортових систем управління щодо здійснення автоматичного підтримання значень певних параметрів за зміни умов виконання польоту. Для підвищення живучості безпілотного літального апарата І класу наведено обрис бортової інформаційної системи ідентифікації особливих випадків у польоті та синтезу керуючого впливу, описано функціональне призначення її складових. До складу цієї системи запропоновано включити підсистему ідентифікації особливих випадків у польоті і визначення рівня загрози безпілотному літальному апарату та підсистему синтезу керуючого впливу. Зазначено необхідність деталізації особливих випадків у польоті, визначених керівними документами у сфері діяльності державної авіації України, для безпілотних літальних апаратів І класу та запропоновано підхід до їх класифікації. Наведено бачення найближчих часткових наукових завдань та перелік очікуваних наукових результатів досліджень за даним напрямком.

Ключові слова: *безпілотний літальний апарат; бортова інформаційна система; небезпечні фактори; особливі випадки у польоті.*

Постановка проблеми в загальному вигляді. Досвід проведення антитерористичної операції на тимчасово окупованих територіях Луганської та Донецької областей та операції Об'єднаних сил (ООС) свідчить про застосування Збройними Силами України та іншими військовими формуваннями безпілотних авіаційних комплексів (БпАК) для виконання широкого спектра бойових та спеціальних завдань. Водночас створювані противником радіоперешкоди засобам радіозв'язку значно ускладнюють управління безпілотним літальним апаратом (БпЛА) І класу та виконання ним бойових завдань, несуть загрозу втрати літального апарата в цілому. У зв'язку з цим важливого значення набувають питання безпеки власних БпЛА в умовах радіоелектронної протидії (РЕП) з боку противника, адже для забезпечення їх застосування необхідне використання одного або кількох радіоканалів та приймання сигналів супутникових навігаційних систем (СНС), а саме їх приймальна апаратура є вразливою до РЕП. Крім цього, значного впливу на

політ БпЛА завдають метеорологічні умови, імовірними є також і відмови складових авіоніки. Ситуації, які виникають внаслідок впливу небезпечних факторів, відносять до особливих випадків у польоті (ОВП) [1]. Кожен із них характеризується певними параметрами (які вимагають подальшого детального аналізу), відтак їх можливо нейтралізувати за рахунок використання бортової інформаційної системи ідентифікації особливих випадків у польоті та синтезу керуючого впливу для підвищення живучості БпЛА, а також завдяки збільшенню ймовірності виконання цільової задачі. Прикладами ОВП, які можуть призвести до зриву виконання завдання або взагалі до втарти БпЛА, є РЕП (відмова) приймача супутникової навігаційної системи або обмерзання приймача повітряного тиску, які відбуваються за неможливості керування БпАК людиною-оператором. Тому наукове завдання з розроблення бортової інформаційної системи з ідентифіції та нейтралізації ОВП є актуальним.

Аналіз останніх досліджень і публікацій. Протягом останніх років спостерігається зростання світового ринку БпАК: відбувається збільшення обсягів виробництва, покращення їх тактико-технічних характеристик, розроблення та впровадження новітніх технологій [2, 3]. Різні за аеродинамічною схемою побудови, призначенням, характеристиками БпАК широко застосовуються як у військовій справі, так і в цивільній сфері, причому перелік завдань, покладених на них, постійно розширюється. Спостерігається тенденція до проведення провідними країнами світу наукових досліджень та випробувань перспективних розробок, спрямованих на групове застосування, розширення можливостей автоматичного керування (у тому числі з впровадженням елементів штучного інтелекту) БпЛА під час виконання специфічних завдань [4–6].

Груповому застосуванню БпЛА присвячено низку наукових праць як оглядового [7–9], так і дослідницького характеру, у яких розглядається конкретна проблематика в цій сфері [10, 11].

Серед підходів до розширення можливостей автоматичного керування з використанням елементів штучного інтелекту основними напрямками є: удосконалення автоматичного управління на певних етапах польоту [12, 13]; розроблення теоретичних основ машинного зору [14, 15]; дослідження у сфері сенсорних мереж та мереж зв'язку [16, 17]; навігація БпЛА з використанням візуальних орієнтирів та додаткових засобів [18, 19]; уникнення зіткнення БпЛА з перешкодами [20, 21]; моделювання в спеціалізованих програмних середовищах процесів, пов'язаних з БпЛА та управлінням ними [14, 15]. Концептуально питання інтелектуалізації систем управління БпЛА розглянуто в [22].

Значущим є факт систематичного проведення в РФ, починаючи з 2016 року, у м. Коломна на базі 924 Державного центру безпілотної авіації Міністерства оборони щорічної науково-практичної конференції "Перспективи розвитку і застосування комплексів із БпЛА". На даному заході серед інших обговорюються також питання щодо інтелектуалізації БпЛА, причому матеріали конференцій від 2018 року й дотепер у відкритих джерелах відсутні. Цікавим також є проведення з 2014 року семінару "Безпілотні транспортні засоби з елементами штучного інтелекту", під час якого основними є питання інтелектуалізації.

Результати проаналізованих наукових робіт реалізувати практично на наявних польотних контролерах неможливо, тому розширення переліку виконуваних функцій та забезпечення безпеки польотів у повітряному просторі вимагають ускладнення бортової апаратури.

Аналіз останніх досліджень і публікацій показав, що в наукових працях відсутній комплексний підхід до аналізу поточного стану та умов польоту БпЛА для ідентифікації впливу небезпечних факторів і синтезу відповідного алгоритму (стратегії) управління.

Формулювання завдання дослідження. Метою статті є сформувати обрис перспективної бортової інформаційної системи ідентифікації ОВП та синтезу керуючого впливу для підвищення живучості БпЛА І класу.

Виклад основного матеріалу. Наведений в [1] узагальнений перелік ситуацій, які належать до ОВП, не в повній мірі відображає особливості застосування, побудови та керування таких повітряних суден, як БпЛА І класу, тому для досягнення цілей роботи потребує адаптації, а саме: конкретизації (відповідно до визначення ОВП) ситуацій, характерних для БпЛА І класу; визначення причин їх виникнення – одного або комбінацій кількох небезпечних факторів; аналізу можливих наслідків.

Крім цього, для проведення детального аналізу параметрів польоту, які потребують контролю необхідна класифікація ОВП та їх комбінацій. Тому пропонуємо ОВП класифікувати за джерелом небезпечних факторів відносно БпЛА на зовнішні та внутрішні, а за походженням (своєю природою) – на природні та техногенні.

Внутрішні ОВП, спричинені внутрішніми небезпечними факторами, пов'язані з надійністю роботи бортових систем, у першу чергу польотного контролера та аеродинамічних органів управління. Їх ідентифікація потребує оцінювання стану БпЛА як технічної системи.

Зовнішні природні ОВП пов’язані з метеорологічними умовами виконання польотів та їх мінливістю: збільшенням швидкості вітру та зміною його напрямку, обмерзанням аеродинамічних органів управління та приймача повітряного тиску. Їх виявлення потребує контролю значень та аналізу змін метеорологічних елементів з відповідних датчиків та / або інших параметрів польоту, які з ними пов’язані, а також проведення на борту БпЛА елементів штурманських розрахунків. Водночас такі ОВП виникають відповідно до загальних законів авіаційної метеорології, їх вплив та можливі наслідки можна прорахувати.

Зовнішні техногенні фактори для БпЛА, які застосовуються у військовій сфері, носять навмисний характер, тому є найбільш небезпечними. Виходячи з аналізу бойового досвіду та реалій застосування БпАК підрозділами Збройних Сил (ЗС) України в ООС, слід зауважити, що РЕП спрямована на унеможливлення керування зовнішнім пілотом (оператором), перешкоджання точному визначенню місцезнаходження БпЛА шляхом встановлення завад чи спотворення сигналів СНС (так званий "спуфінг").

Проблематика застосування БпЛА в умовах РЕП є дуже актуальною: у багатьох відкритих джерелах повідомляється про розробку в провідних країнах світу як військових, так і комерційних апаратних засобів постановки радіоперешкод, призначених саме для протидії БпЛА в рамках заходів забезпечення безпеки об'єктів критичної інфраструктури, населення, виконання інших завдань. У [23] наведено досить детальний опис комплексу "Шиповник Аэро" та станції радіоелектронної боротьби "Красуха-4" із акцентуванням можливості даних засобів протидіяти саме БпЛА.

Можливість подавлення сигналів СНС, зокрема застосування перешкод, які повторюють структуру супутникового навігаційного повідомлення, досліджувалася в працях [15, 24, 25].

Також імовірним є виникнення небезпечних для БпЛА І класу факторів унаслідок помилки зовнішнього пілота (оператора), але питання визначення умов та критерію для втручання бортової системи в дії людини потребує додаткових наукових досліджень.

Польотні контролери БпЛА І класу, наявні в ЗС України, мають обмежені можливості щодо управління польотом в особливих випадках. Вони лише забезпечують повернення БпЛА до точки старту за відсутності зв'язку з пунктом дистанційного пілотування (ПДП) в одному або кількох радіоканалах управління (залежно від налаштувань) або в разі зниження напруги бортової акумуляторної батареї (для БпЛА, оснащених електричним двигуном) до певного значення, запрограмованого виробником. При цьому можливе зниження безпілотника з робочої висоти. Якщо після повернення в район запуску зв'язок БпЛА з ПДП не відновлено і керування зовнішнім пілотом (оператором) неможливе, то апарат здійснює некеровану посадку після виснаження бортової батареї. Водночас літальний апарат зі складу БпАК Fly Eye (WB Electronics, Республіка Польща) виконує більш складний алгоритм для відновлення зв'язку, а саме: повертається в останню точку, у якій спостерігався зв'язок; перебуває в ній визначений період часу; збільшує поточну висоту польоту на 100 метрів і після повторного очікування повертається в район запуску.

Літальний апарат зі складу БпАК Orbiter 2b (Aeronautics, Держава Ізраїль) навіть без керування людиною оцінює напрямок та швидкість вітру в районі точки посадки та здійснює маневри з урахуванням поточних значень метеоумов.

Виникнення деяких ОВП або їх певних комбінацій за відсутності в людини-оператора можливості здійснювати керування через подавлення каналів управління може спричинити втрату БпЛА на території противника, що призводить до викриття факту ведення повітряної розвідки, невиконання бойових завдань, зниження рівня укомплектованості та боєготовності підрозділу БпАК, завдає збитків державі, створює для противника інформаційний прецедент та зменшує мотивацію зовнішніх пілотів (операторів) до подальшого якісного виконання своїх обов'язків.

Під підвищенням живучості будемо розуміти виявлення умов, за яких керування БпЛА зовнішнім пілотом (оператором) не можливе, а спроможностей польотного контролера недостатньо для уникнення втрати або пошкодження БпЛА та здійснення функцій автоматичного управління для продовження виконання цільового завдання та збереження авіаційної техніки, що пропонується реалізувати шляхом створення відповідної системи.

Автори вбачають два основні шляхи підвищення рівня інтелектуалізації вітчизняних БпЛА. Один з них – розробка польотного контролера із заздалегідь передбаченими інтелектуальними функціями та відповідним програмним забезпеченням. Перевагами цього способу є можливість на початкових етапах розробки закласти в польотний контролер результати багатьох наукових напрацювань, що забезпечить якісно новий рівень ефективності виконання завдань БпЛА. Його недоліком є необхідність виконання великого обсягу робіт та, відповідно, значна тривалість і висока вартість їх виконання. Більш доцільним є спосіб розробки "надбудови" над польотним контролером як додаткового елемента авіоніки, на який будуть покладені завдання щодо реалізації додаткових функцій, не притаманних базовим польотним контролерам. Можливості такої реалізації сприяє той факт, що вітчизняні БпЛА І класу підрозділів ЗС України побудовані на базі одного сімейства вільно доступних польотних контролерів.

На рис. 1 запропоновано обрис перспективної бортової інформаційної системи ідентифікації ОВП та синтезу керуючого впливу для підвищення живучості БпЛА І класу.

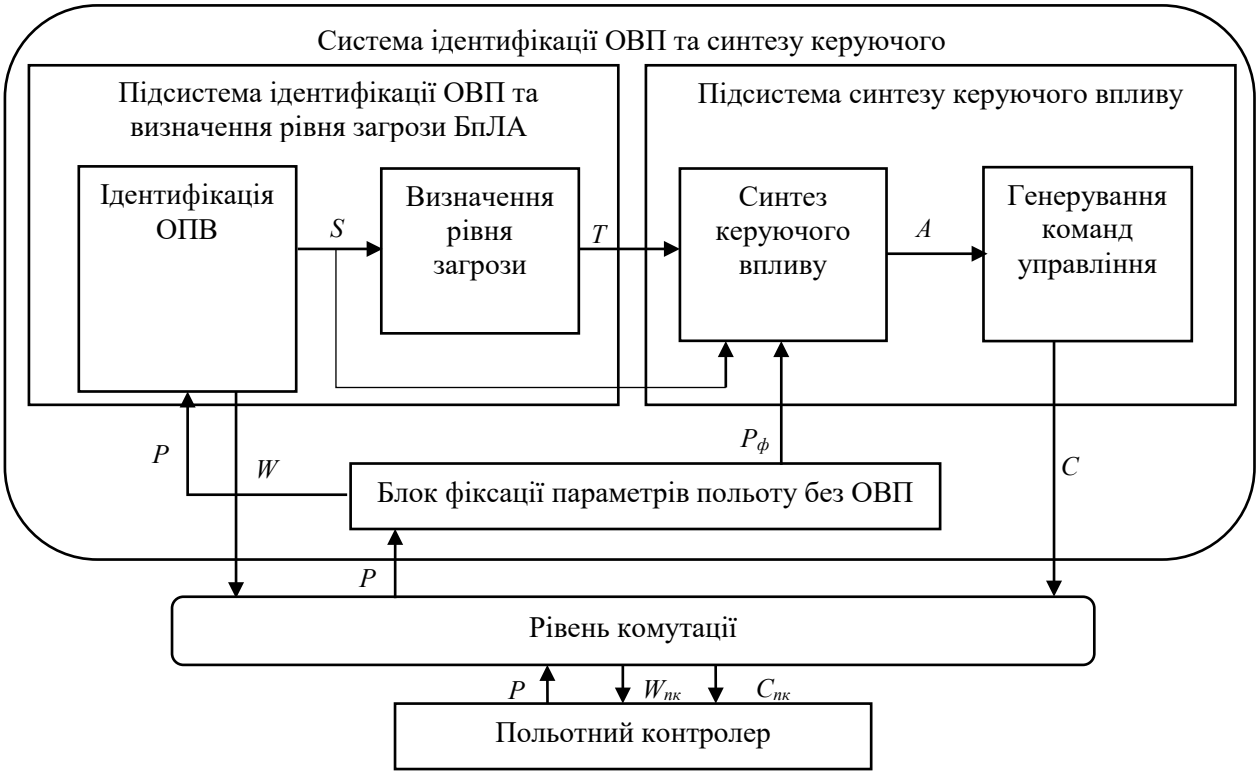


Рис. 1. Функціональна структура перспективної бортової інформаційної системи ідентифікації ОВП та синтезу керуючого впливу

Рівень комутації забезпечує інтерфейс між польотним контролером та елементами бортової інформаційної системи для передачі визначених параметрів *P*, які підлягають контролю, а також для передачі на польотний контролер повідомлень для зовнішнього пілота (оператора) $W_{пк}$, згенерованих команд $C_{пк}$ відповідно до результатів синтезу керуючого впливу. Повідомлення $W_{пк}$ передаються на пункт дистанційного пілотування для сповіщення членів зовнішнього екіпажу. Відповідно до згенерованих команд $C_{пк}$ польотний контролер здійснює управління аеродинамічними органами управління для виконання маневрів БпЛА.

У складі зазначеної системи передбачається:

блок фіксації параметрів польоту без ОВП, призначений для запам'ятовування (кешування) поточних параметрів польоту до настання особливих умов. Зафіксовані значення передаються в блок синтезу керуючого впливу для інформації про останню надійну "точку відліку";

підсистема ідентифікації ОВП та визначення рівня загрози БпЛА, що здійснює аналіз змін контрольованих параметрів *P*, формування сигналу *S* (залежно від характеру ОВП) для визначення рівня загрози БпЛА (позначимо рівень загрози *T*) відповідно до закладених у неї алгоритмів. У випадку виявлення ОВП підсистема також генерує повідомлення *W*, яке на рівні комутації перетворюється в необхідний для польотного контролера формат $W_{пк}$ і передається на ПДП бортовими засобами зв'язку БпЛА;

підсистема синтезу керуючого впливу, яка, отримуючи сигнали про характер ОВП (*S*), рівень загрози БпЛА (*T*) та параметри польоту до настання ОВП ($P_ф$), здійснює синтез

керуючого впливу A, який є алгоритмом управління, та відповідно до нього генерування набору команд управління. Ці команди через рівень комутації перетворюються в необхідний для польотного контролера формат $C_{пк}$.

Найближчими частковими науковими завданнями автори розглядають:

визначення повного переліку характерних БпЛА І класу ОВП, які підлягають ідентифікації; встановлення параметрів польоту, значення або зміни яких характеризують кожний ОВП;

аналіз підходів до розпізнавання поточного стану технічних систем, вибір науково-методичного апарату, придатного до використання, з урахуванням специфіки БпЛА та описаного завдання;

аналіз підходів та вибір науково-методичного апарату для синтезу керуючого впливу з урахуванням поточного стану БпЛА.

Передбачуваними науковими результатами є: метод ідентифікації особливих випадків у польоті БпЛА І класу; метод синтезу керуючого впливу на БпЛА І класу в ОВП; сукупність алгоритмів з описом їх логіки та способом формування результатів розв'язання завдань щодо управління БпЛА І класу в ОВП.

Висновки. Одним із шляхів підвищення живучості БпЛА І класу з урахуванням умов їх застосування за досвідом бойових дій є розроблення перспективної бортової інформаційної системи ідентифікації ОВП та синтезу керуючого впливу, обрис якої запропоновано в статті. Очікуваним результатом впровадження запропонованої системи є зменшення кількості втрачених БпЛА І класу внаслідок впливу небезпечних факторів різної природи, зокрема й від впливу засобів радіоелектронної боротьби противника.

СПИСОК ЛІТЕРАТУРИ

1. Правила польотів державної авіації в повітряному просторі України : наказ Міністерства оборони України від 09.12.2015 № 700. URL: https://zakon.rada.gov.ua/laws/show/z1622-15 (дата звернення: 13.11.2020).
2. Commercial Drones Market Statistics 2022: Major Factors that can Increase the Global Demand URL: https://apnews.com/press-release/wired-release/80ff63e46e1fc2bcec43cf76af/2960eb (last accessed: 12.12.2020).
3. Commercial Drones Market by Type (Fixed wing drones, Rotary bade drones, Hybrid drones segment), Application (Agriculture and Environment, Media and Entertainment, Energy, Government, Construction & Archaeology) – Global Opportunity Analysis and Industry Forecast, 2014–2022. URL: https://www.alliedmarketresearch.com/commercial-drone-market (last accessed: 15.12.2020).
4. Chinese helicopter drones capable of intelligent swarm attacks. URL: http://eng.chinamil.com.cn/view/2019-05/10/content_9500318.htm (last accessed: 15.11.2020).
5. OFFensive Swarm-Enabled Tactics (OFFSET). URL: https://www.darpa.mil/program/offensive-swarm-enabled-tactics (last accessed: 15.11.2020).
6. Department of Defense Announces Successful Micro-Drone Demonstration. URL: https://www.defense.gov/Newsroom/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration (last accessed: 10.12.2020).
7. Мартинюк О. Р., Мурасов Р. К. Огляд концепцій групового застосування безпілотних літальних апаратів // Сучасні інформаційні технології у сфері безпеки та оборони. 2013. № 2. С. 90–92.

8. Основні тенденції створення та застосування груп безпілотних літальних апаратів / Лупандін В. А., Мегельбей Г. В., Мацько О. Й. та ін. // Наука і техніка Повітряних Сил Збройних Сил України. 2019. № 2. С. 88–96.
9. Перспективи та особливості групового використання безпілотних літальних апаратів / Бондар С. О., Кожохіна О. В., Боровик В. О. та ін. // Управляющие системы и машины. 2018. № 5. С. 25–37.
10. Пулеко І. В. Проблеми управління угрупованням малих безпілотних літальних апаратів з позицій теорії робототехнічних систем // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ ДУТ, 2015. Вип. 11. С. 106–114.
11. Бондарєв Д. І., Кучеров Д. П., Шмельова Т. Ф. Оптимізація структури групового польоту безпілотних літальних апаратів // Зб. наук. праць Харків. ун-ту Повітряних Сил. 2016. № 3 (48). С. 61–66.
12. Burnashev V. V. Automatic steering algorithms of the airplane short-cut touchdown // Інформаційні системи, механіка та керування. Київ : "ЕКМО", 2010. Вип. 5. С. 136–144.
13. Intelligent Control for Unmanned Aerial Systems with System Uncertainties and Disturbances Using Artificial Neural Network. URL: https://www.mdpi.com/2504-446X/2/3/30/htm (last accessed: 10.12.2020).
14. Второй Всероссийский научно-практический семинар «Беспилотные транспортные средства с элементами искусственного интеллекта (БТС-ИИ-2015)» : Труды семинара (9 октября 2015 г.). Санкт-Петербург : «Политехника-сервис», 2015. 140 с.
15. Перспективы развития и применения комплексов с беспилотными летательными аппаратами : Сб. докладов и статей по материалам науч.-практич. конф. Коломна : 924 ГЦ БпА МО РФ, 2016. 278 с.
16. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Теоретические и практические направления исследований в области летающих сенсорных сетей // Электросвязь. 2015. № 7. С. 9–11.
17. Воротніков В. В., Гуменюк І. В. Метод планування польотних операцій безпілотних літальних апаратів для забезпечення зв'язаності вузлів безпровідної мережі // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2017. Вип. 14. С. 62–68.
18. Застосування бортових радіопеленгаційних засобів у навігаційних системах малих безпілотних літальних апаратів / Шпилька О. О., Мирончук О. Ю., Ткач А. О. та ін. // Військово-технічний збірник. 2016. № 15. С. 48–53.
19. How Microsoft Uses Transfer Learning to Train Autonomous Drones. URL: https://medium.com/swlh/how-microsoft-uses-transfer-learning-to-train-autonomous-drones-f5cd745f6e26 (last accessed: 24.12.2020).
20. Learning Visuomotor Policies for Aerial Navigation Using Cross-Modal Representations. URL: https://arxiv.org/abs/1909.06993 (last accessed: 11.12.2020).
21. Obstacle Detection and Avoidance System Based on Monocular Camera and Size Expansion Algorithm for UAVs. URL: https://www.mdpi.com/1424-8220/17/5/1061/htm (last accessed: 11.12.2020). https://doi.org/10.3390/s17051061
22. Гриценко В. І., Волков О. Є., Комар М. М., Богачук Ю. П. Інтелектуалізація сучасних систем автоматичного керування безпілотними літальними апаратами // Кибернетика и вычислительная техника. 2018. № 1. С. 45–59.
23. Ясечко М. Н., Очкуренко А. В. , Ковальчук А. А. , Максюта Д. В. Современные радиотехнические средства борьбы с беспилотными летательными аппаратами в зоне

проведения АТО // Зб. наук. праць Харків. ун-ту Повітряних Сил. 2015. Вип. 3. С. 54–57.
24. Герасименко К. В. Моделі навмисних перешкод сигналам супутникових радіонавігаційних систем // Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 4. С. 79–81.
25. Кащеев А. А., Кошелев В. И. Оценка эффективности подавления сигналов спутниковых радионавигационных систем преднамеренными помехами // Журнал радиоэлектроники. 2012. № 7. С. 1–12.

Подано 24.12.2020

REFERENCES

1. Pravyla polotiv derzhavnoi aviatsii v povitrianomu prostori Ukrainy : nakaz Ministerstva oborony Ukrainy vid 09.12.2015 № 700 [Rules of state aviation flighs in the airspace of Ukraine: Ministry of Defence of Ukraine order from 09.12.2015 № 700.]. (2015). Retrieved from https://zakon.rada.gov.ua/laws/show/z1622-15 [in Ukrainian].
2. Commercial Drones Market Statistics 2022: Major Factors that can Increase the Global Demand. (n.d.). Retrieved from https://apnews.com/press-release/wired-release/80ff63e46e1fc2bcec43cf76af/2960eb.
3. Commercial Drones Market by Type (Fixed wing drones, Rotary bade drones, Hybrid drones segment), Application (Agriculture and Environment, Media and Entertainment, Energy, Government, Construction & Archaeology) – Global Opportunity Analysis and Industry Forecast, 2014–2022. (n.d.). Retrieved from https://www.alliedmarketresearch.com/commercial-drone-market.
4. Chinese helicopter drones capable of intelligent swarm attacks. (n.d.). Retrieved from http://eng.chinamil.com.cn/view/2019-05/10/content_9500318.htm.
5. OFFensive Swarm-Enabled Tactics (OFFSET). (n.d.). Retrieved from https://www.darpa.mil/program/offensive-swarm-enabled-tactics.
6. Department of Defense Announces Successful Micro-Drone Demonstration. (n.d.). Retrieved from https://www.defense.gov/Newsroom/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration.
7. Martyniuk, O. R., & Murasov, R. K. (2013). Ohliad kontseptsii hrupovoho zastosuvannia bezpilotnykh litalnykh aparativ [Review of concepts of unmanned aerial vehicles group application]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony [Modern Information Technologies in the Sphere of Security and Defence], 2,* 90–92 [in Ukrainian].
8. Lupandin, V. A., Mehelbei, H. V., Matsko, O. Y., Kurtseitov, T. L., & Mironenko, P. O. (2019). Osnovni tendentsii stvorennia ta zastosuvannia hrup bezpilotnykh litalnykh aparativ [Major trends of the development and application of a unmanned aerial vehicle groups]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy [Science and Technology of the Air Force of Ukraine], 2,* 88–96 [in Ukrainian].
9. Bondar, S. O., Kozhokhina, O. V., Borovyk, V. O., Linder, Ya. M., & Korshunov, M. V. (2018). Perspektyvy ta osoblyvosti hrupovoho vykorystannia bezpilotnykh litalnykh aparativ [Groups of unmanned aerial vehicles usage perspectives and peculiarities]. *Upravliaiushchye systemy y mashyny [Control systems and computers], 5,* 25–37 [in Ukrainian].
10. Puleko, I. V. (2015). Problemy upravlinnia uhrupovanniam malykh bezpilotnykh litalnykh aparativ z pozytsii teorii robototekhnichnykh system [Problems of group control by small unmanned aerial vehicles on theory robotic 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], 11, 106–114. Zhytomyr: ZhMI DUT [in Ukrainian].

11. Bondariev, D. I., Kucherov, D. P., & Shmelova, T. F. (2016). Optymizatsiia struktury hrupovoho polotu bezpilotnykh litalnykh aparativ [Modelling of group flights of unmanned aerial vehicles using graph theory]. *Zb. nauk. prats Kharkiv. un-tu Povitrianykh Syl [Scientific works of Kharkiv National Air Force University], 3* (48), 61–66 [in Ukrainian].
12. Burnashev, V. V. (2010). Automatic steering algorithms of the airplane short-cut touchdown. *Informatsiini systemy, mekhanika ta keruvannia [Information systems, mechanics and control], 5,* 136–144. Kyiv: "EKMO".
13. Intelligent Control for Unmanned Aerial Systems with System Uncertainties and Disturbances Using Artificial Neural Network. (n.d.). Retrieved from https://www.mdpi.com/2504-446X/2/3/30/htm.
14. *Vtoroi Vserossyiskyi nauchno-praktycheskyi semynar «Bespylotnye transportnye sredstva s elementamy yskusstvennoho yntellekta (BTS-YY-2015)» [Second All-Russian Scientific and Practical Seminar "Unmanned Vehicles with Elements of Artificial Intelligence"].* (October 9, 2015). Saint Petersburg [in Russian].
15. *Perspektyvy razvytyia y prymenenyia kompleksov s bespylotnymy letatelnymy apparatamy : Sb. dokladov y statei po materyalam nauch.-praktych. konf. [Perspectives for the development and application of complexes with unmanned aerial vehicles: Collection of thesis and articles on the materials of the scientific-practical conference].* (2016). Kolomna [in Russian].
16. Kucheriavyi, A. E., Vladyko, A. H., & Kyrychek, R. V. (2015). Teoretycheskye y praktycheskye napravlenyia yssledovanyi v oblasty letaiushchykh sensornykh setei [Theoretical and practical ways of researches in the sphere of flying sensor networks]. *Elektrosviaz [Telecommunication], 7,* 9–11 [in Russian].
17. Vorotnikov, V. V., & Humeniuk, I. V. (2017). Metod planuvannia polotnykh operatsii bezpilotnykh litalnykh aparativ dlia zabezpechennia zv'iazanosti vuzliv bezprovidnoi merezhi [Unmanned aerial vehicles flight operations planning method to ensure connectivity of wireless network nodes]. *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], 14,* 62–68. Zhytomyr: ZhMI [in Ukrainian].
18. Shpylka, O. O., Myronchuk, O. Yu., & Tkach, A. O., et al. (2016). Zastosuvannia bortovykh radiopelenhatsiinykh zasobiv u navihatsiinykh systemakh malykh bezpilotnykh litalnykh aparativ [The application of the on-board devices radio direction-finding in the navigation systems of drones]. *Viiskovo-tekhnichnyi zbirnyk [Military Technical Collection], 15,* 48–53 [in Ukrainian].
19. How Microsoft Uses Transfer Learning to Train Autonomous Drones. (n.d.). Retrieved from https://medium.com/swlh/how-microsoft-uses-transfer-learning-to-train-autonomous-drones-/f5cd745f6e26.
20. Learning Visuomotor Policies for Aerial Navigation Using Cross-Modal Representations. (n.d.). Retrieved from https://arxiv.org/abs/1909.06993.
21. Obstacle Detection and Avoidance System Based on Monocular Camera and Size Expansion Algorithm for UAVs. (n.d.). Retrieved from https://www.mdpi.com/1424-8220/17/5/1061/htm. https://doi.org/10.3390/s17051061
22. Hrytsenko, V. I., Volkov, O. Ye., Komar, M. M., & Bohachuk, Yu. P. (2018). Intelektualizatsiia suchasnykh system avtomatychnoho keruvannia bezpilotnymy litalnymy

aparatamy [Intellectualization of modern systems of automatic control of unmanned aerial vehicles]. *Kibernetika i vychislitel'naia tekhnika [Cybernetics and computer engineering], 1,* 45–59 [in Ukrainian].
23. Yasechko, M. N., Ochkurenko, A. V. , Kovalchuk, A. A. , & Maksiuta, D. V. (2015). Sovremennye radyotekhnycheskye sredstva borby s bespylotnymy letatelnymy apparatamy v zone provedenyia ATO [Modern electronic means of dealing with unmanned aircraft in the zone of the ATO]. *Zb. nauk. prats Kharkiv. un-tu Povitrianykh Syl [Scientific works of Kharkiv National Air Force University], 3,* 54–57 [in Russian].
24. Herasymenko, K. V. (2015). Modeli navmysnykh pereshkod syhnalam suputnykovykh radionavihatsiinykh system [Models jamming signals of satellite radio navigation systems]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy [Science and Technology of the Air Force of Ukraine], 4,* 79–81 [in Ukrainian].
25. Kashcheev, A. A., & Koshelev, V. Y. (2012). Otsenka effektyvnosty podavlenyia syhnalov sputnykovykh radyonavyhatsyonnykh system prednamerennymy pomekhamy [Estimation of efficiency of the suppression of signal satellite radionavigation systems with structured and noise hindrance]. *Zhurnal radyoelektronyky [Journal of Radio Electronics], 7,* 1–12 [in Russian].

O. M. Pereguda, A. V. Rodionov, S. P. Samoilyk

APPROACH TO INCREASING THE SURVIVABILITY OF CLASS I UNMANNED AERIAL VEHICLE IN EMERGENCY OPERATIONS

The article proposes an approach to increasing the survivability of class I unmanned aerial vehicles in emergency operations which involves development of an onboard information system for identifying emergency occasions in flight and the synthesis of a control action on the unmanned aircraft in case of hazardous factors influence. As the result of the analysis of the main trends in the development of unmanned aerial vehicles onboard control systems, it was found that the leading countries are paying significant attention to increasing their intellectualization level. This is necessary to ensure the fulfilment of complex tasks that are assigned to modern unmanned aerial vehicles in the military and civilian spheres. The main directions of such researches are identifying the problem of swarm application of unmanned aerial vehicles and expanding the capabilities of onboard control systems maintain automatically the values of certain parameters when the flight conditions changes. As the approach to increasing the survivability of a class I unmanned aerial vehicle, a vision of an onboard information system for identifying emergency occasions in flight and synthesis of control action is proposed, the functional purpose of its components is described. It is suggested that this system will be comprised of a subsystem for identifying emergency cases in flight and determining the class I unmanned aerial vehicle threat level and a subsystem for synthesizing control action. Governing documents and regulations for the state aviation of Ukraine determines the list of aircraft emergency occasions. Article mentions the necessity of detailing emergency occasions in flight, which are typical for class I unmanned aerial vehicles and an approach to their classification is proposed. A vision of the nearest partial scientific tasks and a list of expected scientific results of research in this direction are given.

Keywords*: unmanned aerial vehicle; onboard information system; hazardous factors; emergency occasions in flight.*

ISSN 2076-1546

УДК 681.518 DOI: 10.46972/2076-1546.2020.18.07

В. С. Шевченко, Р. В. Нетребко, А. І. Нетребко, І. В. Зімчук

РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВИБОРУ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ НА ЕТАПІ ОЦІНЮВАННЯ ОБСТАНОВКИ

У статті показано хід реалізації програмного забезпечення вибору засобів радіоелектронної розвідки на етапі оцінювання обстановки на основі проведених авторами теоретичних досліджень. Вказано, на підставі яких нормативних документів оцінюють обстановку з вибором засобів радіоелектронної розвідки, з яких етапів складається цей процес, що потрібно для вибору даних засобів.

Здійснено проєктування інформаційних потоків роботи програми щодо вибору засобів радіоелектронної розвідки на етапі оцінювання обстановки за допомогою діаграм Data Flow Diagram, розроблено відповідний алгоритм. Побудовано загальну блок-схему алгоритму роботи програмного забезпечення вибору засобів радіоелектронної розвідки на етапі оцінювання обстановки. На основі проведених досліджень розроблено базу даних для збереження переліку засобів радіоелектронної розвідки. Реалізовано прототип програмного забезпечення вибору засобів радіоелектронної розвідки на етапі оцінювання обстановки та наведено приклади роботи кожного з основних блоків у вигляді скріншотів, попередньо спроєктованих у діаграмах та блок-схемах алгоритмів. Окреслено основні етапи роботи запропонованого програмного забезпечення. Визначено переваги та недоліки розробленого програмного забезпечення вибору засобів радіоелектронної розвідки на етапі оцінювання обстановки. Вказано подальші кроки дослідження та удосконалення програми вибору засобів радіоелектронної розвідки на етапі оцінювання обстановки та нанесення її на мапу, а також покращення інтерфейсу.

Ключові слова: *радіоелектронна розвідка; оцінка обстановки; засоби радіоелектронної розвідки; радіоелектронна обстановка; етапи проєктування; програмне забезпечення; алгоритм; антитерористична операція; радіоелектронні засоби; тактико-технічні характеристики; база даних; діаграма потоків даних.*

Постановка проблеми в загальному вигляді. Успіх бою завжди залежав від якості оцінки обстановки. Уміле керівництво підрозділами й частинами сприяло розгрому противника з найменшими втратами та здобуттю перемоги за короткий час. У сучасних умовах стан і розвиток оцінювання обстановки визначають як один із найважливіших показників бойової міці й бойової готовності Збройних Сил, рівня їх організаційної та технічної досконалості [1].

Останнім часом значно розширилися можливості для поліпшення оцінювання обстановки. Глибоке знання законів війни, усебічне врахування їх дій та форм виявлення в конкретних умовах дають змогу правильно визначати основні, найбільш істотні тенденції розвитку військової справи, правильно оцінювати обстановку, передбачати її можливі зміни, приймати найбільш доцільні рішення. Передусім це пов’язано з інтенсивним розвитком науки управління, електронної обчислювальної техніки та засобів зв'язку. Докорінні зміни в засобах і способах ведення бойових дій зумовлюють різке підвищення вимог до оцінювання обстановки. Шляхи досягнення цього різні:

покращення організаційної структури систем управління, розвиток та впровадження високоефективних технічних засобів управління, удосконалення організаційних форм і методів роботи штабів, покращення підготовки кадрів для органів управління [2].

Використання програмного забезпечення вибору засобів радіоелектронної розвідки (РЕР) на етапі оцінювання обстановки є досить актуальним. Це дає змогу аналізувати роботу відповідних засобів, робити запити, здійснювати вибірку та розрахунок, передивлятися детальну інформацію будь-якого засобу РЕР, відфільтровувати їх, надавати можливість вибирати одиниці виміру та виводити засоби з їхніми характеристиками на друк. Завдяки цьому можна передбачити розвиток подій і тим самим значною мірою забезпечити успішне виконання поставлених завдань.

Аналіз останніх досліджень і публікацій. Збройна боротьба підкоряється об'єктивним законам розвитку і безупинно змінюється, що стосується як форм, так і засобів. Пошук ефективних з них є постійним завданням тактики. Значну допомогу командирам і штабам об'єднань Збройних Сил та Повітряних Сил надає використання математичних моделей та систем імітаційного моделювання в ході планування діяльності угруповань, дослідження закономірностей форм і способів діяльності Збройних Сил [3].

Аналіз застосування РЕР у ході виконання завдань антитерористичної операції (АТО) показав, що поряд із викоританням сучасних розробок у галузі навігаційних систем, супутникових радіонавігаційних систем актуальними залишаються питання навігації, швидкого й оптимального вибору засобів РЕР на етапі оцінювання обстановки. Окреслені проблеми розглядалися в працях Пічугіна М. Ф., Бондаренка Ю. Л., Бойка І. Л., Левченка О. В. тощо.

Під радіоелектронною обстановкою (РЕО) розуміють чинники й умови, у яких функціонують радіоелектронні засоби (РЕЗ), а також складову тактичної, оперативної та стратегічної обстановки. Оцінка РЕО дозволяє своєчасно вжити заходи, що забезпечать розвідзахищеність і стійкість функціонування РЕЗ своїх сил і виключити їх взаємний перешкоджальний вплив [4]. На сьогодні є декілька моделей, реалізованих на персональній електронно-обчислювальній машині (ПЕОМ) у складі тренажно-імітаційного комплексу "Віраж-РД", які сприяють автоматизованому оцінюванню окремих елементів РЕО, а саме: визначенню спроможностей противника та своїх сил щодо ведення РЕР; оцінці можливостей з радіоелектронного подавлення радіолокаційних станцій (РЛС) протиповітряної оборони (ППО) нічних засобів обробки та передачі інформації.

Тому актуальним завданням є удосконалення програмного забезпечення вибору засобів РЕР, а саме створення автоматизованого програмного продукту.

Формулювання завдання дослідження. Метою статті є показати етапи проєктування та розробки програмного забезпечення вибору засобів РЕР на етапі оцінювання обстановки.

Виклад основного матеріалу. Правильне з'ясування отриманого завдання і доведення попередніх розпоряджень неможливі без врахування умов його виконання та без обліку умов обстановки. Тому начальник уже на початковому етапі здійснює попереднє оцінювання обстановки, враховує найбільш важливі, основні умови його виконання. Для вибору ж способу дій, визначення конкретного складу сил і засобів начальник та адміністративний відділ здійснюють детальне оцінювання обстановки, проводять необхідні розрахунки.

Прогнозування перспектив розвитку подій дозволяє успішно подолати такі труднощі сучасного бою, як неповні дані про обстановку й нестачу часу, заздалегідь та обґрунтовано окреслити шляхи й засоби досягнення поставленої мети. Сьогодні прогнозувати можливі зміни обстановки командир повинен на значно більшу глибину й із більшим випередженням у часі, аніж у роки Другої світової війни. А це здебільшого залежить від: рівня підготовленості командира та інших посадових осіб, які беруть участь в управлінні військами; знання ними тактики дій противника; урахування факторів, які впливають на розвиток подій; ведення активної й цілеспрямованої розвідки; наявності надійного зв'язку; своєчасних донесень підлеглих і постійної інформації з боку вищих органів управління й держав-партнерів [5].

Упровадження програмного забезпечення дозволить автоматизувати оцінювання обстановки. Виконання цього завдання можна розбити на такі основні етапи:

введення основних даних про засоби РЕР;

проведення необхідних розрахунків;

фільтрація та аналіз засобів РЕР, які відповідають обстановці та поставленим завданням;

отримання звітів та звітної документації.

Система повинна підтримувати виконання таких транзакцій: введення, оновлення та знищення даних про засоби РЕР у базі даних; формування звітів, доступних для збереження або друку.

У процесах аналізу та проєктування інформаційної підсистеми одним з основних засобів відображення структури компонентів програмних систем є графічні моделі, перевагами яких, порівняно зі словесними описами, є простота і компактність, а також легкість сприйняття. Для подання різних аспектів концептуальної моделі системи використовують три типи діаграм: функціонального проєктування, до яких належать DFD-діаграми потоків даних; діаграми моделювання даних (ERD-діаграми «сутність – зв’язок»); діаграми моделювання поведінки. Для дослідження потоків даних інформаційної підсистеми було обрано DFD-діаграми (Data Flow Diagram), на яких відображаються потоки даних, процеси перетворення вхідних потоків на вихідні, сховища інформації, джерела та споживачі інформації, зовнішні щодо системи. Кожний із процесів може бути поданий діаграмою нижчого рівня. Надалі ці діаграми є підґрунтям для формування структури розроблювальних інформаційних систем [6].

Розроблена DFD-діаграма (рис. 1) програмного забезпечення містить вхідні та вихідні потоки даних. Вхідними є функціональні тактико-технічні характеристики (ТТХ), розбиті на шість груп, за допомогою яких можна здійснити вибір засобів РЕР.

Тактико-технічні характеристики засобів РЕР. У програмному забезпеченні можна додавати чи видаляти поля з характеристиками для більш точного знаходження будь-якого засобу. Без ТТХ засобів РЕР функціонування програми стає нераціональним та безглуздим.

Діапазон частот. Залежно від значення частоти (довжини хвилі) радіохвилі належать до того чи іншого діапазону радіочастот (діапазону довжин хвиль). Можна також запропонувати класифікацію радіохвиль за способом розповсюдження у вільному просторі та навколо земної кулі. Це дозволяє здійснювати вибірку за заданим параметром серед усіх засобів РЕР.

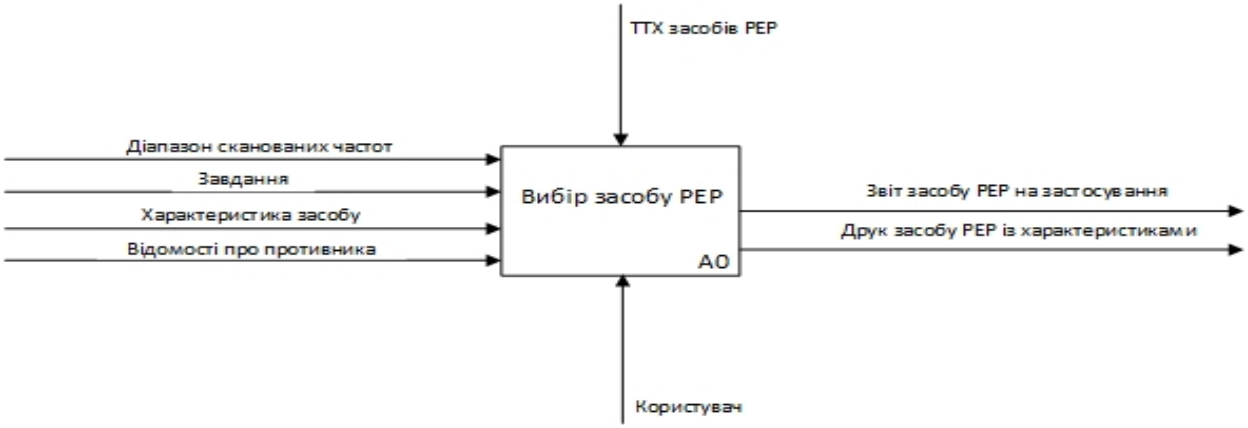


Рис. 1. Контекстна діаграма процесу вибору засобів РЕР на етапі оцінювання обстановки

Завдання. На даний час техніка й засоби досить сучасні та вдосконалені, тому можуть виконувати будь-які завдання різного типу: пошук, передачу, пеленгацію, перехоплення, подавлення. Обравши завдання, яке виконує засіб РЕР за своїм призначенням, можна знайти необхідний варіант.

Характеристики засобу. За необхідності вводяться додаткові параметри засобів РЕР для вибірки.

Відомості про противника. На етапі оцінювання обстановки за допомогою раніше добутої інформації вводять початкові дані, що допомагають краще знайти необхідний засіб.

Користувач. Має доступ до програмного забезпечення (ПЗ), вводить параметри, які необхідно, може здійснювати перегляд, видалення чи редагування засобу в ПЗ, позначати на карті основні точки розташування противника та своїх військ, переглядати зображення засобу та переконатися, що його вибрано правильно, а також завантажувати звітну документацію на друк.

Вихідними даними є: звіт засобу РЕР на застосування, друк звіту про засіб РЕР із характеристиками.

Інформація, що надходить до системи, потрібна для подальшого її оброблення та формування необхідних звітів на вимогу користувача.

Декомпозицію контекстної DFD-діаграми наведено на рис. 2.

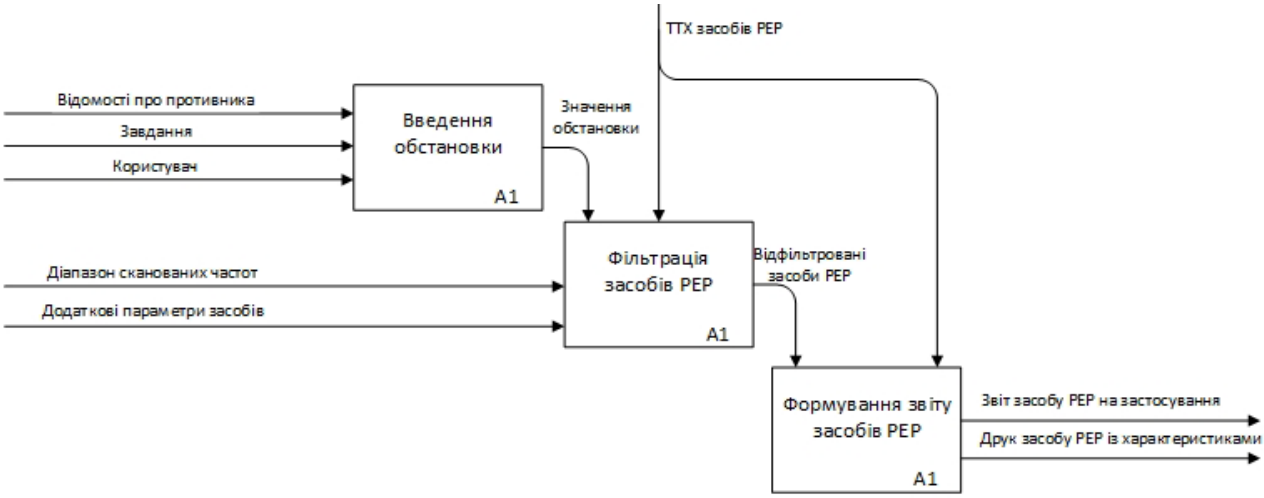


Рис. 2. Декомпозована діаграма процесу вибору засобів РЕР на етапі оцінювання обстановки

Декомпозована діаграма включає такі блоки: введення обстановки, фільтрацію засобів РЕР, формування звіту щодо вибраних засобів РЕР.

Також реалізовано загальну блок-схему функціонування програми (рис. 3).

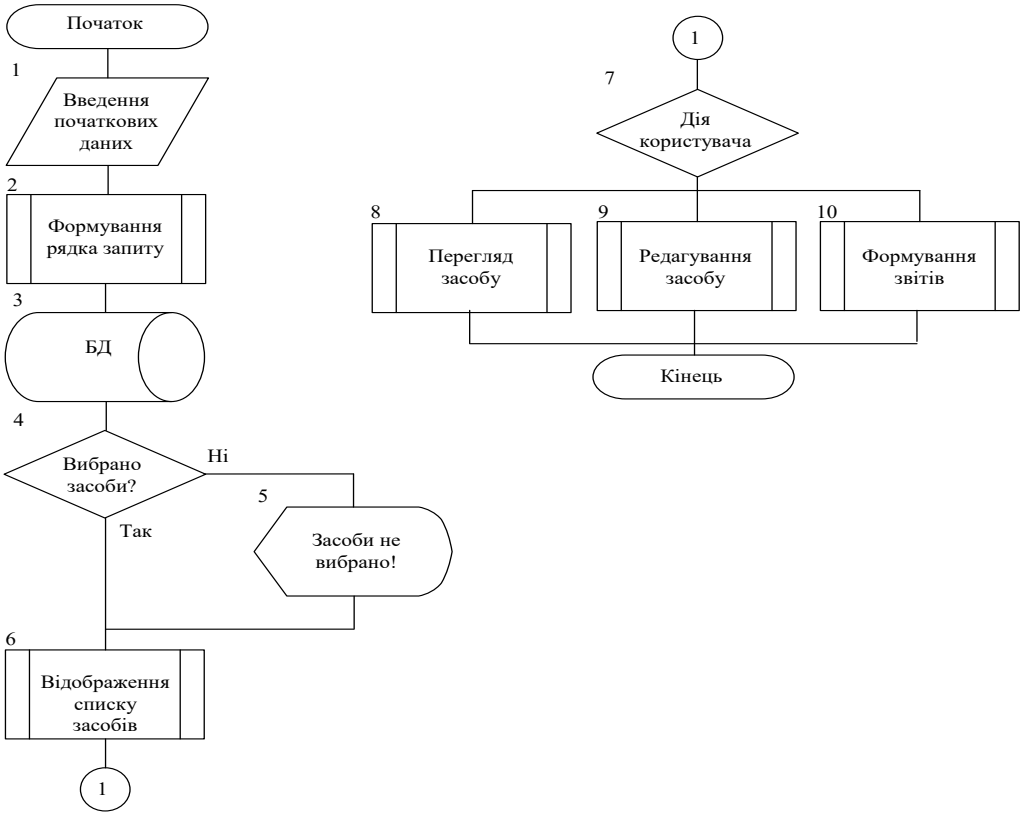


Рис. 3. Блок-схема алгоритму роботи програми

Спроєктувавши роботу програми за допомогою блок-схем, опишемо деякі фрагменти функціонування алгоритму за кожним із блоків.

На початковому етапі роботи (блок 1) вводять вхідні дані – параметри фільтрації $F = \{f_1, f_2, ..., f_n\}$, після чого відбувається формування рядка запиту (блок 2). У блоці 3 виконується пошуковий запит до бази даних (БД), а саме вибір підмножини засобів $D_{\text{sel}} = \{D_{\text{a}}, D_b, ..., D_c\}$ із множини $D = \{D_1, D_2, ..., D_n\}$, $D_{sel} \subset \text{D}$, які відповідають параметрам фільтрації. У блоці 4 відбувається перевірка засобів за результатами вибірки, у разі відсутності тих, які б задовольняли параметри фільтрації, користувачеві виводиться відповідне повідомлення (блок 5), за наявності таких засобів – вони пропонуються користувачеві для подальшої роботи (блок 6). Після отримання множини D_{sel} користувач має змогу вибрати D_{i} із множини D_{sel} (блок 7) для подальших операцій, а саме: перегляду (блок 8), редагування (додавання) (блок 9) та формування звітної інформації (блок 10).

Результатом виконання алгоритму є рішення про засіб РЕР на етапі оцінювання обстановки у вигляді звітної документації.

На основі розроблених діаграм та алгоритму роботи програми було реалізовано програмне забезпечення для автоматизованого вибору засобів РЕР на етапі оцінювання обстановки.

Функціонування програми опишемо за допомогою робочих скріншотів. На рис. 4 область фільтрів дає можливість користувачеві вводити певні параметри фільтрації засобів у БД.

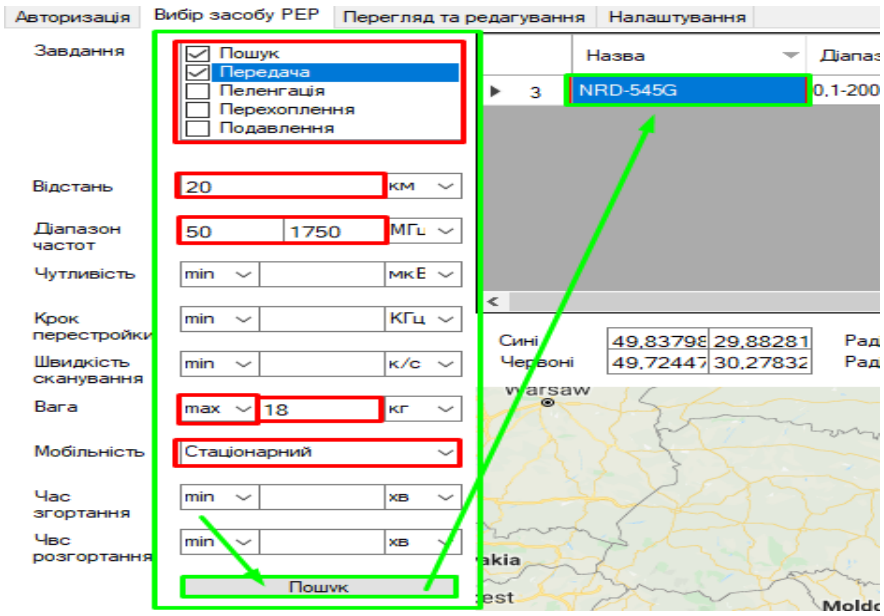


Рис. 4. Область пошукових фільтрів

Область табличного відображення доступних засобів РЕР (рис. 5) надає можливість користувачеві швидко переглядати основні характеристики засобів, сортувати та аналізувати на відповідність поставленим завданням.

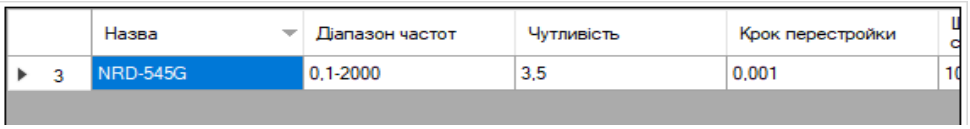


Рис. 5. Область табличного відображення

Область мапи (рис. 6) надає користувачеві можливість візуального уявлення про своє розташування та місце дислокації противника, що дозволяє оцінити дальність, на якій повинен працювати засіб РЕР.

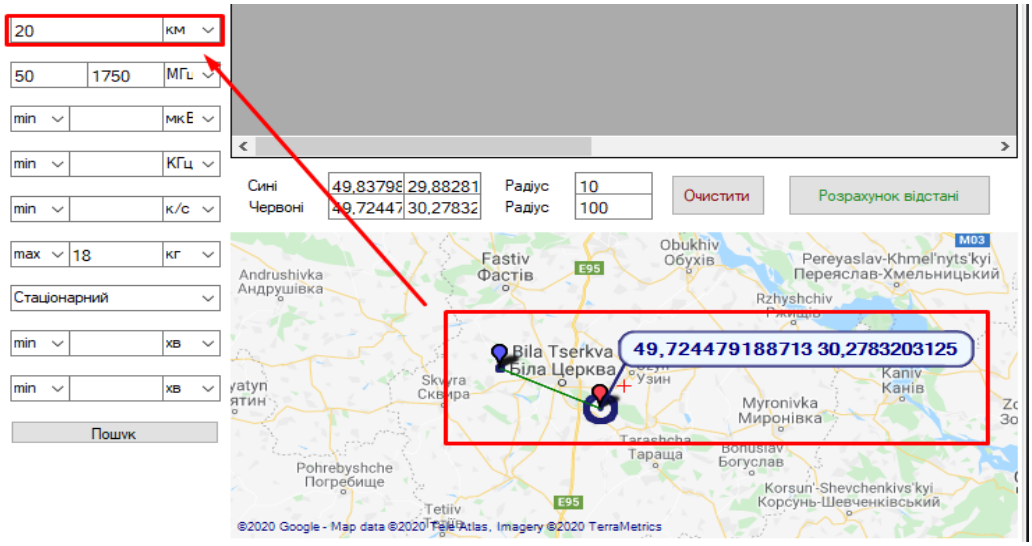


Рис. 6. Область мапи

Обравши засіб натисканням на рядок в області табличного відображення, користувач має змогу більш детально ознайомитися з його характеристиками у відповідній вкладці (рис. 7).

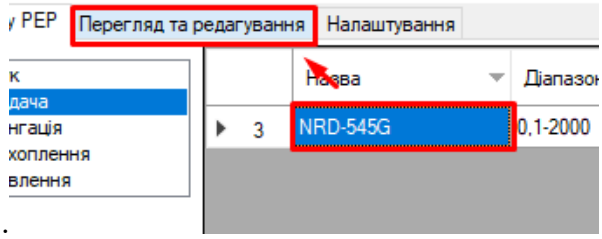


Рис. 7. Перехід у вкладку для детального ознайомлення із засобами РЕР

Вкладка перегляду та редагування (рис. 8) складається із зображення попереднього перегляду, можливостей засобу, звітної документації, характеристик засобу та кнопок керування.

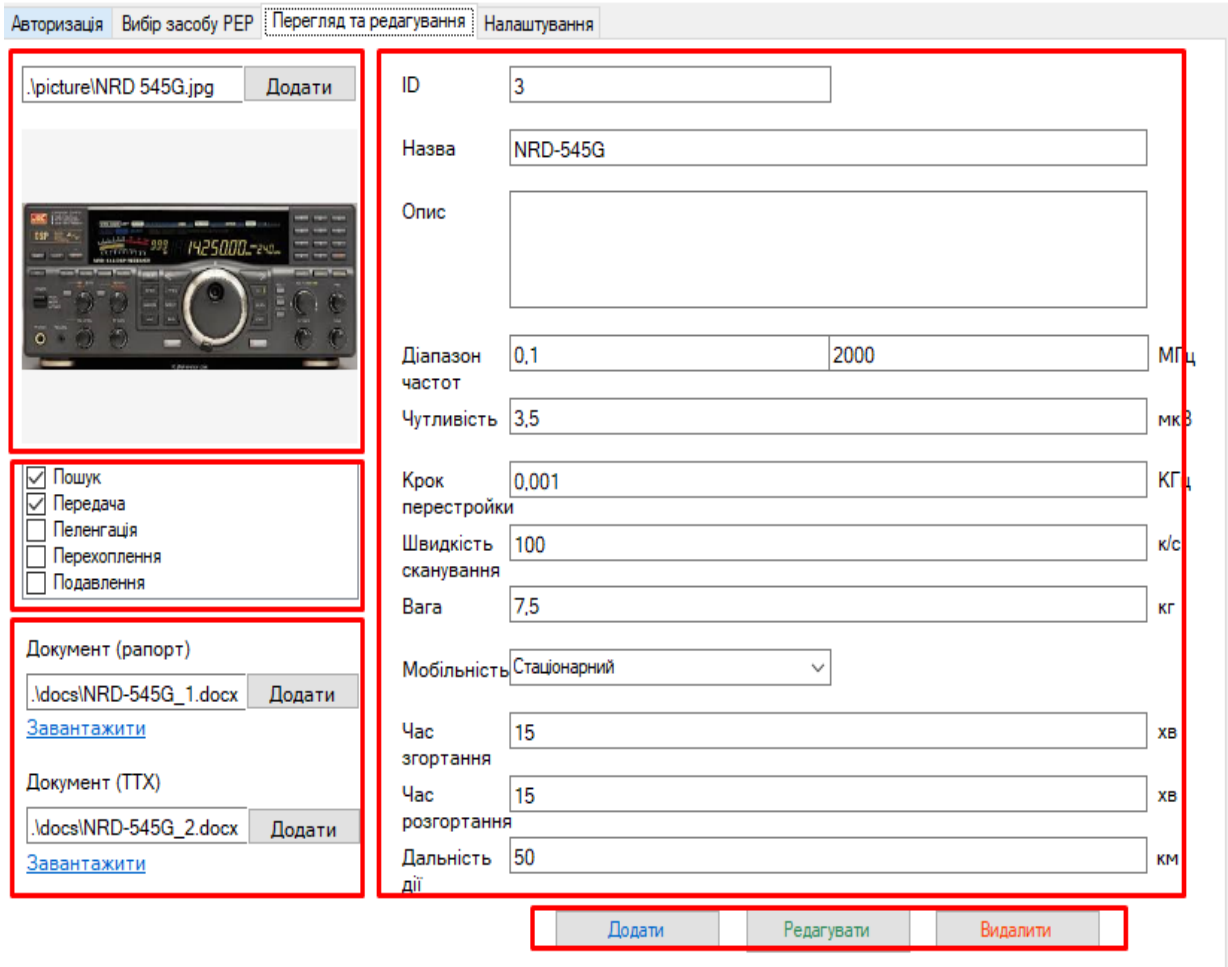


Рис. 8. Вкладка перегляду та редагування

Користувач має можливість змінити зображення засобу за допомогою відповідної кнопки «додавання зображення», після натискання на яку йому буде запропоновано вибір зображення на жорсткому диску комп'ютера. Так само користувач може змінити відповідні документи до кожного засобу РЕР.

Користувач має змогу завантажувати звітну документацію для подальшого використання або друку. Після натискання на відповідні кнопки йому буде запропоновано вказати шлях та назву файлу.

Програмне забезпечення спрямоване на підвищення оперативності прийняття рішень у ході планування ведення розвідки в заданому районі та надання рекомендацій щодо

вибору засобів РЕР за обраним критерієм. А це означає, що можна передбачити розвиток подій і тим самим зменшити бойові втрати серед військовослужбовців, а також забезпечити успішне виконання поставлених завдань.

Дане програмне забезпечення створене для командирів (начальників) і може застосовуватися на командних пунктах частин та підрозділів РЕР для планування ведення розвідки.

Основними результатами автори вважають те, що впровадження програмного забезпечення дозволить автоматизувати етап оцінювання обстановки. Воно спрямоване на підвищення оперативності прийняття рішень у ході планування ведення розвідки в заданому районі та надання рекомендацій щодо вибору засобів РЕР за обраним критерієм. А це означає, що можна передбачити розвиток подій і тим самим зменшити бойові втрати серед військовослужбовців, а також забезпечити успішне виконання поставлених завдань.

Висновки. Отже, у статті розглянуто інформаційні потоки, необхідні для подальшого оброблення інформації та формування потрібних звітів на вимогу користувача. Вказано основні блоки, які потрібно розробити в програмному забезпеченні, та реалізовано саме програмне забезпечення. Запропонований програмний продукт полегшить роботу командирам (начальникам) щодо вибору засобів РЕР на етапі оцінювання обстановки, зменшить витрачений ресурс часу. Наступним кроком дослідження є удосконалення програмного забезпечення для більш точного визначення засобу РЕР на етапі оцінювання обстановки, нанесення бойової обстановки на мапу та покращення інтерфейсу.

СПИСОК ЛІТЕРАТУРИ

1. Основи управління та прийняття рішень у військовій справі : навч. посіб. / М. Ф. Пічугін, Г. П. Чернявський, В. А. Шуренок, В. Є. Полуектов. Житомир : ЖВІ НАУ, 2007. 56 с.
2. Розвідка та іноземні армії. Ч. 1. Основи військової розвідки : навч. посіб. / Ю. Л. Бондаренко, В. В. Вінник, О. В. Устименко, С. І. Черняєв. Житомир : ЖВІ, 2018. 140 с.
3. Бойко І. Л. Основи управління та прийняття рішень // Наука і освіта. 2016. URL: http://electrician.pto.org.ua /index.php/authors-ua/itemlist/category/osnovy_upravlinnya/ (дата звернення: 20.06.2020).
4. Вартасарян В. А. Радиоэлектронная разведка. Москва : Воениздат, 1991. 225 с.
5. Левченко О. В., Вінник В. В., Устименко О. В. Розвідка та іноземні армії. Ч. 2. Інформаційна робота : навч. посіб. Житомир : ЖВІ, 2019. 150 с.

Подано 25.06.2020

REFERENCES

1. Pichuhin, M. F., Cherniavskyi, H. P., Shurenok, V. A., & Poluektov, V. Ye. (2007). *Osnovy upravlinnia ta pryiniattia rishen u viiskovii spravi [Fundamentals of management and decision-making in military affairs]*. Zhytomyr: ZhMI NAU [in Ukrainian].
2. Bondarenko, Yu. L., Vinnyk, V. V., Ustymenko, O. V., & Cherniaiev, S. I. (2018). *Rozvidka ta inozemni armii. Ch. 1. Osnovy viiskovoi rozvidky [Intelligence and foreign armies. Part 1. Fundamentals of military intelligence]*. Zhytomyr: ZhMI [in Ukrainian].

3. Boiko, I. L. (2016). Osnovy upravlinnia ta pryiniattia rishen [Fundamentals of management and decision making]. *Nauka i osvita [Science and Education]*. Retrieved from http://electrician.pto.org.ua /index.php/authors-ua/itemlist/category/osnovy_upravlinnya/ [in Ukrainian].

4. Vartasarian, V. A. (1991*). Radioelektronnaia razvedka [Electronic intelligence]*. Moscow: Voenizdat [in Russian].

5. Levchenko, O. V., Vinnyk, V. V., & Ustymenko, O. V. (2019). *Rozvidka ta inozemni armii. Ch. 2. Informatsiina robota [Intelligence and foreign armies. Part 2. Information work]*. Zhytomyr: ZhMI [in Ukrainian].

V. S. Shevchenko, R. V. Netrebko, A. I. Netrebko, I. V. Zimchuk

IMPLEMENTATION OF SOFTWARE SELECTION OF RADIO ELECTRONIC INTELLIGENCE MEANS AT THE STAGE OF ASSESSMENT OF THE SITUATION

The article shows the implementation of the software for the selection of electronic intelligence at the stage of assessing the situation on the basis of theoretical studies conducted by the authors. It is indicated on the basis of which documents the assessment of the situation with the choice of electronic reconnaissance means is carried out, what stages this process consists of, what is needed for the selection of electronic reconnaissance means. The design of information flows of the program for the selection of electronic intelligence means at the stage of assessing the situation with the help of Data Flow Diagrams. The general block diagram of algorithm of work of the software of a choice of means of electronic reconnaissance at a stage of an assessment of a situation is constructed. On the basis of the conducted researches the database for storage of the list of means of electronic reconnaissance is developed. The prototype of the software for the selection of electronic intelligence means at the stage of situation assessment is implemented and examples of work on each of the main blocks are given in the form of screenshots, which were pre-designed in diagrams and block diagrams of algorithms. The advantages and disadvantages of the developed software for the selection of electronic reconnaissance means at the stage of situation assessment are determined. The further steps of research and improvement of the program of a choice of means of radio-electronic intelligence at a stage of an assessment of a situation are specified.

Keywords*: electronic reconnaissance; situation assessment; electronic reconnaissance means; electronic environmen;, design stages; software; anti-terrorist operation; electronic means; tactical and technical characteristics; database; data slow diagram.*

УДК 355.4 DOI: 10.46972/2076-1546.2020.18.08

Д. А. Іщенко, В. А. Кирилюк, С. Д. Іщенко, Л. М. Марищук

ПАРАДИГМА ПРОТИДІЇ РОЗВІДУВАЛЬНО-УДАРНИМ БЕЗПІЛОТНИМ АВІАЦІЙНИМ КОМПЛЕКСАМ

У статті показано актуальність проблеми протидії розвідувально-ударним безпілотним авіаційним комплексам, обґрунтовано необхідність удосконалення науково-методичного забезпечення її вирішення за відповідно визначеною парадигмою.

Парадигмою протидії безпілотним авіаційним комплексам запропоновано вважати концептуальну теоретико-методологічну модель боротьби з безпілотними засобами, яка на теперішній час надає можливості визначення проблем розвитку сил та засобів протидії цьому виду озброєння.

Розроблена парадигма протидії може бути елементом науково-методичного забезпечення, що сприяє розв'язанню проблеми комплексного застосування сил та засобів протидії розвідувально-ударним безпілотним авіаційним комплексам з метою набуття спроможностей військ (сил) для виконання завдань за призначенням в умовах застосування безпілотних засобів.

Визнання такої парадигми фахівцями означає, що їх діяльність будується на основі прийнятої моделі протидії безпілотним авіаційним комплексам з використанням єдиних правил і стандартів, запроваджених у цій галузі. Спільність та узгодженість підходів, яку вони передбачають, є передумовами для забезпечення необхідного наукового рівня визначеного напряму дослідження.

Запропонований підхід окреслює завдання, зміст, складові, принципи оцінювання засобів протидії безпілотним авіаційним комплексам за внеском в ефективність системи захисту об'єкта від розвідувально-ударних (ударних) комплексів противника, що систематизує знання в предметній галузі та створює підґрунтя для практичної реалізації результатів досліджень щодо проблем сучасної збройної боротьби.

Перспективою подальших досліджень є уточнення математичних розрахунків відповідно до особливостей військ (сил), військового об'єкта, системи захисту від розвідувально-ударних (ударних) безпілотних авіаційних комплексів противника та зразків військової техніки, які входять до її складу.

Ключові слова: *безпілотні авіаційні комплекси; модель боротьби з безпілотними засобами; парадигма протидії розвідувально-ударним безпілотним авіаційним комплексам.*

Постановка проблеми в загальному вигляді. Досвід ведення бойових дій з російськими окупаційними військами за повернення тимчасово окупованих територій підтверджує, що в умовах сучасних війн і воєнних конфліктів (Сирія, Нагірний Карабах) зростає значення фактора застосування безпілотних авіаційних комплексів (БпАК), або за термінологією Збройних сил (ЗС) Російської Федерації (РФ) – комплексів з безпілотними літальними апаратами (БпЛА).

Як зазначається в [1], має місце використання безпілотних систем щонайменше 95 країнами світу, зокрема й тими, що мають обмежене державне фінансування цього напрямку.

Вплив фактора БпЛА на хід і результат бойових дій характеризується збільшенням їх кількості й покращенням якісних характеристик наземної та повітряної складових, а також нарощуванням функціональних можливостей щодо здійснення впливів засобами вогневого ураження. Відповідно, БпАК набувають ознак розвідувально-ударних (РУ) комплексів, що забезпечує зростання спроможностей військових частин (підрозділів) військ (сил) до виконання завдань за призначенням із використанням зазначеного виду озброєння.

Результатами поглибленого аналізу сучасних воєнних конфліктів за напрямком радіоелектронної боротьби (РЕБ) та виконання завдань Об'єднаними силами з використанням БпАК і засобів РЕБ підтверджується закономірність щодо залежності успішності використання РУ БпАК від ефективності протидії (ПД) їх застосуванню. Розвиток РУ БпАК (зокрема створення в РФ перспективних зразків "Корсар", "Альтиус", "Охотник" тощо) обумовлює необхідність і своєчасність удосконалення та комплексного застосування сил і засобів – складових ПД РУ БпАК: розвідки, вогневого ураження, механічного й радіоелектронного впливу комплексів РЕБ на радіоелектронні системи БпАК, а також на засоби ураження, що запускають з борту БпЛА.

В умовах ресурсних обмежень для досягнення переваги над противником у силах і засобах побудова раціональної системи ПД РУ БпАК є обов'язковим завданням ведення сучасних бойових дій, вирішення якого передбачає наявність відповідного науково-методичного апарату. Відсутність такого апарату породжує проблему ефективності ПД РУ БпАК. Парадигма ПД РУ БпАК як концептуальна теоретико-методологічна модель боротьби з безпілотними засобами повинна бути основоутворювальним елементом такого науково-методичного апарату.

Отже, розроблення парадигми ПД РУ БпАК є актуальним завданням у вирішенні зазначеної проблеми.

Аналіз останніх досліджень і публікацій показав, що в більшості робіт, присвячених проблемі ПД РУ БпАК, розглянуто лише окремі її елементи. Концепцію створення комплексної системи ПД БпАК противника було розроблено у 2017 році на термін до 2020 року, тому вона потребує вдосконалення з урахуванням нових поглядів і практики застосування РУ БпАК [2], а також результатів аналізу досвіду військових конфліктів останнього десятиліття: україно-російського у період з 2014 до 2020 року [3], військового конфлікту в Сирії (2011–2020 років) [2, 3] і збройного конфлікту між ЗС Вірменії та Азербайджану в Нагірному Карабаху в 2020 році [2–4].

У наш час спостерігається значне зростання безпілотних платформ усіх розмірів і форм із відповідним збільшенням кількості корисного навантаження та можливостей, зрушення у бік підтримки інтеграції безпілотних систем в об'єднані сили та їх використання на полі бою [5]. З іншого боку, такий фактор ускладнює повітряні, наземні та морські операції і зумовлює потребу створення систем ПД БпАК. На теперішній час на світовому ринку знаходиться значна кількість засобів ПД БпАК, зокрема й вітчизняного виробництва [1, 6], які можуть функціонувати у складі протибезпілотних систем (C-UAS) [1]. Слід відзначити, що застосування таких засобів у ході антитерористичної операції та операції Об'єднаних сил забезпечує набуття спроможностей за функціональною групою PROTECT [7, 8].

Разом з тим аналіз наявних засобів показує, що вони розроблені для найшвидшого задоволення потреб військ (сил) у ПД БпАК. В умовах ресурсних та часових обмежень питання взаємодії (координації, інтеграції), а також взаємозалежності в системах не завжди досліджуються як пріоритетні.

Прогностичний аналіз зростання суперечності в боротьбі між безпілотними (UAS) та протибезпілотними (C-UAS) системами дозволяє стверджувати, що розвиток РУ (ударних) БпАК та перерозподіл безпілотних засобів для підтримки інших бойових командирів (CCDR) спричиняє власний набір унікальних проблем, які, ймовірно, будуть потребувати, щоб безпілотні системи працювали у більш складних умовах [5], що для ефективної ПД БпАК обумовлює потребу відповідного (з перспективою) вдосконалення озброєння, тактики підрозділів (сил і засобів), навчання фахівців за призначенням і підготовки військ (сил).

На думку фахівців, можливості безпілотних систем не є унікальними в порівнянні з пілотованими системами [5], тому проведений аналіз РУ БпАК як об'єкта протидії показує, що визначальний внесок у результативність застосування комплексу робить його повітряна складова (БпЛА), що дозволяє визначити його як засіб повітряного нападу (ЗПН).

Аналіз джерел [9, 10] дозволив застосування терміна "парадигма" (з грец. – приклад, взірець), визначення поняття якого найбільше відповідає завданню дослідження. У загальному значенні це теоретико-методологічна модель [9]. Парадигма – початкова концептуальна схема, модель постановки проблем і їх рішення, а також комплекс методів дослідження, домінуючих протягом певного історичного періоду в науковому співтоваристві [10].

Отже, аналіз останніх досліджень і публікацій показав можливість, необхідність та доцільність ітераційного уточнення Концепції створення комплексної системи ПД БпАК противника з урахуванням розробленої парадигми ПД РУ БпАК (концептуальної теоретико-методологічної моделі боротьби з безпілотними засобами).

Формулювання завдання дослідження. Метою дослідження є аналіз завдань, вирішуваних засобами C-UAS, та їх взаємозв'язків для викриття елементів БпАК і здійснення впливів щодо них і бортових засобів ураження, а також розроблення моделі процесу ПД РУ БпАК як послідовності частково впорядкованих кроків, потрібних для недопущення виконання противником цільових завдань комплексами з БпАК.

Виклад основного матеріалу. Для вирішення визначеного завдання приймемо такі положення.

Моделювання ПД РУ БпАК є першим кроком у розробці системи, яка реалізує процес ПД, коли розробник спочатку створює концептуальну модель того, як елементи системи взаємодіють один з одним. У перспективі моделювання ПД РУ БпАК передбачає просування від концептуальної до фізичної моделі, яка може бути використана в ході випробувань (заходів оперативної (бойової) підготовки).

Концептуальна модель ПД РУ БпАК – це абстрактна модель складових процесу (системи) ПД, що відображає взаємозв'язок між реальними процесами (об'єктами) предметної області – збройної боротьби засобів C-UAS з елементами БпАК противника.

Інформаційно-логічна модель (ІЛМ) ПД РУ БпАК розглядається як відбиття

предметної області боротьби з безпілотними засобами у вигляді сукупності засобів C-UAS інформаційних об'єктів та їхніх структурних зв'язків. ІЛМ розроблюється як узагальнений неформальний опис створюваної системи, що об'єднує часткові відомості, отримані в результаті вивчення зібраних даних, опитування користувачів засобів C-UAS і вивчення досвіду їх використання, а також прогнозування майбутніх застосувань. Цей опис виконано вербально та частково формалізовано з використанням математичних формул, таблиць, графіків.

Відповідно до теорії та практики бойових дій [22], зміст боротьби із ЗПН доцільно розглядати як процес, у якому формально можна виділити низку етапів. Етапи ПД БпАК можна виділити за аналогією до "класичної" боротьби з авіацією (ЗПН) противника, додатково враховуючи сили і засоби, визначальні для кожного етапу ПД БпАК:

до здійснення вильоту БпЛА – вогневе ураження апаратів на стартових позиціях (літаків на аеродромах) та наземних елементів комплексів (аеродромів) ударами авіації, ракетних військ та артилерії, спеціальними діями;

під час польоту БпЛА до входу в задану область та здійснення пуску зброї – знищення літаків у польоті засобами "повітря – повітря" авіації та зенітними засобами "поверхня – повітря" сил протиповітряної оборони (ППО);

під час запуску та польоту засобу ударної зброї до цілі – знищення засобів ураження класу "повітря – поверхня" (керованих та некерованих ракет) у польоті засобами "повітря – повітря" авіації та зенітними засобами "поверхня – повітря" сил ППО.

Практично на всіх етапах "класичної" боротьби із ЗПН противника має місце застосування сил і засобів РЕБ у системі комплексного застосування бойових сил і засобів активного впливу та бойового (оперативного) забезпечення.

БпЛА як ЗПН має відповідні особливості, які виявляються в різному ступені відповідно до класу та типу, що потребує врахування у дослідженнях питань ПД БпАК. Досвід антитерористичної операції та операції Об'єднаних сил показує обов'язковість врахування прогнозованих дій РФ. Аналіз відомих підходів фахівців РФ [11] демонструє визначення факторів необхідності оцінювання можливостей РЕБ у ході дослідження концептуальних питань ПД БпЛА. Основним змістом факторів є зменшення можливостей наявних систем боротьби з "класичними" ЗПН порівняно з БпАК з виявлення, вогневого ураження та інформаційного протиборства.

Питанням ПД БпАК і РЕБ у процесі застосування БпЛА присвячено достатню кількість досліджень і публікацій [1, 11]. У більшості робіт розглянуто питання вирішення завдання РЕБ – дезорганізації в контурі управління БпАК, а також радіоелектронного подавлення (РЕП) радіоелектронних засобів (РЕЗ) (навігації, управління та телеметрії) БпЛА на всіх етапах ПД. Водночас питання ПД БпАК засобами та методами РЕБ під час запуску з борту БпЛА та польоту засобу ударної зброї до цілі потребують дослідження, тому що необхідно визначити місця, ролі, можливості їх реалізації в комплексній системі боротьби з БпАК і забезпечення набуття спроможності PROTECT.

З урахуванням того, що жодна на поточний час система озброєння, яка використовується з безпілотних систем, не була спеціально розроблена для безпілотних платформ, за результатами аналізу [5, 12] визначено, що на сучасному етапі та на середньострокову перспективу найбільш актуальною щодо розвитку безпілотних систем є проблема ПД РУ комплексам, які мають у складі БпЛА, оснащені керованими засобами

ураження (КЗУ) з лазерними системами наведення (ЛСН). КЗУ може бути ударна або протитанкова самонавідна ракета, побудована за напівактивним методом самонаведення, за [5] до таких належать: LAHAT, БпЛА Hunter, SPIKE з ЛСН, UAS Battlelab, APKWS II. Наприклад, зброя БпЛА – ракета LAHAT вагою 13 кг, оснащена багатоцільовою бойовою частиною з кумулятивним зарядом, може забезпечити реалізацію наведення на відстані не менше 10 км до цілі, яка "підсвічується" лазерним вказівником. Лазер підсвічування цілі, традиційно як для напівактивної ЛСН, знаходиться на борту БпЛА, крім того, система може працювати за позначенням цілі іншим лазерним вказівником (передовим навідником).

Розвиток тактики застосування засобів, що реалізують метод лазерного наведення, дозволив фахівцям розробити способи використання КЗУ з ЛСН та визначити [12] можливі варіанти таких БпАК. Для розроблення способів ПД РУ БпАК необхідно за наявним досвідом [13–15] актуалізувати можливі варіанти дій противника з використанням БпЛА, які є носіями КЗУ з ЛСН. Визначають варіанти за варіацією розташування КЗУ з ЛСН та джерела лазерного опромінювання об'єкта-цілі на одному чи різних носіях.

Варіант 1. БпЛА – носій КЗУ з ЛСН є також носієм джерела лазерного опромінювання (лазера підсвітлення). Його політ здійснюється на висотах, що забезпечують початок підсвітлення об'єкта-цілі з дальності близько 10 км. Для забезпечення стійкого підсвітлення під час здійснення прицільного пуску та наведення КЗУ з ЛСН на об'єкт-ціль БпЛА-носій повинен здійснювати рух і лазерне опромінювання об'єкта протягом усього часу наведення КЗУ до зустрічі із ціллю. Це може становити до 20–30 с.

Варіант 2. БпЛА – носій КЗУ з ЛСН та інший носій джерела лазерного опромінювання (лазера підсвітлення) (БпЛА, пілотований літак, наземний навідник) синхронно виходять у задані райони та виконують дії за призначенням з лазерного опромінювання та пуску КЗУ. Після пуску БпЛА – носій КЗУ із ЛСН виходить із зони ПД БпАК, інший носій лазера здійснює лазерне опромінювання об'єкта протягом усього часу наведення КЗУ до зустрічі із ціллю.

Потребує врахування в разі визначення варіантів: застосування БпАК разом із пілотованими повітряними засобами; застосування декількох БпАК; застосування організованого "рою" БпЛА тощо.

Запропоновані варіанти можуть бути реалізовані в різні способи та тактичні прийоми, що мають власні просторово-часові параметри та ймовірнісні характеристики їх реалізації.

За результатами аналізу досвіду щодо побудови та застосування БпЛА, попередніх досліджень протибезпілотних (C-UAS) технологій, відкритих джерел спеціалізованої інформації [1] доцільно визначити методи, що потребують реалізації в протибезпілотних системах ПД БпАК (методи C-UAS).

1. Методи інформаційного забезпечення C-UAS (виявлення джерел інформації та викриття, ідентифікації, відстеження елементів БпАК – об'єктів розвідки, вироблення цілевказівок):

радіоелектронна (радіо (РР), радіотехнічна (РТР)) розвідка (РЕР) радіоелектронних об'єктів;

оптико-електронна (оптична візуальна (ОВР)) розвідка (ОЕР);

радіолокаційна розвідка (РЛР);

акустична розвідка (АкР).

2. Методи радіоелектронного (електромагнітного) впливу (дезорганізації управління елементами БпАК (UAS), подавлення і перехоплення з використанням електромагнітного спектра частот):

РЕП радіоперешкодами РЕЗ систем управління і навігації (СУіН) та оптико-електронними перешкодами (ОЕП) чутливих елементів (приймачів) ЛСН;

мікрохвильове високої потужності опромінювання РЕЗ;

лазерне (світлове) опромінювання цільової апаратури та елементів ЛСН;

введення в оману (маніпуляція, спуфінг) системи управління.

3. Методи фізичного (кінетичного) впливу (ураження, виведення з ладу елементів БпАК (UAS):

вогневе ураження засобами ракетних військ і артилерії (РВіА), авіації повітряних сил (ПС) і армійської (АА), зенітної артилерії та зенітними ракетами ППО, стрілецького озброєння та спеціальних дій, у тому числі Сил спеціальних операції (ССО);

зіткнення в повітрі (таран) безпілотними засобами протидії, у тому числі БпАК ПД;

захоплення засобами повітряного загородження та припинення керованого руху (аеростат, сітка).

Технічні засоби, що реалізують вказані методи розміщують на платформах протибезпілотних C-UAS систем, які за розташуванням у просторі та можливістю до пересування можна поділити на:

наземні (польові) стаціонарні (пересувні) та наземні (корабельні) мобільні;

повітряні пілотовані та безпілотні (БпЛА) літакового (вертолітного) типу;

космічні (спостереження, РЕР, РЛР, ОЕР);

ручні (рушниці впливу).

Підтвердженням можливості реалізації вказаних методів із використанням засобів інформаційного забезпечення, радіоелектронного і фізичного впливу та побудови системи захисту об’єкта від РУ (ударних) БпАК, зокрема оснащених КЗУ з ЛСН, за модульним принципом із застосуванням різних платформ може бути варіант її побудови, наведений у [16, 17]. У таких системах передбачено комплексне застосування модулів боротьби з КЗУ високоточної зброї досить широкої номенклатури: керованих ракет із протирадіолокаційними, лазерними, телевізійними, інфрачервоними головками самонаведення; керованих авіабомб; крилатих ракет тощо [18, 19].

Можливий варіант складу засобів у системі комплексного застосування сил і засобів для боротьби з РУ БпАК, що мають на борту КЗУ, зокрема з ЛСН, наведено в табл. 1.

Запропонований варіант дозволяє досліджувати питання взаємодії (координації, інтеграції), а також взаємозалежності засобів у протибезпілотних системах C-UAS технологій.

Умовою побудови таких систем є обов’язковість загальносистемного управління щодо введення (безпосередньо або опосередковано) складових у систему, їх інформаційного забезпечення та організації взаємодії в інтересах виконання загального завдання системи та ефективності функціонування засобів відповідно до цільового призначення. Система повинна досліджуватися за підходом [1], згідно з яким протидія БпЛА – складний багатоетапний процес, що включає взаємодію між кількома окремими системами та між цими системами й оператором (операторами) – людиною.

Таблиця 1

Складові засоби системи боротьби з розвідувально-ударними БпАК

<table>
<tr><td rowspan="2">№ з/п</td><td rowspan="2" colspan="2">Потенційна складова (система комплексної ПД БпАК противника розвідувального (РУ) призначення)</td><td colspan="4">Функціонування в системі комплексної ПД БпАК противника (за етапами)</td></tr>
<tr><td>Етап 1. Знаходження БпЛА на стартовій позиції</td><td>Етап 2. Рух БпЛА за маршрутом польоту</td><td colspan="2">Етап 3. Пуск БпЛА КЗУ по об’єкту ураження</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2" colspan="2">Засоби космічного спостереження (цільове навантаження)</td><td>+ (РР, РЛР, ОЕР)</td><td>+ (РР)</td><td>+ (РР)</td><td>+ (РР)</td></tr>
<tr><td colspan="4">Виявлення елементів БпАК противника</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2" colspan="2">Засоби РЕР (РР)</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td colspan="4">Виявлення ДІ, викриття СУ, спостереження ОР у БпАК противника</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2" colspan="2">Засоби РЛР, АкР, ОВР</td><td rowspan="2"></td><td>+</td><td>+</td><td>+</td></tr>
<tr><td colspan="3">Виявлення елементів БпАК противника (БпЛА, КЗУ) у польоті</td></tr>
<tr><td rowspan="4">4</td><td rowspan="4">Засоби РЕБ. Дезорганізація управління БпАК противника</td><td rowspan="2">РЕР (РТР), електронне забезпечення</td><td>+</td><td>+</td><td>+</td><td>+ Виявлення лазерних випромінювань</td></tr>
<tr><td colspan="4">Виявлення РЕОб, викриття СУ БпАК противника</td></tr>
<tr><td rowspan="2">РЕП</td><td rowspan="2">+ (РП РЕЗ СУ і Н)</td><td rowspan="2">+ РП РЕЗ СУіН</td><td>+ РП РЕЗ СУіН</td><td>+ РП РЕЗ СУіН</td></tr>
<tr><td>ОЕП засобам розвідки</td><td>ОЕП КЗУ з ЛСН</td></tr>
<tr><td colspan="4">Подавлення РЕОб (РЕЗ) БпАК противника</td></tr>
<tr><td>5</td><td colspan="2">Засоби вогневого ураження елементів БпАК противника</td><td>+ (РВіА, ССО)</td><td>+ (ПС, АА і ППО, ССО)</td><td>+ (ПС, АА і ППО)</td><td>+</td></tr>
<tr><td rowspan="2">6</td><td rowspan="2" colspan="2">БпАК ПД (РУ, перехоплення)</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td colspan="4">Виявлення елементів БпАК противника та здійснення впливів</td></tr>
</table>

За даними The Center For The Study of The Drone at Bard College “Counter-Drone Systems 2nd Edition” і результатами аналізу інформації про ситуацію на світовому ринку засобів C-UAS технологій [1], у порівнянні 2018 та 2019 років спостерігається зростання кількості продуктів (товарів) технологій на 52% (з 277 до 537); кількості фірм, що їх виробляють, на 56% (зі 155 до 277), а також незначне (8%) зростання кількості країн (з 33 до 38), у яких здійснюється розроблення та виробництво (табл. 2, 3).

Таблиця 2

Результати аналізу засобів C-UAS технологій за призначенням і методами виявлення та впливу

Призначення	Кількість засобів		Кількість методів виявлення або впливу	Метод (спосіб), що реалізується
Виявлення	175	138	190 – один датчик; 133 – комбінація датчиків (42 з них – чотири та більше)	159 – РТР
				147 – РЛР
				113 – ОЕР
				111 – інфрачервона розвідка
				34 – акустична розвідка
Вплив	214		147 – один метод; 215 – комбінація (системи управління та передавання даних і глобальні навігаційні супутникові системи як об'єкти впливу вважаються різними)	259 – радіоперешкоди
				31 – спуфінг
				18 – лазери
				27 – сітки
				8 – зіткнення

Таблиця 3

Результати аналізу засобів C-UAS технологій за базуванням

Платформа (базування)	Кількість засобів	
Наземна	375	260 – фіксовані
		55 – мобільні
		59 – не визначено
На борту БпЛА	34	
Поєднання наземних елементів і тих, що на борту БпЛА	12	
Портативні	106	

Одночасно з отриманими результатами щодо потужного розвитку засобів систем C-UAS необхідно враховувати власний досвід і висновки фахівців [1] про значну кількість проблемних питань у технологічному, економічному, правовому аспектах їх якості та ефективності застосування.

Відзначається, що відсутність "міжнародних стандартів щодо належного проєктування та використання систем C-UAS" потенційно обумовлює "значні розбіжності між продуктивністю та надійністю систем", які "працюють не так, як рекламуються".

За такої неповної визначеності вихідних умов, створення комплексної системи захисту військових об'єктів [20] за модульним принципом використання засобів спеціалізованих C-UAS і таких, що не є спеціалізованими, але за технічними властивостями та характеристиками також можуть бути корисними й ефективними в системі ПД БпАК, потребує не тільки проведення за обґрунтованими методиками експериментів і випробувань, але й попередніх теоретичних досліджень із використанням як формалізованих, так і слабоструктурованих методів.

Систему ПД (C-UAS) потрібно оцінити за вихідними даними (кількість і види засобів противника, військ (сил), час тощо):

щодо створення – адекватність (відповідність) загальній оперативній (тактичній) та радіоелектронній обстановці за сукупністю складових ПД (C-UAS);

щодо правильності призначення заходів у діях військ (сил) та сукупності елементів сил і засобів РЕБ (РЕП, ПД (C-UAS), електронного забезпечення), що узгоджено функціонують у єдиній системі з метою ПД (C-UAS).

Припущення. Застосування за призначенням системи ПД (C-UAS) – це військові дії, що підлягають оцінюванню. Мірою визначення ефективності завжди править ступінь досягнення поставленої мети.

Вважаємо, що мета застосування за призначенням системи ПД (C-UAS) – нейтралізація (послаблення чи припинення дії, впливу тощо) [21] сил та засобів UAS противника щодо власних військ (сил).

Ступінь досягнення поставленої мети – кількість засобів UAS противника (КЗУ), що не виконують (назавжди або тимчасово) завдання впливу на об’єкти, війська (сили), тому що нейтралізовані заходами системи ПД (C-UAS). Частка нейтралізованих засобів противника від загальної їх кількості така, що забезпечує функціонування об’єктів і виконання завдань військами (силами) з ефективністю, не гірше прийнятної, у визначених умовах обстановки.

Терміном “військовий об’єкт” визначено ділянки місцевості, будівлі, споруди, які постійно чи тимчасово використовуються з’єднанням, військовою частиною і підрозділом ЗС для виконання завдань або розміщення та укриття особового складу, зберігання бойової техніки або військового майна; військові транспортні засоби, озброєння та військова техніка, а також об’єкти, які підлягають захисту й охороні (обороні) ЗС [20].

Застосування військ (сил) за призначенням розглядається як функціонування сукупності військових об’єктів.

Особливістю оцінювання ефективності ПД (C-UAS) у ході прогнозування є неповна визначеність для тих, хто проводить оцінювання, щодо кількісного та якісного складу сил і засобів UAS противника, які повинні бути нейтралізовані системою ПД (C-UAS) під час реалізації комплексу заходів із використанням спеціалізованих та неспеціалізованих засобів ПД (C-UAS), що плануються та реалізуються діями військ (сил) для виконання відповідних завдань.

Обмеження. Основним змістом оцінювання ефективності ПД (C-UAS) у ході прогнозування є аналіз варіантів побудови комплексу відповідних заходів захисту та застосування системи ПД (C-UAS) щодо вибору варіанта сукупності сил та засобів і порядку виконання ними спланованих дій, спрямованих на досягнення мети застосування, тобто отримання потрібного позитивного результату, що визначається за певним критерієм, наприклад, не менше ніж заданий окремий чи узагальнений кількісний показник.

Особливістю оцінювання ефективності ПД (C-UAS) у ході проведення відповідних досліджень є те, що частина завдань може бути оцінена:

частково (в основному) реально щодо C-UAS та з імітацією дій сил і засобів противника UAS;

в основному з використанням моделей дій UAS – БпЛА з КЗУ та C-UAS – захисту військового об’єкта від КЗУ з ЛСН.

У будь-якому разі повинно бути оцінено дії сил та засобів із ПД (C-UAS) щодо нейтралізації дій сил та засобів UAS противника, а не збіг обставин або нерезультативність засобів UAS противника, що залишили в працездатному стані об'єкти ураження.

Доцільність введення в систему ПД БпАК із КЗУ складових, між якими потрібно організовувати взаємодію, розглянуто на прикладі корисності космічної системи (КС) або комплексу оптико-електронних перешкод (КОЕП) за результатами дослідження необхідної та достатньої умов таких введень.

Судження *X:* "Необхідно ввести складову (КС, КОЕП) до комплексної системи захисту військових об'єктів (ВО) від БпАК противника (системи C-UAS)".

Необхідна умова *P*: "Ефективність C-UAS (E_C) нижче мінімальної припустимої ($E_{C\min n}$)".

Достатня умова *Q*: "Введення засобу (КС, КОЕП) до системи C-UAS додає ефективність $E_З$, достатню за внеском у E_C".

Згідно з аналізом відомостей щодо побудови систем комплексного захисту від високоточної зброї з КЗУ [19], можна стверджувати, що системи C-UAS можуть бути створені за деяким j -варіантом ($j = 1 - J$) за ознакою складу сил і засобів, що реалізують наведені методи інформаційного забезпечення, радіоелектронного та фізичного впливу.

Вимогою до системи C-UAS є те, що в певних, визначених діями БпАК та системи, умовах обстановки ефективність C-UAS E_{Cj} повинна бути не нижче мінімально припустимої – $E_{C\min n}$ для забезпечення захисту ВО від БпАК із КЗУ:

$$E_{Cj} \geq E_{C\min n}. \tag{1}$$

У разі невиконання умови (1) отримуємо $E_{Cj} < E_{C\min n}$, що визначає об'єктивне виникнення та наявність необхідної умови *P*.

Формування вихідних даних для визначення наявності (можливості створення) достатньої умови *Q* потребує дослідження різниці:

$$\Delta E_Q = E_{C\min n} - E_{Cj}, \tag{2}$$

де ΔE_Q – брак ефективності системи, створеної за *j*-м варіантом складу сил та засобів, порівняно з величиною, що визначає потрібну ефективність.

Дослідження ΔE_Q повинно забезпечувати правильне встановлення обставин виникнення умови *P* і формування вихідних даних для аналізу умови *Q*.

За результатами дослідження може бути встановлено, що всі складові системи C-UAS у j -му варіанті складу сил і засобів функціонують із повною реалізацією можливостей, а ΔE_Q обумовлений діями противника, яким не можливо протидіяти через відсутність (брак) відповідних засобів.

Наприклад: застосування противником певної кількості КЗУ з ЛСН, що доставляються РУ БпЛА, яким не можливо протидіяти через відсутність засобу – КОЕП;

зміна противником районів зосередження (військових об'єктів) зусиль РУ БпАК у застосуванні (перегрупування, зміна дислокації підрозділів), які не можливо своєчасно

виявити через відсутність засобу – КС.

За подібними результатами дослідження ΔE_Q визначається актуальність умови Q, але її наявність потребує підтвердження:

$$E_З \geq \Delta E_Q . \quad (3)$$

Виконання (3) свідчить про наявність достатньої умови Q. Виконанням умов P і Q підтверджується правильність судження X: "Необхідно ввести складову (КС, КОЕП) до комплексної системи захисту ВО від БпАК противника (системи C-UAS)".

Організація комплексної протидії РУ БпАК, озброєних КЗУ з ЛСН, потребує певного науково-методичного забезпечення. У табл. 4 наведено варіанти можливих станів системи ПД на етапах функціонування та результати системного аналізу потрібних заходів щодо протидії РУ БпАК, озброєних КЗУ з ЛСН.

Таблиця 4

Варіанти можливих станів системи ПД на етапах функціонування та результати системного аналізу

Вихідний стан засобів C-UAS	Заходи, що виконують	Наступний стан
1. Початок роботи C-UAS	Розвідка елементів БпАК	2. БпАК не виявлено
1а. РР систем управління		
1б. КР елементів бойового порядку		
1в. РЛР БпЛА (КЗУ)		
1г. РТР РЕЗ		
1д. АкР БпЛА (двигунів)		
1е. ОЕР БпЛА		
1ж. ОВР БпЛА		
2. БпАК не виявлено (інформація про нього відсутня)	Чергування C-UAS	3. Контроль стану C-UAS
3. Контроль стану C-UAS	Перевірка готовності C-UAS	4. Контроль готовності ПД БпАК
4. Контроль готовності ПД БпАК	Перевірка готовності ПД БпАК	5. ПД БпАК готовий до роботи
5. ПД БпАК готовий до роботи	Підтримання готовності ПД БпАК	1. Початок роботи C-UAS
6. БпАК виявлено	Приведення в готовність C-UAS до здійснення впливів на елементи БпАК	7. C-UAS впливів у готовності
7. C-UAS впливів у готовності	Електронне забезпечення РЕП БпАК	8. Застосування засобів РЕБ
7а. Готовність засобів ОЕП КЗУ		
7б. Готовність засобів РП РЕЗ каналів навігації (КН)		
7в. Готовність засобів РП РЕЗ каналів управління (КУ)		
7г. Готовність засобів спуфінгу		
7д. Готовність засобів ОЕП каналів спеціальної інформації (КСІ)		

Кінець таблиці 4

Вихідний стан засобів C-UAS	Заходи, що виконують	Наступний стан
8. Застосування засобів РЕБ	РЕП	9. РЕЗ БпАК подавлено
8а. КН подавлено		
8б. КУ подавлено		
8в. КСІ подавлено		
8г. Спуфінг проведено		
9. РЕЗ БпАК подавлено	Приведення елементів C-UAS у вихідний стан	16. C-UAS у вихідному стані
7. C-UAS вплив у готовності	Інформаційне забезпечення вогневого ураження (ВУ) елементів БпАК	10. Застосування засобів ВУ
7е. Готовність ВУ		
10. Застосування засобів ВУ	ВУ елементів БпАК	11. Елементи БпАК уражено
10а. ВУ наземних елементів		
10б. ВУ наземних БпЛА		
10в. ВУ КЗУ БпЛА		
11. Елементи БпАК уражено	Приведення елементів C-UAS у вихідний стан	16. C-UAS у вихідному стані
7. C-UAS вплив у готовності	Інформаційне забезпечення механічного пошкодження елементів БпАК	12. Застосування механічних засобів
7ж. Готовність механічного впливу		
12. Застосування механічних засобів	Механічний вплив на елементи БпАК	13. БпАК механічно пошкоджено
12а. Застосування тарана		
12б. Застосування сіток		
13. БпАК механічно пошкоджено	Приведення елементів C-UAS у вихідний стан	16. C-UAS у вихідному стані
7. C-UAS вплив у готовності	Інформаційне та електронне забезпечення застосування КОЕП ЛСН	14. Застосування КОЕП ЛСН
14. Застосування КОЕП ЛСН	Оптико-електронне подавлення ЛСН КЗУ	15. КЗУ ЛСН нейтралізовано
14а. ЛСН виявлено		
14б. КЗУ відведено		
15. КЗУ ЛСН нейтралізовано	Приведення елементів C-UAS у вихідний стан	16. C-UAS у вихідному стані
16. C-UAS у вихідному стані	Перевірка готовності ПД БпАК	5. ПД БпАК готовий до роботи

На рис. 1 зображено мережеву модель варіанта застосування засобів C-UAS, що взаємодіють для ефективного функціонування кожної підсистеми (виявлення, радіоелектронного впливу, вогневого ураження тощо) та досягнення загального ефекту ПД – нейтралізації БпЛА противника і КЗУ з ЛСН, запущених ними. Колами позначено стани засобів C-UAS, що визначаються подіями (етапами протидій), які потребують виконання в системі заходів ПД, що позначено стрілками.

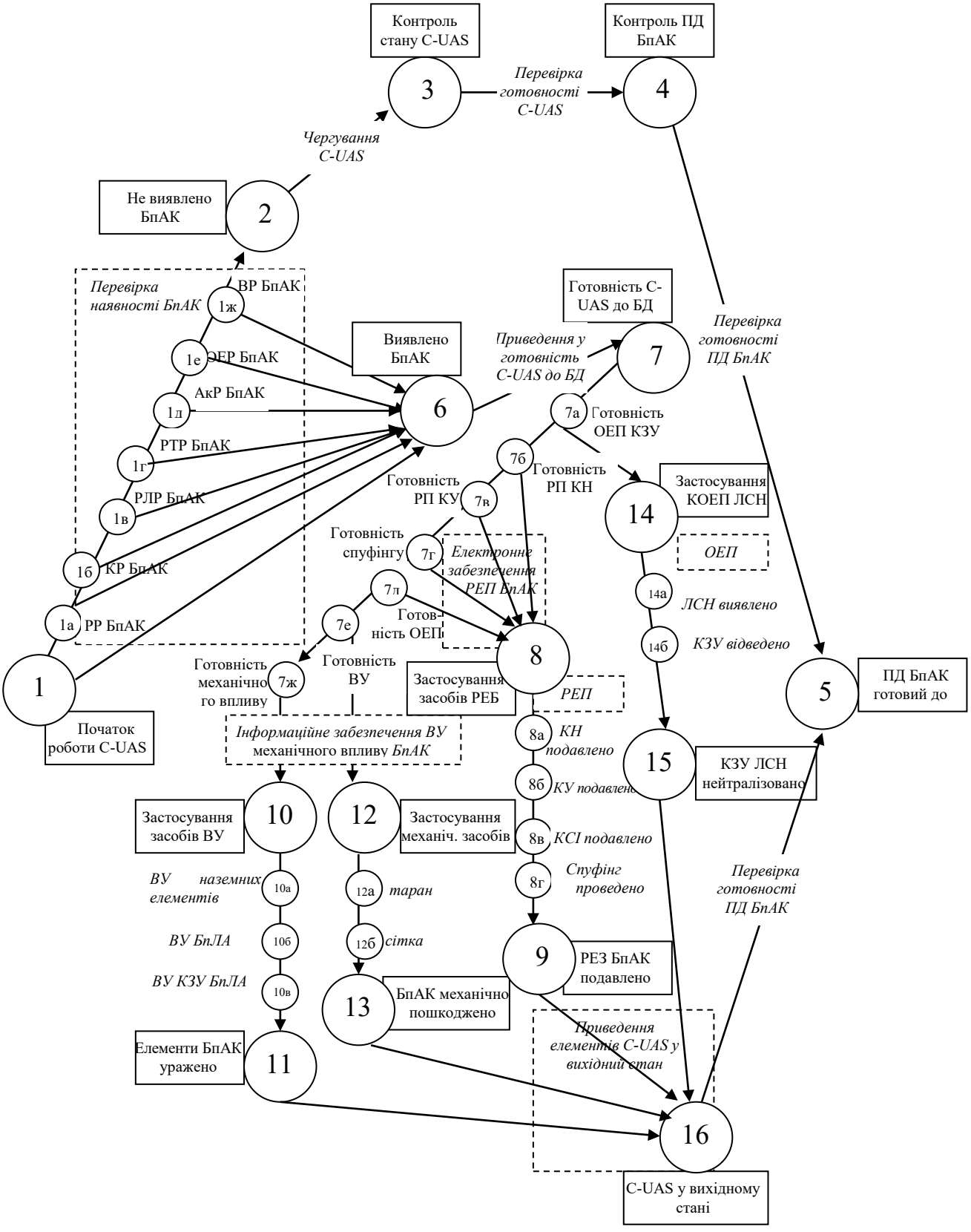


Рис. 1. Мережева модель варіанта застосування засобів С-UAS

Висновки. Запропонований підхід визначає завдання, зміст, складові, принципи, оцінювання засобів С-UAS захисту за внеском в ефективність системи захисту об’єкта від РУ (ударних) БпАК противника, що систематизує знання в предметній галузі та створює передумови для практичного застосування результатів досліджень щодо проблем сучасної збройної боротьби.

Описаний підхід передбачає проведення подальших досліджень щодо уточнення математичних розрахунків відповідно до особливостей військ (сил), військового об'єкта, системи захисту від РУ (ударних) БпАК противника та зразків військової техніки, які входять до її складу.

СПИСОК ЛІТЕРАТУРИ

1. Drone Databook Updata. March 2020. URL: https://https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/ (last accessed: 02.12.2020).
2. Нужны ли Бундесверу боевые дроны? URL: https://www.dw.com/ru/%D0%BD%D1%83%D0%B6%D0%BD%D1%8B-%D0%BB%D0%B8%D0%B1%D1%83%D0%BD%D0%B4%D0%B5%D1%81%D0%B2%D0%B5%D1%80%D1/%83%D0%B1%D0%BE%D0%B5%D0%B2%D1%8B%D0%B5%D0%B4%D1%80%D0%BE/%D0%BD%D1%8B/a-53418088 (дата обращения: 02.12.2020).
3. Воєнна розвідка України має докази використання Росією на території України майже всіх типів БпЛА, які є на озброєнні в ЗС РФ. URL: https://www.mil.gov.ua/news/2020/10/12/voenna-rozvidka-ukraini-mae-dokazi-vikoristannya-rosieyu-na-teritorii-ukraini-majzhe-vsih-tipiv-bpla-yaki-e-na-ozbroenni-v-zs-rf/ (дата звернення: 02.12.2020).
4. Війна в Карабасі: уроки для України та її армії. URL: https://www.radiosvoboda.org/a/viyna-v-karabasi-uroky-dlya-ukrainy-ta-yiyi-armiyi/30939727.html (дата звернення: 02.02.2021).
5. Unmanned system integrated roadmap fy 2013-2038. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf (дата звернення: 02.12.2020).
6. Surakartta (Bukovel) anti-uav defence system / Spetstechnoexport.com; Proximus.com.ua; Kvertus // Unmanned Aerial Vehicles and Anti-UAV Defence Systems : Catalogue. 2020. URL: https://spetstechnoexport.com/system/documents/attachments/000/000/050/original/06-Unmanned_Aerial_Vehicles_and_Anti-UAV_Defence_Systems_WEB_2020_NEW.pdf?1583309637 (last accessed: 02.12.2020).
7. Візія Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років. URL: https://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi-10-rokiv/ (дата звернення: 22.07.2020).
8. Рекомендації з оборонного планування на основі спроможностей у Міністерстві оборони України та Збройних Силах України. URL: www.mil.gov.ua./diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/plani-ukraina-2020/rekomendaczii-z-oboronnogo-planuvannya-na-osnovi-spromozhnostej-v-ministerstvi-oboroni-ukraini-ta-zbrojnih-silah-ukraini.html (дата звернення: 22.07.2020).
9. Thomas S. Kuhn. The Structure of Scientific Revolutions. Vol. II. (Foundations of the Unity of Science). The University of Chicago Press, 1970. ISBN 0-226-45803-2. 210 p.
10. Тлумачний словник з інформатики / Г. Г. Півняк, Б. С. Бусигін, М. М. Дівізінюк та ін. Дніпро : Нац. гірнич. ун-т, 2010. 600 с.
11. Радиоэлектронная борьба в Вооружённых Силах Российской Федерации – 2018. URL: https://informost.ru (дата обращения: 02.12.2020).

12. Борисов Е. Г., Евдокимов В. И. Высокоточное оружие и борьба с ним : учеб. пособ. СПб. : Изд-во «Лань», 2013. 496 с.: ил.
13. BAYKAR Unmanned Aerial Vehicle system. URL: baykardefence. com. Tr (last accessed: 02.12.2020).
14. MAM-C Mini Akilli Muhimmat – Roketsan. URL: https://www.roketsan.com.tr/urun/mam-c-mini-akilli-muhimmat (last accessed: 02.12.2020).
15. Joseph Trevethinck and Thomas Nevdic. Everything We Know About The Fighting That Has Erupted Between Armenia And Azerbaijan. URL: https://www.thedrive.com/the-war-zone/36777/everything-we-know-about-the-fighting-that-has-erupted-between-armenia-and-azerbaijan (дата звернення: 02.12.2020).
16. Комплексный подход к противодействию высокоточному оружию // Национальная оборона. Ноябрь 2020. № 11. URL: https://oborona.ru/includes/periodics/ /defense/2014/0507/193513251/detail.shtml (дата обращения: 02.12.2020).
17. Средства и комплексы радиоэлектронной борьбы с БпЛА. Станция радиоэлектронной борьбы КС беспилотными летальными аппаратами “Гроза-С”. Комплекс для защиты стратегических объектов от мультикоптеров “Гроза-З”. URL: https:// www.kbradar.by (дата обращения: 02.12.2020).
18. Рудиков С. И. Комплекс постановки помех высокоточному оружию с лазерными системами наведения полуактивного типа. URL: https://cyberleninka.ru/article/n/kompleks-postanovki-pomeh-vysokotochnomu-oruzhiyu-s-lazernymi-sistemami-navedeniya-poluaktivnogo-tipa (дата обращения: 02.12.2020).
19. Шлома Л. В. Способ защиты группового объекта от высокоточного оружия с лазерной системой наведения (варианты) : патент РФ № 2401411C2. URL: https://findpatent.ru/patent/240/2401411.html (дата обращения: 02.12.2020).
20. Про затвердження Порядку застосування зброї і бойової техніки з'єднаннями, військовими частинами і підрозділами Збройних Сил під час виконання ними завдань у районі проведення антитерористичної операції у мирний час : постанова Кабінету Міністрів України від 14.02.2018 № 68. URL: https://zakon.rada.gov.ua/laws/show/68-2018-%D0%BF#Text (дата звернення: 02.12.2020).
21. Що таке НЕЙТРАЛИЗАЦІЯ // Словник іншомовних слів. URL: https:// slovopedia.org.ua (дата звернення: 02.12.2020).
22. Протидія безпілотним авіаційним комплексам : метод. посіб. Київ : НУОУ, 2016. 28 с.

Подано 24.12.2020

REFERENCES

1. Drone Databook Updata. (March 2020). Retrieved from https://https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/.
2. Nuzhny li Bundesveru boevye drony? [Does the Bundeswehr need combat drones?]. (n.d.). Retrieved from https://www.dw.com/ru/%D0%BD%D1%83%D0%B6%D0%BD%/D1%8B%D0%BB%D0%B8%D0%B1%D1%83%D0%BD%D0%B4%D0%B5%D1%81%D0%/B2%D0%B5%D1%80%D1%83%D0%B1%D0%BE%D0%B5%D0%B2%D1%8B%D0%B5%/D0%B4%D1%80%D0%BE%D0%BD%D1%8B/a-53418088 [in Russian].
3. Voienna rozvidka Ukrainy maie dokazy vykorystannia Rosiieiu na terytorii Ukrainy maizhe vsikh typiv BpLA, yaki ye na ozbroienni v ZS RF [Ukraine's military intelligence has evidence

of Russia's use in Ukraine of almost all types of UAVs in service with the Russian Armed Forces.]. (n.d.). Retrieved from https://www.mil.gov.ua/news/2020/10/12/voenna-rozvidka-ukraini-mae-dokazi-vikoristannya-rosieyu-na-teritorii-ukraini-majzhe-vsih-tipiv-bpla-yaki-e-na-ozbroenni-v-zs-rf/ [in Ukrainian].

4. Viina v Karabasi: uroky dlia Ukrainy ta yii armii [The war in Karabakh: lessons for Ukraine and its army]. (n.d.). Retrieved from https://www.radiosvoboda.org/a/viyna-v-karabasi-uroky-dlya-ukrainy-ta-yiyi-armiyi/30939727.html [in Ukrainian].

5. Unmanned system integrated roadmap fy 2013-2038. (n.d.). Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf.

6. Surakartta (Bukovel) Anti-UAV defence system / Spetstechnoexport.com; Proximus.com.ua; Kvertus (2020). *Unmanned Aerial Vehicles and Anti-UAV Defence Systems : Catalogue.* Retrieved from https://spetstechnoexport.com/system/documents/attachments/000/000/050/original/06-Unmanned_Aerial_Vehicles_and_Anti-UAV_Defence_Systems_WEB_2020_NEW.pdf?/1583309637.

7. Viziia Heneralnoho shtabu ZS Ukrainy shchodo rozvytku Zbroinykh Syl Ukrainy na naiblyzhchi 10 rokiv [Vision of the General Staff of the Armed Forces of Ukraine on the development of the Armed Forces of Ukraine for the next 10 years]. (n.d.). Retrieved from https://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi-10-rokiv/ [in Ukrainian].

8. Rekomendatsii z oboronnoho planuvannia na osnovi spromozhnosteў u Ministerstvi oborony Ukraïny ta Zbroyўnykh Sylakh Ukrainy [Recommendations on capability-based defense planning in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine]. (n.d.). Retrieved from www.mil.gov.ua. /diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/plani-ukraina-2020/rekomendaczii-z-oboronnogo-planuvannya-na-osnovi-spromozhnostej-v-ministerstvi-oboroni-ukraini-ta-zbrojnih-silah-ukraini.html [in Ukrainian].

9. Thomas S. Kuhn. (1970). *The Structure of Scientific Revolutions*. Vol. II. (Foundations of the Unity of Science). The University of Chicago Press. ISBN 0-226-45803-2.

10. Pivniak, H. H., Busyhin, B. S., & Diviziniuk, M. M., et al. (2010). *Tlumachnyi slovnyk z informatyky [Explanatory dictionary of computer science]*. Dnipro: Nats. hirnych. un-t [in Ukrainian].

11. Radioelektronnaia bor'ba v Vooruzhennykh Silakh Rossiiskoi Federatsii [Electronic warfare in the Armed Forces of the Russian Federation]. (2018). Retrieved from https://informost.ru [in Russian].

12. Borisov, E. G., & Evdokimov, V. I. (2013). *Vysokotochnoe oruzhie i bor'ba s nim [Precision weapons and the fight against them]*. Saint Petersburg [in Russian].

13. BAYKAR Unmanned Aerial Vehicle system. (n.d.). Retrieved from baykardefence. com. Tr.

14. MAM-C Mini Akilli Muhimmat – Roketsan. (n.d.). Retrieved from https://www.roketsan.com.tr/urun/mam-c-mini-akilli-muhimmat.

15. Joseph Trevethinck and Thomas Nevdic. Everything We Know About The Fighting That Has Erupted Between Armenia And Azerbaijan. (n.d.). Retrieved from https://www.thedrive.com/the-war-zone/36777/everything-we-know-about-the-fighting-that-has-erupted-between-armenia-and-azerbaijan.

16. Kompleksnyi podkhod k protivodeistviiu vysokotochnomu oruzhiiu [An integrated approach to countering precision weapons]. (2020). *Natsional'naia oborona [National defense], 11*.

Retrieved from https://oborona.ru/includes/periodics/defense/2014/0507/193513251/detail.shtml [in Russian].
17. Sredstva i kompleksy radioelektronnoi bor'by s BpLA. Stantsiia radioelektronnoi bor'by KS bespilotnymi letal'nymi apparatami “Groza-S”. Kompleks dlia zashchity strategicheskikh ob"ektov ot mul'tikopterov “Groza-Z”. [Means and complexes of electronic warfare against UAVs. Electronic warfare station KS unmanned aerial vehicles "Groza-S". Complex for the protection of strategic objects from multicopters "Groza-Z"]. (n.d.). Retrieved from https:// www.kbradar.by [in Russian].
18. Rudikov, S. I. (n.d.). Kompleks postanovki pomekh vysokotochnomu oruzhiiu s lazernymi sistemami navedeniia poluaktivnogo tipa [Complex for jamming high-precision weapons with semi-active laser guidance systems]. Retrieved from https://cyberleninka.ru/article/n/kompleks-postanovki-pomeh-vysokotochnomu-oruzhiyu-s-lazernymi-sistemami-navedeniya-poluaktivnogo-tipa [in Russian].
19. Shloma, L. V. (n.d.). *Sposob zashchity gruppovogo ob"ekta ot vysokotochnogo oruzhiia s lazernoĭ sistemoĭ navedeniia (varianty) [Method of protecting a group object from precision weapons with a laser guidance system (options)]: patent RF № 2401411S2.* Retrieved from https://findpatent.ru/patent/240/2401411.html [in Russian].
20. Pro zatverdzhennia Poriadku zastosuvannia zbroi i boiovoi tekhniky ziednanniamy, viiskovymy chastynamy i pidrozdilamy Zbroinykh Syl pid chas vykonannia nymy zavdan u raioni provedennia antyterorystychnoi operatsii u myrnyi chas [About the statement of the Order of application of the weapon and military equipment by connections, military units and divisions of Armed forces during performance by them of tasks in the area of carrying out anti-terrorist operation in peacetime] : postanova Kabinetu Ministriv Ukrainy vid 14.02.2018 № 68 [the resolution of the Cabinet of Ministers of Ukraine from 02/14/2018 № 68.]. Retrieved from https://zakon.rada.gov.ua/laws/show/68-2018-%D0%BF#Text [in Ukrainian].
21. Shcho take NEITRALYZATSIIA [What is NEUTRALIZATION]. *Slovnyk inshomovnykh sliv [Dictionary of foreign words]*. Retrieved from https:// slovopedia.org.ua [in Ukrainian].
22. *Protydiia bezpilotnym aviatsiinym kompleksam [Countering unmanned aerial vehicles]*. (2016). Kyiv: NDUU [in Ukrainian].

D. A. Ishchenco, V. A. Kyryliuk,S. D. Ishchenco, L. M. Maryshchuk

PARADIGM OF RESISTANCE TO INTELLIGENCE AND IMPACT UNLIMITED AIRCRAFT COMPLEXES

The work shows the relevance of the problem of countering reconnaissance and strike unmanned aircraft systems and the need to improve the scientific and methodological support of its solution according to a certain corresponding paradigm.

In the work as a paradigm of countering unmanned aerial systems, it is proposed to consider a conceptual theoretical and methodological model of combating unmanned aerial vehicles, which currently provides opportunities for identifying the problems of developing forces and means of countering unmanned aerial systems.

The developed paradigm of counteraction can be an element of scientific and methodological support, contributes to the solution of the problem of the complex use of forces and means of counteraction to reconnaissance and strike unmanned aircraft systems in order to

acquire the capabilities of troops (forces) to perform tasks as intended in the conditions of the use of unmanned vehicles.

The recognition of such a paradigm by specialists determines that their activities are based on the accepted model of countering unmanned aircraft systems, using the same rules and standards established in the industry. The generality and consistency of approaches that they provide are prerequisites for ensuring the required scientific level of a certain direction of research.

The proposed approach outlines the tasks, content, components, principles of assessment of means of counteraction to unmanned aerial vehicles by contributing to the effectiveness of the system of protection of the object from reconnaissance and strike (shock) systems of the enemy, which systematizes knowledge in the subject area. problems of modern armed struggle.

The prospect of further research is to clarify the mathematical calculations in accordance with the characteristics of troops (forces), military facility, protection system against reconnaissance and strike (strike) unmanned aerial vehicles of the enemy and samples of military equipment that are part of it.

Keywords: *unmanned aerial systems, model of combating unmanned aerial vehicles, paradigm of counteraction to reconnaissance and attack unmanned aerial systems.*

УДК 621.396.969.181.4 DOI: 10.46972/2076-1546.2020.18.09

М. В. Бугайов, С. П. Самойлик

РОЗШИРЕННЯ МЕЖ ОДНОЗНАЧНОГО ВИМІРЮВАННЯ ДАЛЬНОСТІ Й РАДІАЛЬНОЇ ШВИДКОСТІ ШЛЯХОМ ВИКОРИСТАННЯ ПАЧОК БАГАТОКОМПОНЕНТНИХ СИГНАЛІВ

У ході проєктування імпульсно-доплерівських радіолокаційних станцій одним із ключових моментів є вибір періоду повторення імпульсів, який визначає межі однозначного вимірювання дальності й радіальної швидкості та створює суперечність у вимірюванні цих величин. Особливо гостро вона проявляється в разі аналізу сигналів, відбитих від гвинтів, турбін та пропелерів літальних апаратів. Основними підходами до вирішення завдання розширення меж однозначного вимірювання дальності та радіальної швидкості є використання вобуляції періоду повторення імпульсів і створення ансамблів сигналів для їх розділення за формою. Формування ансамблю зондуючих сигналів для імпульсної радіолокаційної станції необхідно проводити з урахуванням як взаємокореляційних, так і автокореляційних властивостей. Запропоновано підхід до формування пачок багатокомпонентних сигналів із можливістю розділення імпульсів усередині пачки. Кожен з імпульсів у пачці утворюється шляхом додавання деякої кількості сигналів з лінійною частотною модуляцією, які відрізняються значенням амплітуди та девіації частоти. У разі збільшення девіації частоти амплітуда складової зменшується. Зменшення коефіцієнта взаємної кореляції багатокомпонентних сигналів із утвореного ансамблю можна досягти збільшенням кількості компонент кожного сигналу. Розмір ансамблю сигналів, який можна утворити на основі багатокомпонентних сигналів з лінійною модуляцією частоти, залежить від вимог, що висуваються до коефіцієнта взаємної кореляції та автокореляційної функції сигналів. Показано, що для розширення меж вимірювання координат за фіксованої довжини хвилі необхідно збільшувати кількість імпульсів у пачці. Результати проведених досліджень свідчать про потенційну можливість використання запропонованого багатокомпонентного сигналу з лінійною модуляцією частоти для формування пачок імпульсів з їх подальшим розділенням.

Ключові слова: *період повторення імпульсів; радіолокаційна станція; багатокомпонентний сигнал; пачка сигналів; лінійна частотна модуляція; автокореляційна функція.*

Постановка проблеми в загальному вигляді. Вибір відповідного періоду повторення імпульсів (ППІ) є дуже важливим для проєктування радіолокаційної станції (РЛС), оскільки визначає межі однозначного вимірювання дальності й радіальної швидкості та створює протиріччя у вимірюванні цих величин. У значній мірі це стосується імпульсно-доплерівських РЛС, у яких ППІ визначає межі однозначного вимірювання частотного зсуву прийнятого сигналу. Оскільки в останній час спостерігається підвищений інтерес до аналізу “тонкої” структури прийнятого сигналу [1], що зумовлений, зокрема, модуляційними ефектами гвинтів, турбін та пропелерів літальних апаратів і відповідним розширенням спектра [2], то суперечність однозначних вимірювань ще більше загострюється.

Аналіз останніх досліджень і публікацій. Питанням розширення меж однозначного вимірювання дальності та радіальної швидкості в імпульсних РЛС присвячено значну кількість публікацій [1−10]. У дослідженнях [1−2] розглядається проблема вибору ППІ з урахуванням ефектів вторинної модуляції сигналу для розпізнавання аеродинамічних цілей та боротьби з імітуючими перешкодами. У роботах [3−9] запропоновано різні схеми побудови пачок зондуючих імпульсів на основі ступінчатої зміни несучої частоти, міжімпульсного кодування та вобуляції ППІ. У роботі [10] проведено детальний аналіз стану проблеми стосовно систем селекції рухомих цілей (СРЦ). Отже, аналіз відомих методів вирішення проблеми розширення меж однозначного вимірювання дальності та радіальної швидкості з одночасним підвищенням перешкодозахищеності РЛС є актуальним завданням сучасної радіолокації.

Формулювання завдання дослідження. Метою статті є дослідження можливостей використання багатокомпонентних сигналів із лінійною частотною модуляцією (ЛЧМ) для формування пачок імпульсів з можливістю їх подальшого розділення шляхом узгодженої фільтрації, що дасть змогу незалежно розширювати межі вимірювання як дальності, так і радіальної швидкості.

Виклад основного матеріалу

Аналіз підходів до вирішення проблеми однозначності вимірювань координат. Усунення невизначеності вимірювання дальності та радіальної швидкості досягається застосуванням модуляції параметрів послідовностей або пачок імпульсів і визначенням фазового зсуву модуляції відбитого сигналу. Модуляція може здійснюватися зміною ППІ (безперервно або дискретно), зміною несучої частоти (за лінійним або гармонічним законом) або застосуванням певних форм імпульсної модуляції (широтно-імпульсної, фазо-імпульсної або амплітудно-імпульсної). Вибір виду модуляції проводиться залежно від характеру застосування РЛС і накладених на неї обмежень.

У загальному випадку там, де необхідне точне вимірювання дальності, а роздільна здатність за дальністю мала порівняно з ППІ (використання широкосмугових зондуючих сигналів), застосовують системи з багатьма частотами повторення імпульсів. Використання кількох фіксованих ППІ потребує послідовного неоднозначного вимірювання дальності на кожній частоті повторення з наступним порівнянням результатів вимірювання із виключенням неоднозначності [8−9].

Якщо ж роздільна здатність за дальністю одного порядку порівняно з ППІ (застосування вузькосмугових зондуючих сигналів), то можна використовувати дві різні несучі частоти. Наприклад, одна несуча частота може бути використана для парних номерів імпульсів, а інша – для непарних (різниця між частотами відносно мала). Різниця фаз між відбитими від цілі сигналами на різних частотах пропорційна відстані до цілі і дає змогу вимірювати цю відстань [8]. Системи з частотною модуляцією використовують тоді, коли важлива простота апаратури [9].

У разі СРЦ у РЛС з постійним ППІ мають місце так звані “сліпі” швидкості на частотах Доплера $f_D = \pm k/T$ ($k = 0,\ 1,\ 2\ldots$), оскільки на цих частотах фаза відбитого сигналу від рухомої цілі за період повторення імпульсів T змінюється в $2\pi k$ рази. Для виключення цього явища зазвичай використовують вобуляцію (модуляцію) періоду повторення зондуючих сигналів (період слідування імпульсів може змінюватися від

імпульсу до імпульсу або від пачки до пачки), що призводить до розмивання швидкісної характеристики системи СРЦ і зменшує таким чином кількість і глибину провалів результуючої швидкісної характеристики. Визначення фазового зсуву вобуляції відбитого сигналу дозволить уникнути неоднозначності вимірювання дальності.

Вибір закону вобуляції проводиться, у загальному випадку, за критерієм максимізації коефіцієнта підзавадової видимості з урахуванням мінімуму пульсацій амплітудно-частотної характеристики (АЧХ) фільтра в смузі пропускання. Найчастіше використовують лінійний, перехресний та випадковий види вобуляції.

Розрахунки й моделювання показують, що вобуляція періоду T приводить до зменшення провалів АЧХ нерекурсивних і рекурсивних фільтрів, проте при цьому відбувається звуження смуги режекції фільтра в разі одночасного розширення та спотворення спектра перешкод. Тому ефективність подавлення пасивних перешкод погіршується [9].

Системи з безперервною зміною ППІ навряд чи взагалі можна застосовувати, зважаючи на високий рівень випадкових заважаючих сигналів і пов'язаних із цим труднощів.

Перспективним, але мало дослідженим напрямком вирішення даної проблеми є використання малих значень ППІ із розділенням імпульсів за кодовими ознаками протягом періоду виявлення. Це дозволить позбутися неоднозначності визначення дальності та збільшити кількість імпульсів у пачці без сповільнення огляду. Більша гнучкість забезпечується в разі використання деяких видів стиснення імпульсів, що дозволяють досягти необхідної роздільної здатності за дальністю або точністю за умови довших імпульсів і більш низьких рівнів пікової потужності [10].

Лінійне розділення сигналів. Залежно від параметрів сигналу, що використовуються для їх розділення (селекції), застосовують такі види розділення: просторове, часове, частотне, фазове, амплітудне, а також комбіновані способи, що ґрунтуються на їх поєднанні (просторово-часове, амплітудно-частотне, розділення за формою).

Теорія лінійної селекції сигналів становить значний інтерес в радіолокації. У РЛС доводиться застосовувати її в разі розділення сигналів від кількох цілей, коли необхідно зменшити взаємний заважаючий вплив систем, та боротьби з навмисними перешкодами нешумового типу [8].

Розглянемо теорію лінійної селекції сигналів щодо створення набору (ансамблю) сигналів для формування пачок зондуючих імпульсів. При цьому введемо обмеження на скінченну кількість імпульсів у пачці і на те, що фільтр для кожного імпульсу зі створеного ансамблю повинен реагувати на "свій" сигнал і не реагувати на решту. На практиці немає необхідності досягати повної рівності нулю ефекту дії не "своїх" сигналів. Важливо лише те, щоб сумарний ефект дії цих сигналів був малим порівняно з ефектом дії "свого" сигналу.

Щоб сигнали можна було розділити, вони повинні задовольняти певні умови. Необхідною і достатньою є умова їх лінійної незалежності.

Згідно з теоремою функцій дійсної змінної, щоб функції $u_0(t)$, $u_1(t)$,..., $u_l(t)$, визначені на інтервалі $[-\tau_i/2, \tau_i/2]$, були лінійно незалежними, необхідно і достатньо, щоб не дорівнював нулю визначник Грама:

$$G\left[u_0(t), u_1(t), ..., u_l(t)\right] = \begin{vmatrix} a_{11} & a_{12} & ... & a_{1l} \\ a_{21} & a_{22} & ... & a_{2l} \\ ... & ... & ... & ... \\ a_{l1} & a_{l2} & ... & a_{ll} \end{vmatrix} \neq 0, \quad (1)$$

елементи якого визначають за такою формулою:

$$a_{ij} = \int_{-\tau_i/2}^{\tau_i/2} u_i(t) u_j(t) dt, \quad \text{де} \quad i, j = 1, 2, 3, ..., l. \quad (2)$$

Визначник Грама не дорівнює нулю, зокрема для ортогональної системи функцій, а для ортонормованої – завжди дорівнює одиниці. Іншими словами, будь-які ортогональні (ортонормовані) сигнали завжди можна розділити.

У радіолокації розділення сигналів зазвичай проводиться за наявності шуму, тому намагаються використовувати ортогональні сигнали. Якщо сигнали лінійно незалежні, але не ортогональні, то їх розділення пов'язане з погіршенням відношення сигнал-шум. Чим більша кількість сигналів розділяється, тим більше погіршується дане значення. Ортогональні сигнали розділяються без погіршення відношення сигнал-шум.

Проте вибір ансамблю сигналів для РЛС є більш складною задачею, ніж для систем зв'язку та навігації. У РЛС зондуючий сигнал повинен мати задану автокореляційну функцію (АКФ), тому вибір ансамблю зондуючих сигналів для РЛС необхідно проводити з урахуванням як взаємокореляційних (для надійного розділення сигналів), так і автокореляційних (для однозначного та точного вимірювання параметрів) властивостей.

Розглянемо можливі підходи до побудови ансамблів сигналів.

1. Використання слабокорельованих послідовностей із кодуванням фази. Фазоманіпульовані (ФМн) сигнали порівняно з частотно-модульованими (ЧМ) сигналами вимагають складної системи формування та обробки. Крім того, для ФМн сигналів складно враховувати спотворення спектральних складових сигналу на шляху поширення за значної ширини спектра сигналу. Для ЧМ сигналів у кожен момент часу випромінюється одна спектральна складова, і тому простіше враховувати ефекти на трасі поширення.

2. Застосування процедур ортогоналізації, наприклад, Грама-Шмідта, Гівенса або Хаусхолдера. Дані процедури потребують додаткових обчислювальних затрат у разі цифрового формування сигналів. Крім того, АКФ сигналів після їх ортогоналізації потребує проведення додаткових досліджень.

3. Використання ансамблів ортогональних сигналів, сформованих на основі систем ортонормованих функцій (поліноми Лежандра, Чебишева, Ерміта, Лагерра). АКФ сигналів, побудованих на основі даних поліномів, мають значний рівень бічних пелюсток (рівень першої бічної пелюстки становить 0,4) і досить малу швидкість їх спадання.

Враховуючи вказані вище особливості побудови наборів сигналів, розглянемо можливості використання сигналів із лінійною модуляцією частоти та багатокомпонентних ЛЧМ сигналів для формування їх ансамблів.

Формування пачок багатокомпонентних сигналів. Перед розглядом ансамблів багатокомпонентних сигналів розглянемо кореляційні властивості ансамблю ЛЧМ

сигналів. Два ЛЧМ сигнали з досить добрими кореляційними властивостями можна записати у такому вигляді:

$$u_1(t)=\cos\left(2\pi f_0+\frac{\pi\Delta f}{\tau_i}t^2\right),\quad u_2(t)=\cos\left(2\pi f_0-\frac{\pi\Delta f}{\tau_i}t^2\right), \tag{3}$$

де Δf − девіація частоти.

Ці сигнали займають одну і ту ж смугу частот, але мають протилежний закон зміни частоти. Характер поведінки взаємокореляційної функції при цьому описується такою формулою:

$$\rho_{12}=1\Big/\sqrt{\tau_i\Delta f}\,. \tag{4}$$

Тобто кореляція обернено пропорційна кореню з бази сигналу. Це дещо гірше, ніж у кодів, утворених за допомогою псевдовипадкових послідовностей.

Ансамбль ЛЧМ сигналів можна отримати, використовуючи сигнали, що відрізняються значенням девіації частоти Δf, яка може бути як додатною, так і від'ємною. Значення взаємної кореляції двох сигналів із такого ансамблю за великих значень добутку $\tau_i\left|\Delta f_i-\Delta f_j\right|$ описується виразом

$$\rho_{ij}\ \Big/\sqrt{\tau_i\left|\Delta f_i-\Delta f_j\right|}\,. \tag{5}$$

З виразу (5) видно, що для забезпечення добрих кореляційних властивостей ансамблю ЛЧМ сигналів необхідно відповідним чином обрати величину $\Delta f_i-\Delta f$. Чим більше максимально допустиме в системі значення $\Delta f_{\max}$, тим більшу кількість слабокорельованих ЛЧМ сигналів можна побудувати.

Ансамбль багатокомпонентних ЛЧМ сигналів можна записати в такому вигляді:

$$u_0(t,\alpha_0,\beta_0),u_1(t,\alpha_1,\beta_1),...,u_L(t,\alpha_L,\beta_L), \tag{6}$$

де α_i − коефіцієнт, що визначає амплітуду складових сигналу;

β_i − коефіцієнт, що визначає девіацію частоти складових сигналу;

L − розмірність ансамблю сигналів.

Кожен із сигналів ансамблю можна описати таким виразом:

$$u_i(t,\alpha_i,\beta_i)=\left[\sum_{n=0}^{N-1}\alpha_i^n\cos\left(\pi\frac{\Delta f\beta_i^n t^2}{\tau_i}\right)\right]\cdot\sum_{n=0}^{N-1}\alpha_i^{-n},\quad t\le\left|\frac{\tau_i}{2}\right|, \tag{7}$$

де N − кількість компонент сигналу;

n − номер складової сигналу;

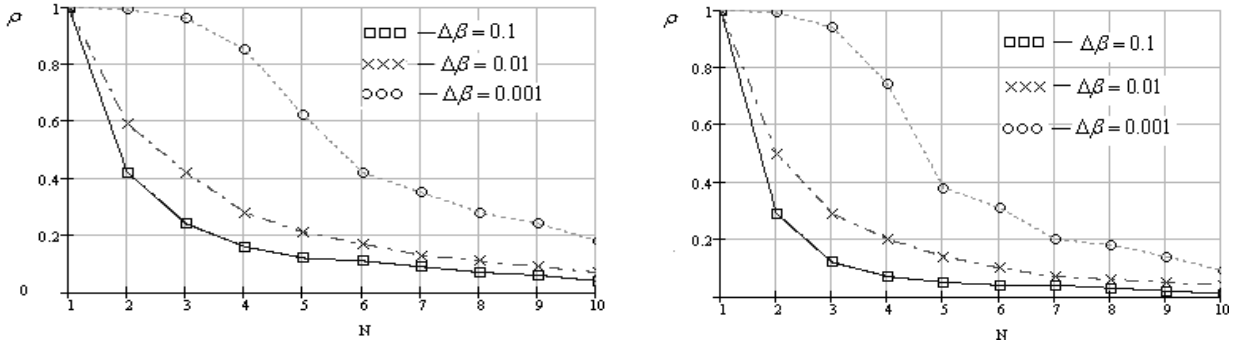
$\sum_{n=0}^{N-1}\alpha_i^{-n}$ − нормуючий множник.

Запишемо вираз для визначення коефіцієнта взаємної кореляції ρ_{ij} двох багатокомпонентних ЛЧМ сигналів:

$$\rho_{ij} = \frac{1}{E}\int_{-\tau_i/2}^{\tau_i/2} u_i\left(t,\alpha_i,\beta_i\right)u_j\left(t,\alpha_j,\beta_j\right)dt, \tag{8}$$

де E – енергія сигналу.

Проаналізуємо значення коефіцієнта ρ_{ij} залежно від кількості складових сигналу N за різних значень коефіцієнтів β і фіксованого значення коефіцієнта α. На рис. 1а показано залежність коефіцієнта взаємної кореляції ρ_{ij} у разі $\alpha = 1,4$ і початкового значення $\beta = 1,35$. Аналіз кривих показує, що збільшення кількості компонент сигналу приводить до зменшення кореляції між сигналами. Також збільшення розносу значень коефіцієнта $\Delta\beta$ і, відповідно, збільшення розносу в ширині спектрів багатокомпонентних сигналів спричиняє зменшення коефіцієнта ρ_{ij}. Це пояснюється меншим перекриттям спектрів відповідних сигналів унаслідок більшого розширення спектра одного багатокомпонентного сигналу порівняно з іншим через більше значення коефіцієнта β. На рис. 1б показано аналогічну залежність для сигналів із параметрами $\alpha = 2,0;\ \beta = 1,45$. З порівняльного аналізу графіків залежностей коефіцієнта кореляції (рис. 1а, б) можна зробити висновок, що зменшення коефіцієнта взаємної кореляції двох багатокомпонентних сигналів можна досягти збільшенням кількості компонент N, розносу ширини спектрів сигналу за рахунок збільшення $\Delta\beta$ або початкових значень параметрів сигналу α і β.



а) *б)*

Рис. 1. Залежність коефіцієнта взаємної кореляції ρ двох багатокомпонентних ЛЧМ сигналів: а) для $\alpha = 1,4;\ \beta = 1,35$; б) для $\alpha = 2,0;\ \beta = 1,45$

Варто зазначити, що коефіцієнт взаємної кореляції є досить нечутливим до зміни коефіцієнта α в разі зміни кількості складових сигналу й фіксованого значення β. Навіть за $N = 10$ і рознесення $\Delta\alpha = 0,1$ коефіцієнт кореляції перевищує рівень 0,9.

У роботі [11] проведено аналіз АКФ багатокомпонентного ЛЧМ сигналу залежно від кількості складових сигналу та коефіцієнтів, що визначають амплітуду й девіацію частоти. Також показано, що лише для певних значень пар коефіцієнтів α і β максимальний рівень бічних пелюсток $F_{\max}$ досягає свого мінімального значення (табл. 1). Причому це досягається в разі кількості складових сигналу $N = 5$. Подальше збільшення N зумовлює

незначне підвищення рівня бічних пелюсток АКФ, проте спостерігається розширення основної пелюстки АКФ в області низької кореляції (утворюється п'єдестал).

Таблиця 1

Оптимальні значення параметрів α і β

α	0,4	0,6	0,8	1,0	1,2	1,4	1,6	1,8	2,0	2,2	2,4
β	0,65	0,75	0,79	1,25	1,3	1,35	1,4	1,4	1,45	1,5	1,5
$F_{\max}$	0,053	0,04	0,048	0,06	0,05	0,042	0,035	0,035	0,042	0,05	0,05

Оцінимо можливість утворення ансамблю багатокомпонентних ЛЧМ сигналів із добрими кореляційними властивостями. Сформуємо набір із 6 багатокомпонентних сигналів відповідно до табл. 1:

$$u_0(t,\alpha_0,\beta_0),\ u_1(t,\alpha_1,\beta_1),\ u_2(t,\alpha_2,\beta_2),\ u_3(t,\alpha_3,\beta_3),\ u_4(t,\alpha_4,\beta_4), u_5(t,\alpha_5,\beta_5), \tag{9}$$

де

$$\alpha_0 = 1,00;\ \beta_0 = 1,25;\ \alpha_1 = 1,10;\ \beta_1 = 1,27;\ \alpha_2 = 1,20;\ \beta_2 = 1,30;$$
$$\alpha_3 = 1,30;\ \beta_3 = 1,33;\ \alpha_4 = 1,4;\ \beta_4 = 1,35;\ \alpha_5 = 1,50;\ \beta_5 = 1,40.$$

Розрахуємо значення коефіцієнтів кореляції всіх пар сигналів даного ансамблю та обчислимо визначник Грама відповідно до формули (1):

$$G\left[u_0(t), u_1(t), ..., u_5(t)\right] = \begin{vmatrix} 1,00 & 0,33 & 0,26 & 0,23 & 0,23 & 0,20 \\ 0,33 & 1,00 & 0,25 & 0,19 & 0,19 & 0,14 \\ 0,26 & 0,25 & 1,00 & 0,18 & 0,18 & 0,13 \\ 0,23 & 0,19 & 0,18 & 1,00 & 0,19 & 0,12 \\ 0,23 & 0,19 & 0,18 & 0,19 & 1,00 & 0,12 \\ 0,20 & 0,14 & 0,14 & 0,12 & 0,12 & 1,00 \end{vmatrix} = 0,634. \tag{10}$$

Оскільки значення визначника Грама не дорівнює нулю, то сигнали утвореного ансамблю можна розділити шляхом узгодженої фільтрації. Як бачимо з виразу (10), максимальна кореляція спостерігається між $u_0(t)$ та $u_1(t)$ і становить 0,33, а мінімальна – між $u_3(t)$ і $u_5(t)$; $u_4(t)$ і $u_5(t)$ − 0,12.

Розмір ансамблю сигналів, який можна утворити на основі багатокомпонентних сигналів, залежить від вимог, що висуваються до коефіцієнта взаємної кореляції та АКФ сигналів. Крім того, даний ансамбль можна розширити удвічі за рахунок використання багатокомпонентних ЛЧМ сигналів із різними знаками девіації частоти.

Даний підхід до розділення сигналів можна використати для формування пачок сигналів, коли необхідно вимірювати як дальність до об'єкта, так і його радіальну швидкість у широких межах. Зокрема, спектр сигналу, відбитого від аеродинамічної цілі, що має гвинти, турбіни або пропелери, містить багато спектральних ліній і є досить широким. Позначимо ППІ, необхідний для однозначного вимірювання радіальної швидкості, $T_{\min}$, а дальності − $T_{\max}$ (рис. 2).

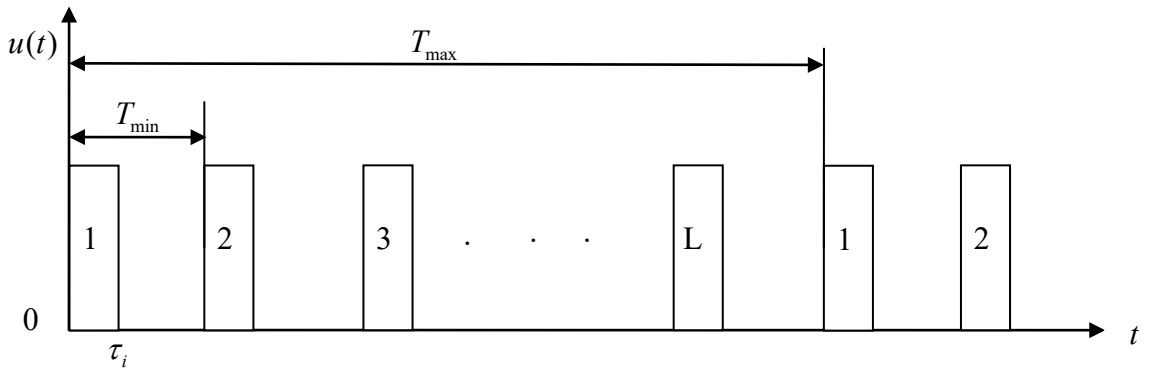


Рис. 2. Пачка багатокомпонентних сигналів

Тоді кількість імпульсів у пачці можна визначити як відношення максимального ППІ до мінімального ППІ:

$$L = \frac{T_{\max}}{T_{\min}} = \frac{8}{c\lambda} \cdot R_{\max} \upsilon_{R\max}, \tag{11}$$

де c – швидкість поширення електромагнітних хвиль;

λ – робоча довжина хвилі;

$R_{\max}$ – максимальне очікуване значення дальності до цілі;

$\upsilon_{R\max}$ – максимальне очікуване значення радіальної швидкості цілі.

Із виразу (11) видно, що з розширенням меж вимірювання координат у разі фіксованої довжини хвилі необхідно збільшувати кількість імпульсів у пачці.

Висновки. Результати проведених досліджень свідчать про потенційну можливість використання запропонованого багатокомпонентного ЛЧМ сигналу для формування пачок імпульсів з їх подальшим розділенням. Наведено залежність коефіцієнта взаємної кореляції багатокомпонентних сигналів залежно від обраних параметрів та надано рекомендації щодо формування ансамблів сигналів. Перспективним є дослідження використання запропонованого підходу для підвищення перешкодостійкості системи, оскільки зміна від імпульсу до імпульсу форми зондуючого сигналу дасть змогу підвищити відношення сигнал-шум у результаті накопичення сигналів у разі дії імітуючих перешкод.

СПИСОК ЛІТЕРАТУРИ

1. Chen V. C. The Micro-Doppler Effect in Radar. ARTECH HOUSE, 2011. 309 p.

2. Гейстер С. Р. Адаптивное обнаружение распознавание с селекцией помех по спектральным портретам. Минск : Военная академия РБ, 2000. 172 с.

3. Levanon N. Stepped-frequency pulse-train radar signal // IEE Proceedings - Radar Sonar and Navigation. 2002. 149 (6). P. 297−309. DOI: 10.1049/ip-rsn:20020432

4. Rasool S. B., Bell M. R. Efficient Pulse-Doppler Processing and Ambiguity Functions of Nonuniform Coherent Pulse Trains // IEEE Radar Conference. 2010. P. 1150−1155.

5. Levanon N. Mitigation Range Ambiguity in High PRF Radar using Inter-Pulse Binary Coding // IEEE Trans. Aerosp. Electron. Syst. 2009. Vol. 45, No. 2. P. 687−697.

6. Bystrov N. E. et al. Range and Doppler Ambiguity Elimination in Coherent Radar using Quasicontinuous Signals // Journal of Mechanical Engineering Research and Developments. 2017. Vol. 40, No. 4. P. 37−46.
7. Rosli S. J. Design of Binary Coded Pulse Trains with Good Autocorrelation Properties for Radar Communications // MATEC Web of Conferences. 2018. Vol. 150. P. 1−5. doi.org/10.1051/matecconf/201815006016
8. Richards M. A. Principles of Modern Radar. Vol. I: Basic Principles. SciTech Publishing, 2010. 962 p.
9. Gini F., Maioand D. A., Patton L. Waveform Design and Diversity for Advanced Radar Systems. The Institution of Engineering and Technology, London, United Kingdom, 2012. 571 p.
10. Gaspare Galati. Advanced Radar Techniques and Systems. London, Peter Peregrinus Ltd, 1993. 1013 p.
11. Даник Ю. Г., Бугайов М. В., Поздняков П. В. Зниження рівня бічних пелюсток автокореляційної функції багатокомпонентного сигналу з лінійною модуляцією частоти // Системи управління, навігації та зв'язку. 2013. № 3. С. 31−36.

Подано 25.09.2020

REFERENCES

1. Chen, V. C. (2011). *The Micro-Doppler Effect in Radar.*
2. Geister, S. R. (2000). *Adaptivnoe obnaruzhenie raspoznavanie s selektsiei pomekh po spektral'nym portretam [Adaptive detection-recognition with interference selection based on spectral portraits]*. Minsk [in Russian].
3. Levanon, N. (2002). Stepped-frequency pulse-train radar signal. *IEE Proceedings - Radar Sonar and Navigation, 149* (6), 297−309. http://dx.doi.org 10.1049/ip-rsn:20020432
4. Rasool, S. B., & Bell, M. R. (2010). Efficient Pulse-Doppler Processing and Ambiguity Functions of Nonuniform Coherent Pulse Trains. In *IEEE Radar Conference*. (pp. 1150−1155).
5. Levanon, N. (2009). Mitigation Range Ambiguity in High PRF Radar using Inter-Pulse Binary Coding. *IEEE Trans. Aerosp. Electron. Syst*, *Vol. 45,* No. 2, 687−697.
6. Bystrov, N. E. et al. (2017). Range and Doppler Ambiguity Elimination in Coherent Radar using Quasicontinuous Signals. *Journal of Mechanical Engineering Research and Developments, Vol. 40,* No. 4, 37−46.
7. Rosli, S. J. (2018). Design of Binary Coded Pulse Trains with Good Autocorrelation Properties for Radar Communications In *MATEC Web of Conferences, Vol. 150,* 1−5. https://doi.org 10.1051/matecconf/201815006016
8. Richards, M. A. (2010). *Principles of Modern Radar. Vol. I: Basic Principles.* SciTech Publishing.
9. Gini, F., Maioand, D. A., & Patton, L. (2012). *Waveform Design and Diversity for Advanced Radar Systems.* The Institution of Engineering and Technology, London, United Kingdom.
10. Gaspare Galati. (1993). *Advanced Radar Techniques and Systems.* London, Peter Peregrinus Ltd.
11. Danyk, Yu. H., Buhaiov, M. V., & Pozdniakov, P. V. (2013). Znyzhennia rivnia bichnykh peliustok avtokoreliatsiinoi funktsii bahatokomponentnoho syhnalu z liniinoiu moduliatsiieiu

chastoty [Decreasing the level of side lobes of the autocorrelation function of a multicomponent signal with linear frequency modulation]. *Systemy upravlinnia, navihatsii ta zv'iazku [Control, navigation and communication systems], 3,* 31−36 [in Ukrainian].

M. V. Buhaiov, S. P. Samoilyk

RANGE AND RADIAL VELOCITY MEASUREMENT AMBIGUITY ELIMINATION WITH TRAINS OF MULTICOMPONENT SIGNALS

When designing pulse-Doppler radar, one of the key points is the choice of the pulse repetition period, which determines the boundaries of unambiguous measurement of range and radial velocity and creates contradictions in the measurement of these values. This contradiction is especially acute in the analysis of signals reflected from the propellers and turbines of aircraft. The main approaches to solving the problem of expanding the boundaries of unambiguous measurement of range and radial velocity is the use of variable pulse repetition period and the creation of signal ensembles to separate them by shape. Generation of an ensemble of sounding signals for a pulsed radar must be carried out taking into account both cross-correlation and auto-correlation properties. An approach to the generation of multicomponent signal trains with the possibility of pulse separation inside the train is proposed. Each of the pulses in the train is formed by adding a number of chirp signals, which differ in the values of amplitude and frequency deviation. As the frequency deviation increases, the amplitude of the component decreases. Reducing the cross-correlation coefficient of multicomponent signals from the formed ensemble can be achieved by increasing the number of components of each signal. The size of the signal ensemble, which can be formed on the basis of multicomponent chirp signals, depends on the requirements for the cross-correlation coefficient and auto-correlation function of the signals. It is shown that in order to expand the limits of coordinate measurement at a fixed wavelength, it is necessary to increase the number of pulses in the train. The results of the research demonstrate the potential possibility of using the proposed multicomponent chirp signal to form train of pulses with its subsequent separation.

Keywords: *pulse repetition period, radar station, multicomponent signal, signal train, linear frequency modulation, autocorrelation function.*

УДК: 044.056:004.93'1 DOI: 10.46972/2076-1546.2020.18.10

І. В. Гуменюк, М. С. Басараба, О. В. Некрилов

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНИХ КОМПОНЕНТІВ МЕРЕЖ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Встановлено, що ефективність та надійність функціонування інформаційно-телекомунікаційних систем, зокрема мереж, які входять до їх складу, суттєво залежить від високого рівня захищеності критичних компонентів. Разом з тим постійне удосконалення технічного оснащення даних систем вимагає створення нового та покращення наявного методичного забезпечення кібернетичної безпеки. Одним із перспективних підходів вважається розроблення універсальної методики забезпечення кібербезпеки в умовах здійснення кібернетичних атак (впливів, загроз тощо) та несанкціонованого доступу неавторизованими користувачами до критичних вузлів (компонентів) мереж інформаційно-телекомунікаційної системи.

Своєчасне виявлення, оперативна протидія кібернетичним загрозам та несанкціонованому доступу до критичних компонентів мереж є необхідною складовою забезпечення високого рівня кібербезпеки інформаційно-телекомунікаційної системи в цілому, особливо в умовах ведення гібридної війни та збройної агресії з боку Російської Федерації, що обумовлює необхідність розроблення відповідного методичного забезпечення. З цією метою у статті запропоновано методику забезпечення кібербезпеки критичних компонентів мереж інформаційно-телекомунікаційної системи, в основу якої покладено: комплексне застосування контролю стану мережевих вузлів та доступу користувачів до них; фіксування фактів здійснення кібернетичних атак на підставі аналізу вхідного (вихідного) трафіка; своєчасне виявлення кібернетичних загроз та скоєння несанкціонованого доступу; оперативну протидію цим спробам.

У роботі наведено результати верифікації запропонованої методики. Показано, що її застосування дозволяє оперативно виявляти факти здійснення кібернетичних загроз та несанкціонованого доступу до критичних компонентів мереж інформаційно-телекомунікаційних систем, а також ефективно протидіяти цим спробам.

Ключові слова: *критичний компонент; мережа; інформаційно-телекомунікаційна система; кібербезпека; кібернетична атака; несанкціонований доступ; система виявлення вторгнень.*

Постановка проблеми в загальному вигляді. Інформаційний сектор завжди викликав великий інтерес у кіберзлочинних угруповань. За останніх п’ять років кібератаки здійснювалися на держустанови, сферу науки (освіти), фінансову, промислову та військову галузі [1]. Прикладом тому є значна кількість проведених атак у світі: кібератака хакерського угруповання Angels_Of_Truth (квітень – травень 2016 року, Канада); кібератака типу “credential stuffing” (початок 2019 року, США та Японія); кібератака типу “blackout” (березень 2019 року, Венесуела); серія нетиповий кібератак на банківський та енергетичний сектор (лютий 2020 року, Російська Федерація). В Україні в умовах складної та недостатньо стабільної політико-економічної ситуації такі випадки також мають місце.

Наприклад, кібератака на інфраструктурні об'єкти держави (грудень 2015 року, Прикарпаття, Київська, Чернівецька області); кібератака на внутрішні телекомунікаційні мережі (грудень 2016 року, Міністерство фінансів України); масштабна кібернетична атака російських хакерів (червень 2018 року); понад 10 тисяч різних видів кібератак виявлено та заблоковано (травень – червень 2020 року). Отже, в умовах, що склалися, актуальним є завдання розроблення нових ефективних та удосконалення відомих методів протидії кібернетичним атакам та несанкціонованому доступу (НСД).

Виходячи з даних передумов, сформульовано **мету** статті, яка полягає в розробленні методики забезпечення кібербезпеки критичних компонентів мережі інформаційно-телекомунікаційної системи (ІТС).

Аналіз останніх досліджень і публікацій. На сьогодні вже розроблено та реалізовано низку сучасних методів захисту інформації ІТС. Авторами у [2] розглянуто сучасні системи виявлення вторгнень у комп'ютерних системах; у [3] проаналізовано наявні протоколи та методи маршрутизації потоків даних; у [4] досліджено системи захисту інформації, які реалізовують аналіз, моніторинг, контроль мережевих потоків ІТС; у [5] розглянуто та проаналізовано основні можливості, принципи (механізми) функціонування систем виявлення атак; у [6] описано системи виявлення атак та їх технологічні особливості; у [7] подано теоретичний аналіз сучасних систем виявлення вторгнень, які забезпечують захист інформаційних систем та мереж.

Отже, результати аналізу науково-практичних джерел свідчать про те, що для вирішення завдань захисту ІТС розроблено достатню кількість науково-методичного та практичного забезпечення. Проте універсальній методиці захисту ІТС в умовах здійснення кібератак та НСД у науковій літературі не присвячено належної уваги.

Постановка завдання. Для мережі ІТС з N інформаційними вузлами необхідно розробити дієву методику, яка забезпечить відповідний рівень кібербезпеки її критичних компонентів. Топологію цієї мережі описує зв'язний граф $G=(V,E)$, де V – вузли (критичні компоненти), а E – ребра (канали зв'язку). Аналіз вхідного та вихідного трафіка мережі проводиться постійно. Рівень забезпечення кібербезпеки прийматимемо за нормований показник з межами $[0.1;0.9]$.

Виклад основного матеріалу. Забезпечення надійного захисту інформації, важливих компонентів ІТС є комплексним завданням, яке включає в себе сукупність взаємопов'язаних задач. Саме тому для досягнення мети завдання запропоновано методику, яка складається з таких кроків:

постійний контроль стану мережевих вузлів та каналів зв'язку мережі ІТС;

фіксування фактів здійснення кібернетичних атак із детальним описом рівня небезпеки загроз;

постійний контроль доступу користувачів до мереж ІТС;

своєчасне виявлення НСД до мережі ІТС та кіберзагроз, а також оперативна протидія їм.

Детально розглянемо кожен із кроків.

Етап 1. Постійний контроль стану мережевих вузлів та каналів зв'язку мережі ІТС. Оскільки важливим завданням управління мереж є підтримання функціональності та надійності кожного мережевого компонента, то для ІТС необхідно використовувати

ієрархічне управління, розподіливши мережу на окремі кластери (зони) з виділенням їх контролерів, вузлів-шлюзів і внутрішніх вузлів.

Множина N вузлів мережі ІТС розподіляється на k кластерів, які локально мінімізовані за відстанню між інформаційною точкою та центрами кластерів. Цільова функція алгоритму розраховується за формулою

$$J = \sum_{h=1}^{k} \sum_{v_i \in V_h} \left\| v_i - \mu_h \right\|^2 , \tag{1}$$

де μ_h – значення центрів кластера.

Цільова функція є локально мінімізованою для усіх кластерів (кожна точка з набору об'єктів знаходитися на мінімальній відстані від центра кластера, до якого вона належить). Вибір відповідного кластера для заданої точки в процесі роботи алгоритму обумовлений у такий спосіб:

$$\left\| v_i - \mu_h \right\|^2 = min \left\{ \left\| v_i - \mu_h \right\|^2 \right\}_{h=1}^{k} . \tag{2}$$

При цьому кожен кластер містить однакову кількість внутрішніх вузлів. Визначаємо опорну мережу контролерів кластерів та вузли-шлюзи, які формують віртуальну магістраль усієї мережі, що використовується як для передачі маршрутної інформації, так і для користувацького трафіка. Проаналізуємо процедуру формування основних елементів мережі.

Визначення контролерів кластерів. Територіально розподілені на непересічні кластери абоненти за відомими методами на максимальному енергетичному рівні (усі вузли знаходяться в зоні дії хоча б одного доступного вузла) розсилають HELLO-повідомлення з метою визначення доступності усіх вузлів з урахуванням метрики кожного кластера. За отриманими відповідями кожний вузол визначає максимально можливу кількість вузлів, які можуть бути підключені до нього, та формує таблицю зв'язності. Вузли один одному, зокрема через транзитні (HOP-повідомлення), відправляють Cluster-повідомлення. У такий спосіб визначається вузол як потенційно можливий контролер кластера із максимальним ступенем зв'язаності (кількістю підключених до нього вузлів). Контролер кластера, у свою чергу, розсилає повідомлення кожному вузлу кластера, формуючи нову таблицю маршрутизації.

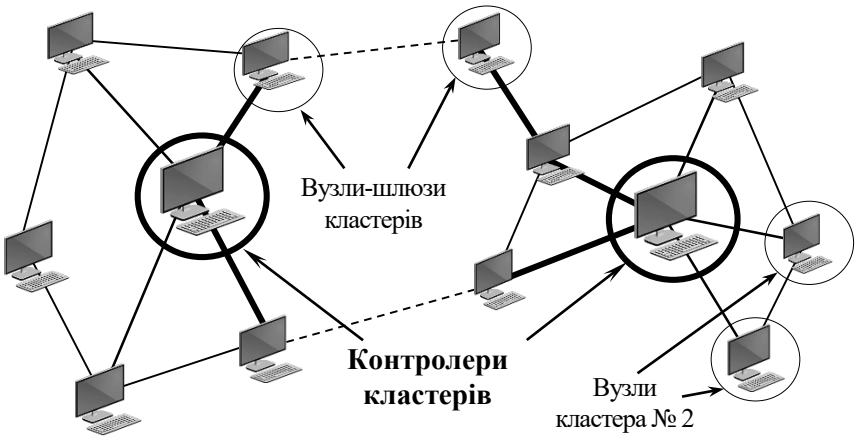


Рис. 1. Визначення контролерів кластерів та вузлів-шлюзів мережі

Визначення вузлів-шлюзів. Вузли різних кластерів з урахуванням однакової метрики мережі розсилають один одному, зокрема й через транзитні вузли, повідомлення для визначення відстаней між ними.

У такий спосіб вони формують тимчасову таблицю маршрутизації, у якій міститься інформація про відповідні відстані. Вузли різних кластерів з мінімальними значеннями відстаней визначаються як потенційно можливі вузли-шлюзи (див. рис. 1). Ці вузли формують власні таблиці маршрутизації до потенційних контролерів та шлюзів інших кластерів [8].

Для постійної підтримки актуальності таблиць маршрутизації та цілісності топології мережі контролери кластерів періодично розсилають вузлам інформацію про стан каналів. В умовах успішного проведення кібератаки на вузол кластера (він визначається як потенційно небезпечний) здійснюється його фізична ізоляція (рис. 2). Такий підхід ефективний для забезпечення кібербезпеки іншого кластера.

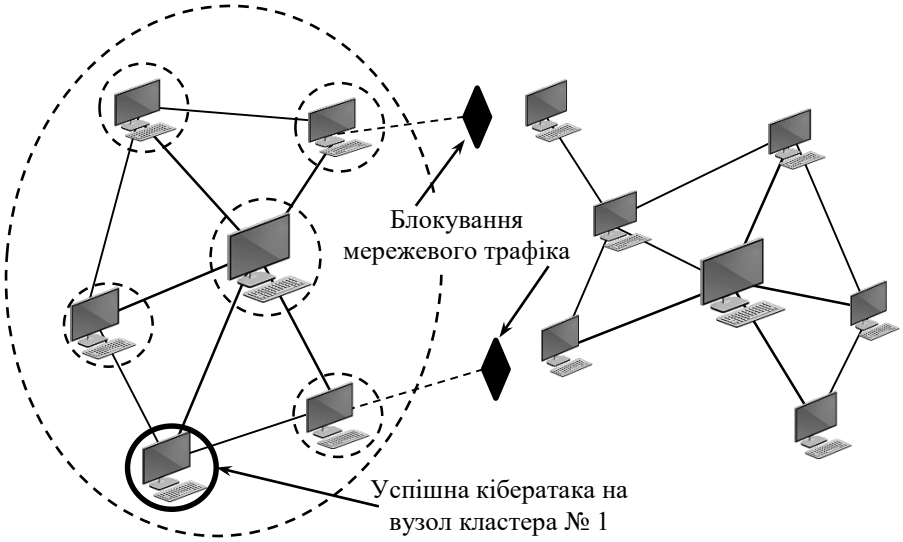


Рис. 2. Фізична ізоляція потенційно небезпечного кластера

Етап 2. Фіксування фактів здійснення кібернетичних атак із детальним описом рівня небезпеки загроз. На даному кроці проводиться аналіз вхідного (вихідного) трафіка кластерів мережі, зокрема з використанням наявної системи виявлення вторгнень Intrusion Detection System (IDS). У результаті виконання поточного кроку визначаються рівні безпеки мережі: допустимий (трафік містить певну загрозу, однак може фільтруватися) та небезпечний (вхідний трафік блокується для подальшого проходження в мережу). Свого пікового значення кібербезпека мережі ІТС набуватиме за умови застосування багаторівневого захисту.

Етап 3. Постійний контроль доступу користувачів до мереж ІТС. На даний момент розвитку інформаційних технологій парольні, які базуються на унікальній персональній інформації, та атрибутні методи ідентифікації втрачають свою актуальність, проте користуються великим попитом серед користувачів. Порівняно з цими методами біометричні характеристики користувача як спосіб автентифікації можуть гарантувати підвищений рівень безпеки, враховуючи особливості біометричних даних конкретної особи.

Для забезпечення перевірки автентичності користувачів на даному етапі реалізовують такі заходи.

Виявлення та локалізація геометрії обличчя користувача на зображенні відеопотоку. Для пошуку форми (геометрії) обличчя на зображенні систем відеоспостереження використано алгоритм Віоли – Джонса. Як правило, цей пошук відбувається швидко, проте інтелектуальне вивчення ознак класифікатором проводиться тривалий час.

У разі використання даного методу відеозображення подається в інтегральному вигляді (матриця значень сумарної яскравості) для підвищення оперативності аналітичних обчислень та розрахунків:

$$L(x,y)=\sum_{i=0}^{i\le x}\sum_{j=0}^{j\le y} I(i,j), \tag{3}$$

де $I(i,j)$ – значення яскравості пікселя на зображенні.

Кожен елемент $L(x,y)$ відповідає сумі пікселів, які знаходяться в певному прямокутнику. При цьому для вхідного відеопотоку проводиться нормалізація зображення за масштабом, яскравістю тощо.

Обчислення набору базових ознак (характеристик) зображення. Основними принципами, на яких ґрунтується метод Віоли – Джонса, є використання базових понять теорії розпізнавання об'єктів, зокрема ознак (примітивів) Хаара, застосування їх каскаду для аналізу результату ідентифікації. Усі ознаки надходять на вхід класифікатора та обробляються з деяким підсиленням, так званим "бустингом" (*від англ.* boost – вдосконалення, посилення) [9].

Ознаки (примітиви) Хаара – це відображення f:

$$\chi \Rightarrow D_f, \tag{4}$$

де D_f – множина допустимих значень ознаки.

За умови, що ознаку $f_1,...,f_n$ визначено, вираз (4) набуде такого вигляду:

$$\chi \Rightarrow \{f_1,...,f_n\}, \tag{5}$$

який називають ознакою опису об'єкта.

Порівняння обчислених ознак з еталонними, що містяться в базі даних.

Загальну структуру контролю доступу користувачів до мереж ІТС наведено на рис. 3.

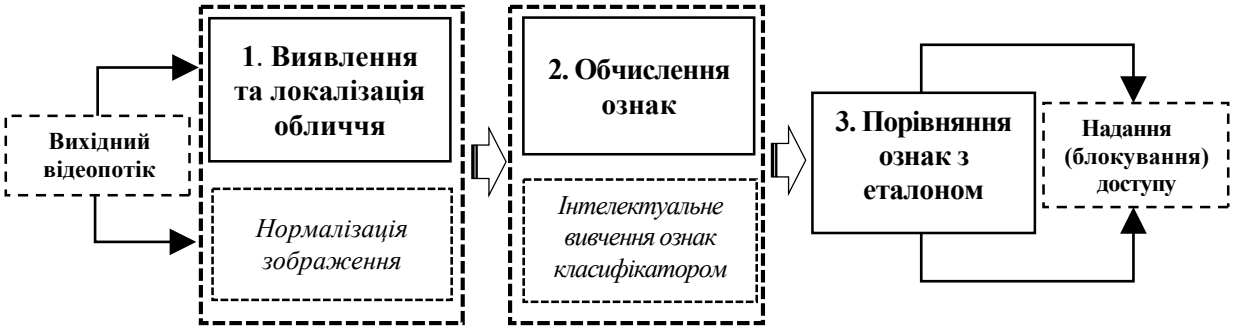


Рис. 3. Структура контролю доступу користувачів до мереж ІТС

За умови скоєння кібератак та/або НСД до мереж ІТС виконується ***своєчасне їх виявлення й оперативна протидія цим спробам та кіберзагрозам.*** Останній етап методики ґрунтується на узагальненні інформації про кіберзагрози або скоєння НСД, зокрема: власне сам факт здійснення кібернетичних атак (час, "компонент-жертва", нова або повторна загроза тощо); деталізований опис рівня небезпеки загрози.

Верифікацію запропонованої методики проведено на мережі ІТС, яка складається з 12 кластеризованих вузлів, кожен із яких умовно приймається за критичний компонент. Топологію вихідної мережі наведено на рис. 4, її характеристику – у табл. 1. Тестовими типами атак обрано user-to-root (U2R) та PROBE.

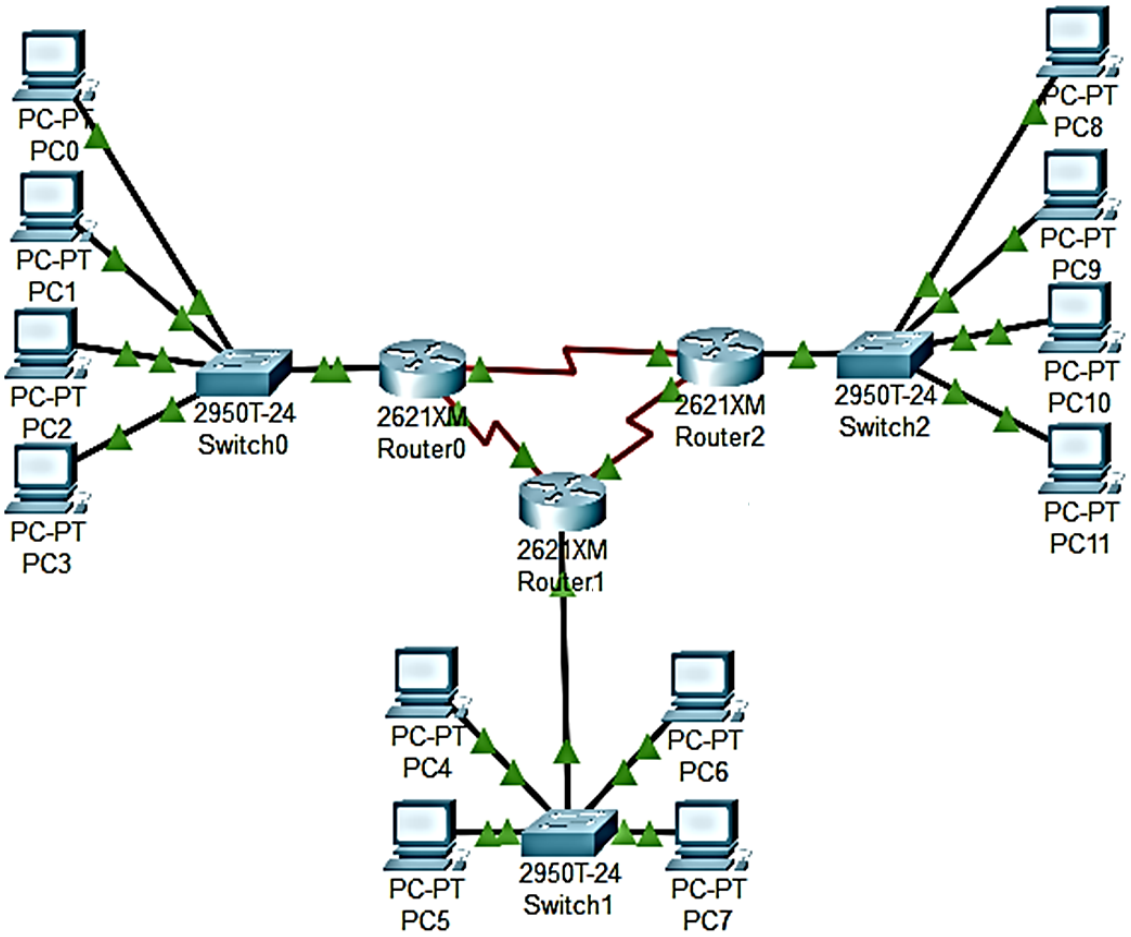


Рис. 4. Структура вихідної мережі ІТС

Таблиця 1

Характеристика досліджуваної мережі

Номер мережевого вузла	Наявність [+] та відсутність [-] компонентів забезпечення кібербезпеки		
	Контроль стану вузлів та каналів зв'язку	Система виявлення вторгнень	Контроль доступу користувачів
Кластер № 1 (Switch 0 – вузол-шлюз; Router 0 – контролер кластера)			
№ 1, PC 0	+	-	-
№ 2, PC 1	+	-	-
№ 3, PC 2	+	-	-
№ 4, PC 3	+	-	-

Продовження таблиці 1

Номер мережевого вузла	Наявність [+] та відсутність [-] компонентів забезпечення кібербезпеки		
	Контроль стану вузлів та каналів зв'язку	Система виявлення вторгнень	Контроль доступу користувачів
Кластер № 2 (Switch 1 – вузол-шлюз; Router 1 – контролер кластера)			
№ 5, PC 4	+	+	-
№ 6, PC 5	+	+	-
№ 7, PC 6	+	+	-
№ 8, PC 7	+	+	-
Кластер № 3 (Switch 2 – вузол-шлюз; Router 2 – контролер кластера)			
№ 9, PC 8	+	+	+
№ 10, PC 9	+	+	+
№ 11, PC 10	+	+	+
№ 12, PC 11	+	+	+

Результати проведення досліджень надано в табл. 2.

Таблиця 2

Результати верифікації запропонованої методики

Мережевий компонент	Рівень кібербезпеки ([0,5 і вище] – достатній; [менше 0,5] – недостатній)		
	Етап 1	Етап 2	Етап 3
Кластер № 1	0,9	0,1	0,1
Кластер № 2	0,9	0,8	0,1
Кластер № 3	0,9	0,9	0,9
Мережа ІТС	0,9	0,5	0,3

Аналіз отриманих результатів свідчить про те, що кожен етап методики (системи IDS, контроль доступу тощо) – один із технічних інструментів забезпечення кібербезпеки, він не повинен розглядатися окремо або як заміна для будь-якого іншого.

Висновки та перспективи подальших досліджень. У даній роботі наведено результати вирішення актуального науково-практичного завдання, яке полягало в удосконаленні наявних методів протидії кібернетичним атакам та НСД, а саме в розробленні методики забезпечення кібербезпеки критичних компонентів мережі ІТС.

В основу запропонованої методики покладено: комплексне застосування контролю стану мережевих вузлів та доступу користувачів до них; фіксування фактів здійснення кібернетичних атак на підставі аналізу вхідного (вихідного) трафіка; своєчасне виявлення кібернетичних загроз та скоєння НСД; оперативну протидію цим спробам.

Практичне значення одержаних результатів полягає в можливості інтеграції наукового результату в мережі ІТС для забезпечення відповідного рівня кібербезпеки.

СПИСОК ЛІТЕРАТУРИ

1. Гуменюк І. В., Басараба М. С., Некрилов О. В. Методика захисту інформації важливих компонентів мережі інформаційно-телекомунікаційної системи // ІІІ Всеукр. наук.-техн. конф. "Комп'ютерні технології: інновації, проблеми, рішення" : тези доповідей. Житомир : Житомирська політехніка, 2020. С. 27–28.

2. Казмірчук С., Корченко А., Паращук Т. Аналіз систем виявлення вторгнень // Захист інформації, 2018. Т. 20, № 4. С. 259–276.
3. Уманець Я. Л. Протоколи та методи маршрутизації потоків даних у перспективних мобільних радіомережах з динамічною топологією // Системи озброєння і військова техніка, 2013. № 2. С. 150–159.
4. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Харків : Вид. ХНЕУ, 2013. 476 с.
5. Толюпа С. В., Штаненко С. С., Берестовенко Г. В. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови // Зб. наук. праць ВІТІ. 2018. № 3. С. 112–122.
6. Зоріна Т. І. Системи виявлення і запобігання атак в комп'ютерних мережах // Вісник Східноукраїнського нац. ун-ту ім. В. Даля. 2013. № 15 (1). С. 48–52.
7. Колодчак О. М. Сучасні методи виявлення аномалій в системах виявлення вторгнень // Computer Systems and Networks, 2012. № 745. 2012. С. 98–104.
8. Пількевич І. А., Бойченко О. С., Гуменюк І. В. Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж // Технічна інженерія. Житомир : ДУ "Житомирська політехніка", 2019. № 2 (84). С. 100–109.
9. Гуменюк І. В., Басараба М. С., Некрилов О. В. Біометрична ідентифікація у кіберпросторі на основі розпізнавання обличчя // Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн : тези доп. наук.-практ. конф. (24–25 жовтня 2019 р.). Житомир : ЖВІ, 2019. С. 205–207.

Подано 10.10.2020

REFERENCES

1. Humeniuk, I. V., Basaraba, M. S., & Nekrylov, O. V. (2020). Metodyka zakhystu informatsii vazhlyvykh komponentiv merezhi informatsiino-telekomunikatsiinoi systemy [Methods of information protection of important components of the information and telecommunication system network]. In *III Vseukr. nauk.-tekhn. konf. "Komp'iuterni tekhnolohii: innovatsii, problemy, rishennia": tezy dopovidei [III All-Ukrainian. scientific and technical conf. "Computer technology: innovations, problems, solutions": abstracts of Papers]*. (pp. 27–28). Zhytomyr: SU Zhytomyr polytechnic [in Ukrainian].
2. Kazmirchuk, S., Korchenko, A., & Parashchuk, T. (2018). Analiz system vyiavlennia vtorhnen [Analysis of intrusion detection systems]. *Zakhyst informatsii [Information security, Vol. 20,* № 4, 259–276 [in Ukrainian].
3. Umanets, Ya. L. (2013). Protokoly ta metody marshrutyzatsii potokiv danykh u perspektyvnykh mobilnykh radiomerezhakh z dynamichnoiu topolohiieiu [Protocols and methods of routing data streams in advanced mobile radio networks with dynamic topology]. *Systemy ozbroiennia i viiskova tekhnika [Weapons systems and military equipment], 2,* 150–159 [in Ukrainian].
4. Ostapov, S. E., Yevseiev, S. P., & Korol, O. H. (2013). *Tekhnolohii zakhystu informatsii [Information protection technologies]*. Kharkiv [in Ukrainian].

5. Toliupa, S. V., Shtanenko, S. S., & Berestovenko, H. V. (2018). Klasyfikatsiini oznaky system vyiavlennia atak ta napriamky yikh pobudovy [Classification features of attack detection systems and directions of their construction]. *Zb. nauk. prats VITI [Collection of scientific works of the Military Institute of Telecommunications and Information Technologies named after Heroiv Krut], 3,* 112–122 [in Ukrainian].
6. Zorina, T. I. (2013). Systemy vyiavlennia i zapobihannia atak v komp'iuternykh merezhakh [Systems of detection and prevention of attacks in computer networks]. *Visnyk Skhidnoukrainskoho nats. un-tu im. V. Dalia [Bulletin of the Volodymyr Dahl East Ukrainian National University], 15* (1), 48–52 [in Ukrainian].
7. Kolodchak, O. M. (2012). Suchasni metody vyiavlennia anomalii v systemakh vyiavlennia vtorhnen [Modern methods of detecting anomalies in intrusion detection systems]. *Computer Systems and Networks, 745,* 98–104 [in Ukrainian].
8. Pilkevych, I. A., Boichenko, O. S., & Humeniuk, I. V. (2019). Metod detsentralizovanoho upravlinnia merezhevymy resursamy informatsiino-komunikatsiinykh merezh [Method of decentralized management of network resources of information and communication networks]. *Tekhnichna inzheneriia [Technical Engineering],* 2 (84), 100–109. Zhytomyr: SU Zhytomyr polytechnic [in Ukrainian].
9. Humeniuk, I. V., Basaraba, M. S., Nekrylov, O. V. (2019). Biometrychna identyfikatsiia u kiberprostori na osnovi rozpiznavannia oblychchia [Biometric identification in cyberspace based on face recognition]. In *Problemy teorii ta praktyky informatsiinoho protyborstva v umovakh vedennia hibrydnykh viin : tezy dop. nauk.-prakt. konf. [Problems of theory and practice of information confrontation in the conditions of hybrid wars: abstracts of reports of the scientific-practical conference of the Korolov Zhytomyr Military Institute]*. Zhytomyr, October 24–25, 2019. (pp. 205–207). Zhytomyr: ZhMI [in Ukrainian].

I. V. Humeniuk, M. S. Basaraba, O. V. Nekrilov

METHODS OF ENSURING CYBER SECURITY OF CRITICAL COMPONENTSNETWORKS OF INFORMATION AND TELECOMMUNICATION SYSTEM

It is established that the efficiency and reliability of information and telecommunication systems, in particular the networks that are part of them, significantly depends on the high level of protection of critical components. However, the constant improvement of the technical equipment of these systems requires the creation of new and improvement of existing methodological support for cyber security. One of the promising approaches is the development of a universal method of cybersecurity in the context of cyberattacks (influences, threats, etc.) and unauthorized access by unauthorized users to critical nodes (components) of information and telecommunications systems.

Timely detection, prompt counteraction to cyber threats and unauthorized access to critical network components is a necessary component of ensuring a high level of cybersecurity of the information and telecommunications system as a whole, especially in the context of hybrid warfare and armed aggression by the Russian Federation. To this end, the article proposes a method of cybersecurity of critical components of information and telecommunications systems, which is based on the integrated application of monitoring the state of network nodes

and user access to them, recording the facts of cyberattacks based on analysis of incoming (outgoing) traffic, timely detection of unauthorized access to and commission of cyber threats, as well as operational response to these attempts. The paper presents the results of verification of the proposed methods.

To this end, the article proposes a method of cybersecurity of critical components of information and telecommunications systems, which is based on the integrated application of monitoring the state of network nodes and user access to them, recording the facts of cyberattacks based on analysis of incoming (outgoing) traffic, timely detection of unauthorized access to and commission of cyber threats, as well as operational response to these attempts. The paper presents the results of verification of the proposed method. It is shown that its application allows to quickly detect the facts of cyber threats and unauthorized access to critical components of information and telecommunication systems networks and effectively counteract these attempts.

Keywords: *critical component; chain; information and telecommunication system; cybersecurity; cyberattack; unauthorized access; intrusion detection system.*

УДК 004.0:056.00 DOI: 10.46972/2076-1546.2020.18.11

О. В. Самчишин, Д. В. Перевізна

АНАЛІЗ ВИДІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ТА ПЕРЕВАГИ АТРИБУТНОЇ ІДЕНТИФІКАЦІЇ ЗА QR-КОДОМ

Поява нових та модернізація сучасних інформаційних технологій, розвиток інформаційно-телекомунікаційних систем обробки та зберігання інформації зумовили необхідність зростання ефективності захисту інформації разом зі складністю архітектури зберігання даних. Захист інформації від несанкціонованого доступу є вкрай необхідним заходом для запобігання матеріального та нематеріального збитку її власника, тому дуже важливо досліджувати ефективність роботи підсистеми управління доступом та захисту даних задля збереження безпеки певної системи інформаційної інфраструктури.

Загроза витоку інформації зробила засоби забезпечення інформаційної та кібербезпеки однією із обов'язкових характеристик інформаційно-телекомунікаційних систем, а захист інформації став невід'ємною складовою професійної діяльності.

В умовах гібридної війни Російської Федерації проти України значно збільшилася кількість кібернетичних атак на інформаційно-телекомунікаційні системи військового призначення. Водночас зросла їх технологічна складність. Даний процес обумовлює необхідність удосконалення систем захисту інформації та процесу надання доступу до них з використанням сучасних видів ідентифікації користувачів.

Ефективним методом захисту інформації є управління доступом. Він регулює використання ресурсів інформаційних систем. Важливим та невід'ємним елементом системи управління доступом є ідентифікація користувачів.

У статті проаналізовано сучасні види ідентифікації користувачів. Розглянуто технологію QR-коду: принцип формування, види кодування, структуру елементів, переваги його використання. Встановлено взаємозв'язок між його складовими. Перспективою подальших досліджень є розроблення алгоритму та програмного додатка ідентифікації користувачів для надання доступу за QR-кодом в інформаційно-телекомунікаційні системи військового призначення.

Ключові слова: *інформаційно-телекомунікаційна система; доступ; користувач; атрибутна ідентифікація*; *QR-код.*

Постановка проблеми в загальному вигляді. В умовах тривалого геополітичного протистояння інформаційна політика Російської Федерації (РФ) набула агресивного характеру. Протягом періоду ведення гібридної війни РФ проти України було здійснено велику кількість кібернетичних атак на інформаційно-телекомунікаційні системи (ІТС) військового призначення, що обумовлює необхідність удосконалення систем захисту інформації та процесу надання доступу до них [1].

Аналіз останніх досліджень і публікацій. Питаннями дослідження, розробки та впровадження сучасних видів ідентифікації користувачів займається велике коло вчених, зокрема, В. Бурячок, В. Толубко, В. Хорошко, М. Грайворонський та багато інших

вітчизняних і зарубіжних науковців [1–4]. Але в даних роботах не розглянуто аспект використання атрибутної ідентифікації користувачів на основі використання QR-коду саме для ІТС військового призначення. Тому це питання потребує додаткового дослідження.

Формулювання завдання дослідження. Метою статті є детальний аналіз сучасних видів ідентифікації користувачів для надання доступу до ІТС та дослідження одного зі способів атрибутної ідентифікації – QR-коду, а саме розгляд принципу його технології, будови, виду кодування, способу та переваг використання.

Виклад основного матеріалу. Ідентифікація дозволяє суб'єктові (користувачу, процесу, який діє від імені певного користувача) повідомити своє ім'я за допомогою унікального параметра — ідентифікатора, який є відомим іншій стороні. Під час ідентифікації здійснюється порівняння заявленого суб'єктом параметра на відповідність відомому іншій стороні. У разі успішної ідентифікації відбувається автентифікація. У такий спосіб інша сторона переконується, що суб'єкт є саме тим, за кого себе видає. Наступним етапом є авторизація. Її суть полягає в наділенні користувача певними правами.

На сьогодні є декілька видів ідентифікації користувачів: парольна, атрибутна, біометрична. Кожна з них має свої переваги і недоліки, що визначає сферу їх використання [2].

Парольна ідентифікація. База даних користувачів парольної системи містить облікові записи всіх її користувачів. Під парольною системою розумітимемо програмно-апаратний комплекс, що реалізовує системи ідентифікації та автентифікації користувачів ІТС на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати низку додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів.

Парольна система є “переднім краєм оборони” всієї системи безпеки. Деякі її елементи (зокрема ті, що реалізують інтерфейс користувача) можуть бути розташовані в ділянках, відкритих для доступу потенційному зловмиснику. Тому парольна система стає одним із перших об'єктів атаки в разі вторгнення зловмисника в захищену систему [2].

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів у базі даних облікових записів. Можливі такі варіанти зберігання паролів:

у відкритому вигляді;

у вигляді згорток (хешування);

зашифрованими за деяким ключем.

Хешування (використання незворотної хеш-функції для будь-якої інформації перетворює її на унікальний код) не забезпечує захисту від підбору паролів за словником у разі отримання бази даних зловмисником. У ході вибору алгоритму хешування, який буде використано для розрахунку згорток паролів, необхідно гарантувати незбіг значень згорток, отриманих на основі різних паролів користувачів (відсутність колізій). Крім того, слід передбачити механізм, що забезпечує унікальність згорток у разі, якщо два користувачі обирають однакові паролі. Для шифрування паролів особливе значення має спосіб генерації та зберігання ключа шифрування в базі даних облікових записів. Перерахуємо деякі можливі варіанти:

ключ генерується програмно та зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження;

ключ генерується програмно та зберігається на зовнішньому носії, з якого він зчитується під час кожного запуску;

ключ генерується на основі обраного адміністратором пароля та вводиться в систему щоразу під час запуску.

Найбільш безпечне зберігання паролів забезпечується в разі їх хешування та подальшого шифрування отриманих згорток, тобто за комбінації другого і третього способів. Враховуючи, що користувачі нерідко обирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого мережею значення згортки пароля становлять серйозну загрозу безпеці парольної системи. У більшості випадків автентифікація відбувається в розподілених системах і пов'язана з передачею мережею інформації про параметри облікових записів користувачів. Якщо інформація, що передається мережею в процесі автентифікації, не захищена належним чином, то виникає загроза її перехоплення зловмисником і використання для порушення захисту парольної системи. Відомо, що багато комп'ютерних систем дозволяють програмно перемикати мережевий адаптер у режим прослуховування мережевого трафіка, адресованого іншим одержувачам у мережі, що ґрунтується на передачі пакетів даних.

Суть парольної ідентифікації зводиться до такого алгоритму: кожен зареєстрований користувач певної системи одержує набір персональних реквізитів (зазвичай використовуються пари логін-пароль). Далі щоразу для входу користувач повинен вказати ці реквізити. Оскільки пара логін-пароль унікальна для кожного користувача, то на її підставі відбувається його ідентифікація в системі.

Головна перевага парольної ідентифікації – це простота реалізації та використання. Крім того, вона не вимагає значних витрат: даний процес реалізований у всіх програмних продуктах, що є в продажу. Отже, система захисту інформації є гранично простою і доступною.

Її недоліком є значна залежність надійності ідентифікації від самих користувачів, тобто від обраних ними паролів. Це зумовлено тим, що більшість користувачів застосовують нестійкі ключові слова, які легко підбираються. До них належать занадто короткі паролі та ті, які складаються тільки з одного виду символів [3].

Атрибутна ідентифікація ґрунтується на визначенні особистості користувача за певним предметом, що перебуває в його персональному користуванні, – спеціальним електронним ключем. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння із собою. На даний момент найбільшого поширення набули два типи пристроїв. До першого належать так звані “токени”, що мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT). Іншим типом ключів, які можуть використовуватися для апаратної ідентифікації, є різноманітні ідентифікаційні карти.

Основною перевагою застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які зловмисникам не вдасться. Крім того, у них реалізовані різні варіанти захисних механізмів. Вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати інші корисні функції [4].

Недоліком апаратної ідентифікації є можливість втрати електронних ключів зареєстрованими користувачами. Під втратою розуміється викрадення, передача іншій особі, дублікат. Крім того, недоліком є також вартість. Для введення в експлуатацію системи атрибутної ідентифікації зареєстрованого користувача потрібно забезпечити ключем. Також згодом деякі типи ключів потребують заміни через зношеність, факт втрати тощо, тобто апаратна ідентифікація вимагає певних експлуатаційних витрат [5].

Біометрична ідентифікація. Біометрія − це ідентифікація людини за унікальними, властивими тільки їй, біологічними ознаками. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки як основу для ідентифікації користувача й ухвалення рішення про можливість доступу до ресурсів комп’ютерних систем.

Серед біометричних механізмів ідентифікації можна виділити такі:

за статичними ознаками – тими, які практично не змінюється з часом, починаючи з народження людини (фізіологічні характеристики);

за динамічними ознаками – поведінковими характеристиками, які ґрунтуються на особливостях, притаманних для підсвідомих рухів у процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів у завданнях ідентифікації користувача комп’ютерних систем використовуються такі:

ідентифікація за відбитком пальця: в основі цього методу лежить унікальність малюнка папілярних візерунків на пальцях. Ідентифікація побудована таким чином: за допомогою сканера одержують зображення відбитка, потім це зображення певним алгоритмом перетворюється на спеціальний цифровий код, який далі порівнюється з еталоном, що зберігається в базі даних;

ідентифікація за розташуванням вен на долоні: приладом, який зчитує інформацію в цьому разі, є інфрачервона камера. У результаті на вході програми для формування цифрового коду з'являється малюнок вен на руці. Не потребує контакту людини з пристроєм для сканування;

ідентифікація за сітківкою ока: сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. Зрозуміло, що цей малюнок спостерігається тільки за певних умов: для сканування людина дивиться на віддалене світлове джерело і спеціальна камера сканує її очне дно, що, у свою чергу, може викликати дискомфортні відчуття;

ідентифікація за райдужною оболонкою ока: малюнок райдужної оболонки ока – унікальний для кожної людини. Для застосування цього методу важлива не тільки спеціальна камера, а й надійне програмне забезпечення (ПЗ), адже саме за його допомогою із зображення виділяється малюнок потрібної райдужної оболонки;

ідентифікація за формою кисті руки: цей метод ґрунтується на розпізнаванні геометричних особливостей кінцівки. Спеціальний сканер формує тривимірний малюнок кисті, у ході його аналізу здійснюються вимірювання, за допомогою яких формується відповідний цифровий код;

ідентифікація за формою обличчя: на практиці використовують як двовимірне, так і тривимірне зображення, причому перше на сьогоднішній день є одним із найменш ефективних методів біометрії, тому має обмежене коло застосування або

використовується тільки в сукупності з іншими методами. Розпізнавання за тривимірним зображенням обличчя схоже на метод ідентифікації за формою кисті руки, оскільки так само будується тривимірний образ. Спеціалізоване ПЗ виділяє з цього образу контури очей, губ й інших частин обличчя. Далі проводяться точні вимірювання між заданими контурами. Саме за цими даними будується цифровий код.

Серед динамічних методів, які використовуються для біометричної ідентифікації особи користувача, можна назвати такі:

ідентифікація за голосом: на сьогодні є велика кількість подібних програм розпізнавання. У методі ідентифікації за голосом важливі його частотні характеристики, оскільки саме за ними будується цифрова модель;

ідентифікація за почерком: досліджується підпис людини. Перевіряються такі динамічні характеристики, як: графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. На основі цих характеристик будується цифровий код;

ідентифікація за клавіатурним почерком: даний метод аналогічний методу ідентифікації за почерком, але замість того, щоб нанести підпис, людині необхідно надрукувати кодове слово. Цифровий код будується за динамікою набору певного слова або фрази.

Попри все теоретичне різноманіття можливих біометричних методів, тих, що застосовуються на практиці, небагато. В основному використовуються розпізнавання за відбитком пальця, за зображенням особи (двомірним або тривимірним), за райдужною оболонкою та за сітківкою ока. Це обумовлено технічною складністю реалізації програмно-апаратних засобів.

Головна перевага біометричних технологій − висока надійність. Оскільки біометричні характеристики кожної людини індивідуальні, то ймовірність зламу системи з використанням біометричної ідентифікації суттєво знижується.

Основним недоліком біометричної ідентифікації є вартість устаткування. З підвищенням його ціни збільшується термін його використання, значно зменшується відсоток помилок іншого роду (наприклад, відмова в доступі зареєстрованому користувачеві).

Отже, було розглянуто три види однофакторної ідентифікації користувачів ІТС. Також на сьогодні набуває поширення комплексна або багатофакторна ідентифікація, коли для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів. Комбінуватися вони можуть у довільному порядку. Утім сьогодні в переважній більшості випадків використовується пара ідентифікаторів − парольний захист і токен. Це унеможливлює підбір пароля користувача зловмисником (без електронного ключа він працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Проте в деяких системах застосовуються процедури ідентифікації, у яких одночасно використовуються паролі, токени та біометричні характеристики людини [6].

Принципово новим та найменш поширеним в ІТС військового призначення є метод атрибутної ідентифікації користувачів на основі технології QR-коду.

QR-код – це різновид двомірного штрих-коду, у який закладається певний контент. Він складається з певного набору міток і пікселів, які становлять собою закодоване повідомлення, збережене в ньому.

Принцип використання QR-кодів полягає в тому, що роздрукований або в електронному вигляді код може бути зчитаний і розшифрований за допомогою пристрою, який має функціональну камеру і встановлене ПЗ для декодування.

Закодувати інформацію в QR-код можна кількома способами, вибір конкретного з них залежить від того, які символи використовуються. Якщо беруть лише цифри від 0 до 9, то можна застосувати цифрове кодування, якщо крім цифр необхідно зашифрувати букви латинського алфавіту, пробіл і спецсимволи, то використовується буквено-цифрове кодування. Ще відоме кодування кандзі, яке застосовують для шифрування китайських і японських ієрогліфів, а також побайтове кодування, коли перед кожним сеансом кодування створюється порожня послідовність біт, яка потім заповнюється.

Цифрове кодування вимагає 10 біт на 3 символи. Уся їх послідовність розбивається на групи по 3 цифри, кожна група (тризначне число) переводиться в 10-бітове двійкове число і додається до послідовності біт. Якщо загальна кількість символів не кратна 3, тобто в кінці залишається 2 символи, то отримане двозначне число кодується 7 бітами, а якщо 1 символ – 0–4 бітами.

Для *буквено-цифрового кодування* 2 символів потрібно 11 біт інформації. Послідовність символів розбивається на групи по 2, у групі кожен символ кодується згідно з таблицею ASCII. Значення першого символа множиться на 45, потім до цього добутку додається значення другого символа. Отримане число переводиться в 11-бітове двійкове число і додається до послідовності біт. Якщо в останній групі залишається один символ, то його значення кодується 6-бітовим числом.

Байтовим кодуванням можна закодувати будь-які символи. Їх вхідний потік кодується в будь-якому кодуванні (рекомендовано в UTF-8), переводиться в двійковий вигляд та об'єднується в один потік бітів.

В основі кодування ієрогліфів (як й інших символів) *кандзі* лежить візуально сприйнятна таблиця або список зображень ієрогліфів з їх кодами. Така таблиця називається “Character set”. Для японської мови основне значення мають дві таблиці символів: JIS 0208:1997 [7] і JIS 0212:1990 [8]. Друга з них є доповненням до першої. JIS 0208:1997 складається з 94 сторінок по 94 символи.

QR-код складається з певного набору міток і пікселів, які становлять собою закодоване повідомлення, збережене в QR-коді (рис. 1).

На будь-якому QR-коді обов'язково повинні бути 6 видів міток [9]:

позиціонування (область, необхідна для детектування коду);

номер версії (визначає, яка версія коду використовується (від 1 до 40));

синхронізація (дублюються у двох напрямках і дозволяють знизити ймовірність виникнення помилок у разі зчитування, системної інформації (наприклад, версія, тип даних тощо));

формат (необхідні для визначення типу даних, закодованих у коді);

вирівнювання (використовуються для кращого позиціонування коду під час обробки (для версії QR-коду вище 1));

рівень виправлення помилки (дозволяють визначити, який рівень перешкодозахищеності був використаний на етапі кодування для правильного вибору способу виявлення можливих помилок у коді).

Рис. 1. Будова QR-коду

Переваги використання QR-коду:

1) дозволяє кодувати більше інформації, ніж лінійні штрих-коди (порівняння об'єму даних, що можуть міститися в QR-коді та штрих-коді, наведено в табл. 1);

2) легко розпізнається сканувальним обладнанням (за допомогою структурних елементів, що містить QR-код, камера без ускладнень фокусується на ньому та відбувається декодування інформації, що в ньому міститься);

3) може бути зчитаний навіть у разі пошкоджень (QR-код має здатність відновлення інформації, що міститься в ньому, навіть якщо певна частина символів на зображенні QR-коду була пошкоджена або не розпізнана. Максимальна кількість кодових слів, що може бути відновлена, становить до 30%).

Таблиця 1

Порівняння об'єму даних у штрих-коді та QR-коді

Тип даних	**QR-код**	**Штрих-код**
Числові дані, символів	7089	1230
Символьні дані, символів	4296	70
Бінарна інформація, байт	2953	516

Дані переваги та новизна QR-коду як атрибута ідентифікації користувачів обумовлюють доцільність додаткового аналізу й досліджень, а також розробки алгоритму та ПЗ ідентифікації користувачів для надання доступу за QR-кодом в ІТС військового призначення.

Висновки. На основі аналізу сучасних методів ідентифікації користувачів було визначено, що на сьогодні найбільш поширеним є парольний захист, оскільки є найпростішим у реалізації. Його недолік полягає у великій кількості методів підбору паролів, що зумовлює високу вірогідність зламу систем парольної ідентифікації. Решта розглянутих видів ідентифікації користувачів також не в змозі в повному обсязі забезпечити захист інформації, цілком унеможлививши ризик несанкціонованого доступу, або мають високу вартість розробки та технологічну складність реалізації. Було досліджено технологію QR-кодів. Перспектива подальших досліджень полягає в розробленні алгоритму та програмного додатка ідентифікації користувачів для надання доступу за QR-кодом в ІТС військового призначення.

СПИСОК ЛІТЕРАТУРИ

1. Косогов О. М., Сірик А. О. Основні проблемні питання та напрямки підвищення ефективності державної інформаційної політики України в умовах гібридної війни. Київ : НУОУ ім. І. Черняховського, 2017. 104 с.
2. Інформаційна та кібербезпека: соціотехнічний аспект : навч. посіб. / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Київ : ДУТ, 2015. 288 с.
3. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій : навч. посіб. Харків : ХНУ ім. В. Н. Каразіна, 2013. 632 с.
4. Грайворонський М. В., Новіков О. М. Безпека інформаційно-телекомунікаційних систем : підруч. Київ : ВНУ, 2009. 608 с.
5. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29 березня 2006 р. (зі змінами) № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006 (дата звернення: 14.11.2020).
6. Самчишин О. В., Перевізна Д. В. Програмний додаток надання доступу на основі атрибутної ідентифікації // Тези доповідей ІІІ Всеукр. наук.-техн. конф. «Комп'ютерні технології: інновації, проблеми, рішення». Житомир : Житомирська політехніка, 2020. С. 11–13.
7. Таблиця символів: JIS 0212: 1990. URL: https://www.normadoc.com/english/jis-z-0212-1998-r2013.html (дата звернення: 16.11.2020).
8. Таблиця символів: JIS 0208: 1997. URL: https://www.normadoc.com/english/jis-x-0208-1997-r2007.html (дата звернення: 16.11.2020).
9. ISO/IEC 18004:2006. URL: https://www.iso.org/ru/standard/43655.html (дата звернення: 17.11.2020).

Подано 17.11.2020

REFERENCES

1. Kosohov, O. M., & Siryk, A. O. (2017). *Osnovni problemni pytannia ta napriamky pidvyshchennia efektyvnosti derzhavnoi informatsiinoi polityky Ukrainy v umovakh hibrydnoi viiny [The main problematic issues and directions of increasing the efficiency of the state information policy of Ukraine in the conditions of hybrid war]*. Kyiv: NDU of Ukraine named

after Ivan Cherniakhovskyi [in Ukrainian].
2. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and cybersecurity: socio-technical aspect]*. Kyiv: SUT [in Ukrainian].
3. Yesin, V. I., Kuznetsov, O. O., & Soroka, L. S. (2013). *Bezpeka informatsiinykh system i tekhnolohii [Security of information systems and technologies]*. Kharkiv: V. N. Karazin KhNU [in Ukrainian].
4. Hraivoronskyi, M. V., & Novikov, O. M. (2009). *Bezpeka informatsiino-telekomunikatsiinykh system [Security of information and telecommunication systems]*. Kyiv: VNU [in Ukrainian].
5. Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh : postanova Kabinetu Ministriv Ukrainy vid 29 bereznia 2006 r. (zi zminamy) № 373. [On approval of the Rules for ensuring information protection in information, telecommunication and information-telecommunication systems: Resolution of the Cabinet of Ministers of Ukraine from March 29, 2006 (as amended) № 373]. (2006). Retrieved from https://zakon.rada.gov.ua/laws/show/373-2006 [in Ukrainian].
6. Samchyshyn, O. V., & Perevizna, D. V. (2020). Prohramnyi dodatok nadannia dostupu na osnovi atrybutnoi identyfikatsii [Software application for providing access based on attribute identification]. In *Tezy dopovidei III Vseukr. nauk.-tekhn. konf. «Komp'iuterni tekhnolohii: innovatsii, problemy, rishennia» [Abstracts of reports III All-Ukrainian scientific and technical conf. "Computer technologies: innovations, problems, solutions"]*. (pp. 11–13). Zhytomyr: Zhytomyr Polytechnic State University [in Ukrainian].
7. Tablytsia symvoliv [Character table]: JIS 0212: 1990. (1990). Retrieved from https://www.normadoc.com/english/jis-z-0212-1998-r2013.html [in Ukrainian].
8. Tablytsia symvoliv [Character table]: JIS 0208: 1997. (1997). Retrieved from https://www.normadoc.com/english/jis-x-0208-1997-r2007.html [in Ukrainian].
9. ISO/IEC 18004:2006. (2006). Retrieved from https://www.iso.org/ru/standard/43655.html.

O. V. Samchyshyn, D. V. Perevizna

ANALYSIS OF TYPES OF USER'S IDENTIFICATION AND ADVANTAGES OF USER'S ATRIBUTE IDENTIFICATION BY QR-CODE

Emergence of new technologies and modernization of existing information technologies, development of information and telecommunication processing and storage systems have increase the level of information security, necessitating an increase of information security's effectiveness with the complexity of data storage architecture. Security of information from unauthorized access is an essential measure to prevent material and non-material damage to its owner. So it is very important to take into account the efficiency of the subsystem of access control and data security in order to ensure security of some information system.

Accordingly the threat of information leakage has made the means of information security and cyber security one of the mandatory characteristics of information and telecommunication systems and information security has become an integral part of professional function.

Under conditions of the hybrid war of the Russian Federation against Ukraine? the number of cyber attacks on military information and telecommunication systems has increased. At the

same time their technological complexity has increased too. This process necessitates the improvement of information security systems and the process of providing access to them by using modern types of users identification.

Access control is an effective method of information security. It regulates the use of information system resources. User's identification is an important and integral element of access control system.

An analysis of modern types of users identification is presented in the paper. The technology of QR-code is considered: the principle of formation, the types of coding, the structure of elements, the advantages of its usage. The interconnection between its components was established. Prospects for further research are the development of an algorithm and software application for user identification to provide access by QR-code to information and telecommunication systems for military purposes.

Keywords: *information and telecommunication system; access; user; attribute identification; QR-code.*

УДК 004.421 DOI: 10.46972/2076-1546.2020.18.12

О. О. Гребенюк, М. Ю. Бедзай

АЛГОРИТМ АВТОМАТИЗОВАНОГО ВИБОРУ МАРШРУТУ ТА РОЗРАХУНКУ МАРШУ ПІДРОЗДІЛУ ДЛЯ ПРОГРАМНОГО ДОДАТКА ДО ЗАСОБІВ МОБІЛЬНОГО ЗВ'ЯЗКУ

Досвід проведення операції Об'єднаних сил свідчить про необхідність створення автоматизованої системи управління діями підрозділів Сухопутних військ на тактичному рівні. Це пов'язано з необхідністю забезпечення інформованості розподілених у географічному просторі частин і підрозділів, приданих сил і засобів, окремих військовослужбовців на полі бою, а також високого рівня оперативності управління ними.

У статті розглянуто основні принципи використання спеціальних програмних додатків для засобів мобільного зв'язку, виконаних на основі геоінформаційної системи для планування маршу частин та підрозділів.

Проаналізовано доцільність використання мобільної платформи на основі засобів мобільного зв'язку як носія програмного забезпечення. Визначено вимоги до інформаційних систем на основі геоінформаційної системи та програмних додатків для засобів мобільного зв'язку з метою покращення оперативності на етапі планування переміщення підрозділу. Запропоновано розробку програмного додатка на основі описаного алгоритму розрахунку маршу з використанням геоінформаційних систем. Розроблений алгоритм визначає послідовність дій щодо автоматизації процесу вибору оптимального маршруту на карті, розрахунку маршу та його основних параметрів. Як цифрові карти запропоновано використовувати картографічні сервіси та технології Google Maps або Яндекс Карт, перевагами яких є багатошаровість та універсальність. Даний підхід дозволить автоматизувати розрахунки, покращить оперативність і ефективність прийняття рішення командиром щодо вибору позиційного району та організації маршу.

У подальшому заслуговує на увагу розширення функціональних можливостей програмного додатка до рівня мобільної інформаційно-довідкової системи командира підрозділу шляхом розробки спеціальних і використання вже відомих програмних утиліт та інформаційних ресурсів.

Ключові слова: *геоінформаційна система; розрахунок маршруту руху; метод Дейкстри; теорія графів.*

Постановка проблеми в загальному вигляді. На даний час у збройних силах (ЗС) провідних країн світу широкого застосування набули автоматизовані системи управління (АСУ) різного функціонального призначення на всіх рівнях воєнних дій (тактичний, оперативний, стратегічний). Найбільш вдалим прикладом АСУ тактичної ланки є американська система "Force Battle Command Brigade and Below" (FBCB2), яка забезпечує автоматизацію процесу управління підрозділами сухопутних військ (СВ) у ланці бригада – батальйон – рота – взвод – відділення (танк) та забезпечує відображення оперативної обстановки на полі бою, доведення у формалізованому текстовому і графічному вигляді розпоряджень та наказів, автоматичний вибір та розрахунок маршруту руху тощо [1].

У ЗС України єдина АСУ діями підрозділів СВ на тактичному рівні відсутня. Натомість використовуються програмні продукти, які вирішують часткові завдання залежно від специфіки підрозділів. Разом з тим досвід проведення ООС свідчить про необхідність створення АСУ на мобільній платформі з метою забезпечення інформованості розподілених у географічному просторі частин і підрозділів, приданих сил і засобів, окремих військовослужбовців на полі бою, а також високого рівня оперативності управління ними.

Для ефективного застосування сил та засобів радіомоніторингу командир підрозділу має виконати значний обсяг роботи, щоб прийняти правильне і виважене рішення. Оцінка обстановки та місцевості, вибір позиційного району, організація та планування маршу до визначених позицій, побудова бойового порядку є важливими етапами в процесі прийняття рішення, яке оформляється на робочій карті [4, 6, 9].

На даний час у ЗС України розробці автоматизованих програмних засобів підтримки прийняття рішення приділяється значна увага. Окремим важливим напрямком розвитку інформаційно-аналітичного забезпечення бойової діяльності підрозділів є удосконалення процесу планування маршу за рахунок використання геоінформаційних систем (ГІС).

Аналіз останніх досліджень і публікацій. Питанню покращення ефективності планування маршу підрозділу (вибору маршруту та розрахунку його показників) присвячено певну кількість наукових робіт та прикладних програм. Так, у рамках науково-дослідних і прикладних робіт [3–6] запропоновано систему зменшення впливу фізико-географічних факторів на ефективність пересування військ. Також розроблено програмні продукти, наприклад, “Аргумент”, “Панорама”, які за допомогою цифрових карт місцевості здійснюють пошук оптимальних шляхів між вибраними точками [2, 5]. Однак ці системи планування маршу підрозділів не враховують особливостей виконання оперативних завдань підрозділами радіомоніторингу. Разом з тим залишається недослідженим питання щодо застосування інформаційної системи забезпечення роботи командира підрозділу у формі програмних додатків для засобів мобільного зв’язку, оскільки останні набули за останній час широкого поширення.

Метою статті є удосконалення процесу прийняття рішення командиром підрозділу шляхом покращення оперативності вибору маршруту та розрахунку показників маршу підрозділу за рахунок застосування спеціального програмного забезпечення у формі програмного додатка для засобів мобільного зв’язку

Формулювання завдання дослідження. Для досягнення поставленої мети необхідно розв’язати сукупність часткових науково-прикладних задач: обрати базову цифрову карту, яку можна застосовувати на мобільних засобах зв’язку; визначити перелік функцій, що мають виконуватися автоматизовано для побудови маршруту; розробити алгоритм розрахунку маршу з використанням ГІС.

Виклад основного матеріалу. Якісне інформаційне забезпечення бойових дій військ (сил) в умовах швидкоплинності сучасних війн і збройних конфліктів стає визначальною умовою досягнення стратегічної, оперативної та тактичної переваги над противником. У ході виконання оперативних завдань на командира підрозділу радіомоніторингу покладено високу відповідальність за оперативне, своєчасне та ефективне виконання завдань.

На даний час бойові дії стають усе більш динамічними, своєчасне реагування на них залежатиме від швидкості проведення маневру силами та засобами. Це приводить до пошуку нових способів ведення бойових дій, а також організації підтримки військ на полі бою з урахуванням останніх досягнень у галузі інформаційних технологій і телекомунікацій.

Забезпечення вимог щодо вибору позиційного району, організації маршу є одним із головних завдань, які визначають здатність командирів і штабів враховувати вплив різноманітних факторів, приймати найкращі для даних умов рішення.

Стислі терміни і великий обсяг інформації, який необхідно при цьому обробляти, висувають усе більш жорсткі вимоги до роботи командира підрозділу. Тому для вдосконалення процесу планування та здійснення маршу підрозділами, підвищення ефективності роботи командира та штабів необхідно розробляти нові підходи до їх організації з більш широким урахуванням особливостей і вимог. Досягти більш якісного планування маршу можна за рахунок використання у військовій справі сучасних геоінформаційних технологій [3].

Основою сучасного підходу до автоматизації управління ЗС є впровадження в процес управління ГІС, використання яких надає органам військового управління візуальну, просторову та деяку додаткову інформацію про місцевість і розташовані на ній об'єкти для планування маршу та визначення правильного маршруту на пристроях відображення. Марш – це організоване пересування військ у колонах на транспортних засобах, бойових машинах або в пішому порядку дорогами і колонними шляхами з метою виходу до встановленого часу у визначений район або на вказаний рубіж у повній бойовій готовності до виконання завдань [4].

У наш час марш, який здійснюють на колісних або гусеничних машинах, вважається основним видом пересування військ, тому що він забезпечує високу швидкість руху і своєчасне прибуття підрозділів у призначений район. Основні показники маршу: протяжність (кілометри); тривалість (години); кількість маршрутів, що виділяються; середня величина добового переходу (кілометри); маршова швидкість руху колони (кілометри за годину).

Для автоматизації процесу планування та організації маршу підрозділів і частин необхідно мати відповідний розрахунковий механізм оптимізації маршрутів пересування сил і засобів на місцевості за різними критеріями. Для пошуку оптимального маршруту можливо сформулювати систему критеріїв [4].

Критерій 1. В умовах, коли рух колони проходить у районі, де відсутня небезпека зустрічі з противником, оптимальним маршрутом є той, що забезпечує найменший час пересування.

Критерій 2. В умовах, коли рух колони проходить у районі, де є велика ймовірність зустрічі з противником, а час руху не обмежений, оптимальним маршрутом є той, що забезпечує найменшу ймовірність зустрічі з противником.

Критерій 3. В умовах, коли рух колони проходить у районі, де є велика ймовірність зустрічі з противником, а час руху обмежений, оптимальним маршрутом є той, що забезпечує найменшу ймовірність зустрічі з противником за умови, що час пересування не перевищить директивно заданого показника.

Критерій 4. В умовах, коли час пересування в районі обмежений і автомобільна техніка дозволяє підтримувати задану швидкість переміщення на всіх типах доріг, оптимальним маршрутом є той, що забезпечує мінімальну відстань переміщення.

Критерій 5. В умовах, коли рух колони проходить у районі, де є велика ймовірність блокування певних ділянок доріг, оптимальним маршрутом є той, що забезпечує найменшу ймовірність такого блокування. Якщо ймовірності блокування противником кожного з двох маршрутів однакові, то більш доцільним з них є той, що забезпечує менший час пересування.

У статті введено обмеження щодо вибору та реалізації критеріїв. Алгоритм автоматизованого вибору маршруту та розрахунку маршу підрозділу розроблено для критерію 1.

Застосування командиром сучасних цифрових карт, наприклад, Google Maps, Яндекс Карт та інших цифрових карт, в основі яких лежить використання супутникових знімків географічних районів, надає можливість оперативного та повного оцінювання місцевості, вибору вигідного позиційного району та прокладання маршруту руху своїх підрозділів.

Загальна блок-схема алгоритму розрахунку маршу з використанням ГІС наведена на рис. 1. Розроблений алгоритм доцільно покласти в основу спеціального програмного забезпечення для автоматизованого прокладання маршруту руху підрозділу на карті та розрахунку показників маршу.

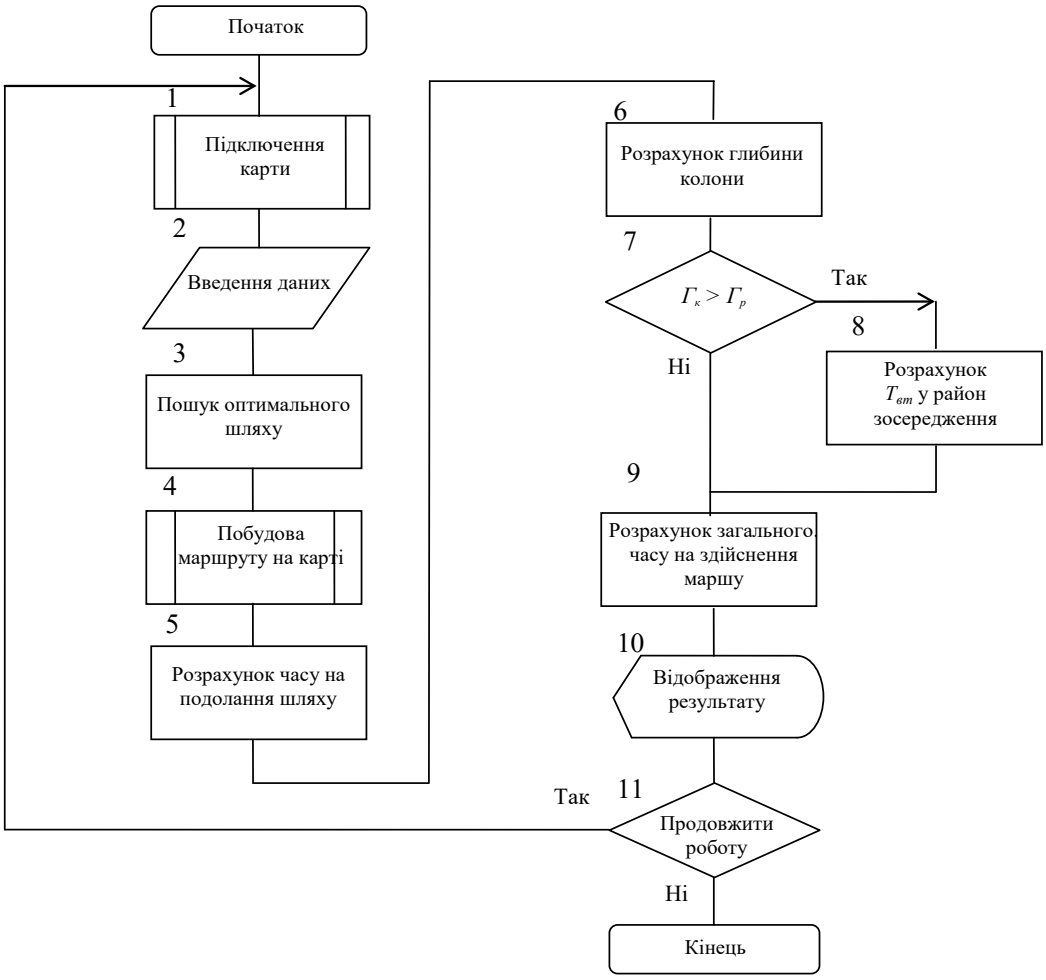


Рис. 1. Блок-схема алгоритму розрахунку маршу на основі ГІС

Блок 1 здійснює завантаження і відображення карти Google Maps або Яндекс Карт та необхідних бібліотек шляхом підключення мобільного засобу до глобальної мережі Інтернет.

Блок 2 забезпечує розрахунок маршу підрозділу, реалізує процес введення даних, необхідних для розрахунків основних показників.

Блок 3 реалізує процес пошуку оптимального шляху між двома точками на карті, використовуючи метод Дейкстри, тобто алгоритму, який знаходить найкоротший шлях від однієї вершини графа до всіх інших вершин.

Блок 4 реалізує побудову маршруту на карті, яку використовує програмний додаток. Для цього необхідні початкові дані, ними є вихідний і кінцевий пункти, які вводяться в блоці 2.

Блок 5 реалізує процес розрахунку часу $T_ч$(год.) на подолання шляху за такою формулою:

$$T_ч = \frac{D}{V_{СЕР}}, \tag{1}$$

де D – протяжність маршруту, км,

$V_{СЕР}$ – середня швидкість колони, км/год.

Блок 6 реалізує процес розрахунку глибини колони $Г_К$ (км) за формулою

$$Г_К = \frac{(K_М * 6{,}5) + (K_М - 1)}{1000} * 50, \tag{2}$$

де $K_М$ – кількість машин у колоні, од.

Блок 7 перевіряє умову розрахунку часу втягування колони. «Так» – глибина колони буде більшою, ніж глибина району зосередження, виконується блок 8. «Ні» – глибина колони буде меншою за глибину району зосередження, виконується блок 12.

Блок 8 реалізує процес розрахунку часу втягування $T_{ВТ}$ (год.) у район зосередження за такою формулою:

$$T_{ВТ} = \frac{(Г_К - Г_Р)}{V_{ср} * 0{,}5} * 60, \tag{3}$$

де $Г_Р$ – глибина району зосередження, км.

Блок 9 реалізує процес розрахунку загального часу на здійснення маршу $T_{МАРШ}$ за формулою

$$T_{МАРШ} = \frac{D}{V_{ср}} + K_М + T_{ВТ}. \tag{4}$$

Блок 10 реалізує процес виведення користувачеві результату загального часу на здійснення маршу.

Блок 11 перевіряє умову продовження роботи даним програмним забезпеченням: якщо «Так», то робота алгоритму переходить до блоку 1, при цьому здійснюється очищення полів та регістрів і надається можливість користувачеві проводити розрахунки з іншими значеннями; якщо «Ні», то робота алгоритму закінчується.

З метою апробації запропонованих в статті рішень було реалізовано варіант програмного забезпечення для ПЕОМ. Програма здійснює: вибір альтернативних

маршрутів руху колони підрозділу з урахуванням особливостей оперативної обстановки в районі проведення ООС; розрахунок показників маршу залежно від визначених початкових умов.

Висновки. Розроблений алгоритм описує послідовність дій щодо автоматизації процесу вибору оптимального маршруту на карті, розрахунку маршу та його основних параметрів. На його основі запропоновано розробити спеціальний програмний додаток для мобільних засобів зв'язку з використанням даних ГІС. Це дозволить автоматизувати розрахунки, значно покращить оперативність і ефективність прийняття рішення командиром щодо вибору позиційного району та організації маршу, вносити корективи в разі зміни оперативної обстановки.

У подальшому заслуговує на увагу розширення функціональних можливостей програмного додатка до рівня мобільної інформаційно-довідкової системи командира підрозділу шляхом розробки спеціальних, а також використання вже відомих програмних утиліт та інформаційних ресурсів.

СПИСОК ЛІТЕРАТУРИ

1. Масной В., Судаков Ю. Автоматизированные системы управления сухопутными войсками США // Зарубежное военное обозрение. 2003. № 9. С. 25–32.

2. Бацамут В. М., Бабак С. А., Добраниця О. П. Автоматизація процесу прийняття рішення на застосування сил військ при ускладненні оперативної обстановки // Честь і закон. 2005. № 3. С. 11–17.

3. Побережний А. А., Горєлишев С. А., Сальников О. М. Методика пошуку раціонального маршруту за допомогою геоінформаційної системи // Наукове забезпечення службово-бойової діяльності ВВ МВС України : зб. тез доп. IV наук.-практ. конф., Харків, 22 лют. 2012 р. Харків : Акад. ВВ МВС України. С. 80–81.

4. Бацамут В. М., Горєлишев С. А, Побережний А. А. Використання геоінформаційної системи у плануванні маршу частин та підрозділів внутрішніх військ МВС України // Зб. наук. праць Академії внутрішніх військ МВС України. 2013. Вип. 2 (22). С. 21–25.

5. Литвиненко Н. І. Застосування ГІС для організації переміщень підрозділів військ (сил) // Геоінформаційний моніторинг навколишнього середовища: GPSi GIS-технології : матеріали XII Міжнар. наук.-техн. симпозіуму, Алушта, 10–15 верес. 2007 р. Алушта, 2007. С. 103–107.

6. Пічугін М. Ф., Бучик С. С., Соболенко С. О., Єрмаков В. О. Основи військового управління. Ч. 1. Основи загальної теорії управління : навч. посіб. Житомир : ЖВІ НАУ, 2010. С. 36–41.

7. Решмин Б. Имитационное моделирование и системы управления : учеб.-практ. пособ. Ижевск : Изд-во "Инфра-инженерия", 2016. С. 4–12.

8. Гаценко С. С., Кальницький Ю. М., Гельвейчук О. М. Проблема розподілу інформаційних потоків в автоматизованих системах управління військами (силами) Збройних Сил України // Зб. наук. праць Центру воєнно-стратегічних досліджень НУО України ім. І. Черняховського. 2014. № 2 (51). С. 107–112.

9. Короленко В. А., Синявский В. К., Верещагин С. И. Автоматизация системы управления войсками: на пути от идеи к решению // Автоматизация управления войсками. 2013. № 1. С. 32–39.

Подано 28.09.2020

REFERENCES

1. Masnoi, V., & Sudakov, Iu. (2003). Avtomatizirovannye sistemy upravleniia sukhoputnymi voiskami SShA [Automated command and control systems for the US Army]. *Zarubezhnoe voennoe obozrenie [Foreign military review], 9,* 25–32 [in Russian].
2. Batsamut, V. M., Babak, S. A., & Dobranytsia, O. P. (2005). Avtomatyzatsiia protsesu pryiniattia rishennia na zastosuvannia syl viisk pry uskladnenni operatyvnoi obstanovky [Automation of the decision-making process for the use of military forces in complicating the operational situation]. *Chest i zakon [Honor and Law],* 3, 11–17 [in Ukrainian].
3. Poberezhnyi, A. A., Horielyshev, S. A., & Salnykov, O. M. (2012). Metodyka poshuku ratsionalnoho marshrutu za dopomohoiu heoinformatsiinoi systemy [Methods of searching for a rational route with the help of a geoinformation system]. In *Naukove zabezpechennia sluzhbovo-boiovoi diialnosti VV MVS Ukrainy: zb. tez dop. IV nauk.-prakt. konf. [Scientific support of service and combat activities of the Ministry of Internal Affairs of Ukraine: coll. thesis add. IV scientific-practical conf.]*. Kharkiv, February 22, 2012. (pp. 80–81). Kharkiv: Akad. VV MVS Ukraine [in Ukrainian].
4. Batsamut, V. M., Horielyshev, S. A, Poberezhnyi, A. A. (2013). Vykorystannia heoinformatsiinoi systemy u planuvanni marshu chastyn ta pidrozdiliv vnutrishnikh viisk MVS Ukrainy [Use of geoinformation system in march planning of units and subdivisions of internal troops of the Ministry of Internal Affairs of Ukraine]. *Zb. nauk. prats Akademii vnutrishnikh viisk MVS Ukrainy [Collection of scientific works of the Academy of Internal Troops of the Ministry of Internal Affairs of Ukraine], 2* (22), 21–25 [in Ukrainian].
5. Lytvynenko, N. I. (2007). Zastosuvannia HIS dlia orhanizatsii peremishchen pidrozdiliv viisk (syl) [Application of GIS for the organization of movements of divisions of troops (forces)]. In *Heoinformatsiinyi monitorynh navkolyshnoho seredovyshcha: GPSi GIS-tekhnolohii: materialy XII Mizhnar. nauk.-tekhn. Sympoziumu [Geoinformation monitoring of environment: GPS and GIS-technologies: materials XII International scientific and technical symposium]*. Alushta, September 10–15, 2007. (pp. 103–107). Alushta [in Ukrainian].
6. Pichuhin, M. F., Buchyk, S. S., Sobolenko, S. O., & Yermakov, V. O. (2010). *Osnovy viiskovoho upravlinnia. Ch. 1. Osnovy zahalnoi teorii upravlinnia [Fundamentals of military management. Part 1. Fundamentals of general management theory]*. Zhytomyr: ZhMI NAU [in Ukrainian].
7. Reshmin, B. (2016). *Imitatsionnoe modelirovanie i sistemy upravleniia [Simulation and control systems]*. Izhevsk [in Russian].
8. Hatsenko, S. S., Kalnytskyi, Yu. M., & Helveichuk, O. M. (2014). Problema rozpodilu informatsiinykh potokiv v avtomatyzovanykh systemakh upravlinnia viiskamy (sylamy) Zbroinykh Syl Ukrainy [The problem of distribution of information flows in automated control systems of troops (forces) of the Armed Forces of Ukraine]. *Zb. nauk. prats Tsentru voienno-stratehichnykh doslidzhen NUO Ukrainy im. I. Cherniakhovskoho [Coll. Science. Proceedings of the Center for Military and Strategic Studies NDU of Ukrainian named after I. Chernyakhovsky], 2* (51), 107–112 [in Ukrainian].
9. Korolenko, V. A., Siniavskii, V. K., & Vereshchagin, S. I. (2013). Avtomatizatsiia sistemy upravleniia voiskami: na puti ot idei k resheniiu [Automation of the command and control

system: on the way from idea to solution]. *Avtomatizatsiia upravleniia voiskami [Automation of command and control], 1,* 32–39 [in Russian].

O. O. Hrebenuk, M. U. Bedzay

AUTOMATED ROUTE SELECTION AND CALCULATION ALGORITHM OF DIVISION MARKET FOR SOFTWARE ADDITION MOBILE COMMUNICATIONS

The experience of the Joint forces operation shows the need to create ACS by the actions of JI units at the tactical level. This due is need to ensure the awareness of geographically distributed units, added forces and means, individual servicemen on the battlefield and a high level of efficiency in the management of units.

The article discusses the basic principles of using special software applications for mobile communications, based on geographic information system (GIS) for planning the march of units and subdivisions.

The expediency of using a mobile platform based on mobile communications as a software carrier is analyzed. Requirements for information systems based on GIS and software applications for mobile communications have been met in order to slow down the efficiency at the stage of planning the relocation of the unit. For this purpose, it is proposed to develop a software application based on the presented algorithm for calculating the march using GIS. The developed algorithm describes the sequence of actions to automate the process of choosing the optimal route on the map, the calculation of the march and its main parameters.

The developed algorithm describes the sequence of actions to automate the process of choosing the optimal route on the map, the calculation of the march and its basic parameters. It's proposed to use digital maps as cartographic services and technologies of Google Maps or Yandex Maps, which advantages are multi-layered and versatile. This approach could automate calculations, improve the efficiency and effectiveness of the commander's decision on the choice of position area and planning the march.

In future, it's worth noting the expansion of the functionality of the software application to the level of mobile information and reference system of the unit commander by developing special app, as well as the use of known software utilities and information resources.

Keywords: *geoinformation system; calculation of the traffic route; Dijkstra's method; graph theory.*

Авсієвич Роман Олексійович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– космічні системи;
– телекомунікації.

Басараба Марина Сергіївна – курсантка Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– комп'ютерні мережі та компоненти;
– інформаційна та кібернетична безпека.

Бедзай Максим Юрійович – офіцер військової частини А0515.
Наукові інтереси:
– системи радіомоніторингу.

Бугайов Микола Вікторович – кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– математичні методи й алгоритми оброблення сигналів.

Гребенюк Олег Олегович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– системи радіомоніторингу.

Гуменюк Ігор Володимирович – кандидат технічних наук, доцент кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– комп'ютерні мережі та компоненти;
– інформаційна та кібернетична безпека.

Дюков Ігор Миколайович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– радіоелектронна боротьба;
– системи зв'язку з широкосмуговими сигналами.

Єрмоленко Олександр Володимирович – науковий співробітник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки.
Наукові інтереси:
– мобільна робототехніка;
– навігаційні системи.

Живець Юрій Михайлович – науковий співробітник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки.
Наукові інтереси:
– мобільна робототехніка;
– навігаційні системи.

Зімчук Ігор Валерійович – кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– алгоритми оцінювання та управління для сучасних інформаційно-керувальних систем.

Іщенко Дем'ян Андрійович – кандидат технічних наук, доцент, старший науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– дослідження складних інформаційних систем;
– моделювання операцій.

Іщенко Сергій Дем'янович – офіцер військової частини А0515.
Наукові інтереси:
– системи моніторингу.

Кальватинський Олександр Вікторович – кандидат технічних наук, начальник лабораторії Центру прийому та обробки спеціальної інформації та контролю навігаційного поля Національного центру управління та випробувань космічних засобів Державного космічного агентства України.
Наукові інтереси:
– приймальні системи спеціальних радіоліній;
– первинна обробка спеціальної інформації;
– методи декодування спеціальної інформації.

Кирилюк Володимир Анатолійович – кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– системи моніторингу, захисту та впливу.

Кубрак Олександр Миколайович – кандидат технічних наук, доцент, начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– радіоелектронна боротьба;
– системи зв'язку з широкосмуговими сигналами.

Марищук Людмила Мічеславівна – старший науковий співробітник науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– організація наукових досліджень.

Марченков Сергій Миколайович – начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційні та психологічні операції;
– інформаційно-аналітична робота;
– національна безпека.

Наумчак Олена Михайлівна – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-психологічна безпека;
– психологічна стійкість до інформаційно-психологічних впливів.

Некрилов Олександр Володимирович – курсант Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– комп'ютерні мережі та компоненти;
– інформаційна та кібернетична безпека.

Нетребко Аліна Іванівна – помічник начальника навчальної частини факультету Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– програмування;
– інформаційні технології;
– інформаційна безпека.

Нетребко Руслан Васильович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– програмування;
– інформаційні технології;
– інформаційна безпека.

Ніцук Юрій Андрійович – доктор фізико-математичних наук, професор кафедри Одеського національного університету імені І. І. Мечникова.
Наукові інтереси:
– навігаційне обладнання.

Олійник Руслан Михайлович – начальник відділу науково-дослідного управління Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки.
Наукові інтереси:
– мобільна робототехніка;
– навігаційні системи.

Перевізна Дар'я Вікторівна – курсантка Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– атрибутна ідентифікація, технологія QR-коду;
– принципи доступу до інформаційно-телекомунікаційних систем.

Перегуда Олександр Михайлович – кандидат технічних наук, старший науковий співробітник, заступник начальника наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– проєктування, розробка та експлуатація автоматизованих систем військового призначення.

Родіонов Андрій Володимирович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– застосування та керування безпілотними авіаційними комплексами;
– інформаційні системи;
– програмування.

Самойлик Сергій Павлович – командир батальйону забезпечення навчального процесу Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– застосування безпілотних авіаційних комплексів;
– інформаційні системи.

Самчишин Олексій Володимирович – кандидат технічних наук, професор кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційна та кібернетична безпека;
– системи захисту інформації.

Семчак Олександр Миколайович – ад'юнкт науково-організаційного відділення Військової академії (м. Одеса).
Наукові інтереси:
– навігаційне обладнання.

Федорчук Дмитро Леонідович – кандидат технічних наук, начальник наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-психологічна безпека;
– психологічна стійкість до інформаційно-психологічних впливів.

Фриз Сергій Петрович – доктор технічних наук, професор, начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– проблеми планування в космічних системах;
– оптимізаційні моделі процесів у технічних системах.

Цілина Сергій Васильович – начальник науково-дослідної лабораторії Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки.
Наукові інтереси:
– мобільна робототехніка;
– навігаційні системи.

Чолпанов Вадим Олександрович – викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– радіоелектронна боротьба;
– системи зв'язку з широкосмуговими сигналами.

Шаріпова Ільнара Вільївна – аспірант Одеського національного університету імені І. І. Мечникова.
Наукові інтереси:
– навігаційне обладнання.

Шевченко Вероніка Сергіївна – курсантка Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– програмування;
– інформаційні технології;
– радіоелектронна розвідка.

ВИМОГИ ДО ОФОРМЛЕННЯ МАТЕРІАЛІВ

Стаття подається в одному примірнику друкованого тексту на білому папері формату А4 у редакторі Microsoft Word шрифтом Times New Roman, розмір літер – 12 пт, стиль – normal (звичайний), міжрядковий інтервал – 1.2, абзац з відступом 0,8 см, інтервал перед та після абзацу – 0 пт, параметри сторінки: зліва – 2,25 см, справа – 2,25 см, зверху – 2,12 см, знизу – 1,2 см, від краю до верхнього та нижнього колонтитула – 1,25 см; сторінки без нумерації. Обсяг статті від 5 до 10 сторінок (без анотацій).

Наукова праця має бути якісно відредагована та **підписана авторами** на звороті останнього аркуша із зазначенням: «У статті інформація з обмеженим доступом відсутня».

До статті додаються: **витяг з протоколу** засідання вченої (наукової, науково-технічної) ради установи (підрозділу) з обґрунтуванням доцільності опублікування роботи; **рецензія** за підписом провідного вченого в даному напрямі наукових досліджень – доктора наук; **дані про авторів** із зазначенням прізвища, імені та по батькові (повністю), наукового ступеня, вченого звання, посади або професії, наукових інтересів (обов'язково), контактного телефону, e-mail.

Разом зі статтею подається її електронний варіант з розширенням doc (e-mail, на CD-R, DVD-R) із файлами, які містять: текст статті українською мовою; прізвища, назву, анотацію (із ключовими словами) українською та англійською мовами, REFERENCES, а також дані про авторів.

ПОРЯДОК ОФОРМЛЕННЯ РУКОПИСУ

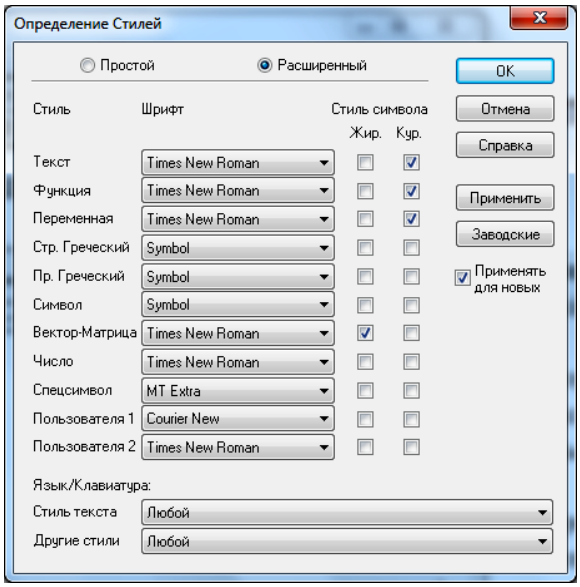
1. Індекс УДК зазначається в лівому верхньому куті перед відомостями про авторів.

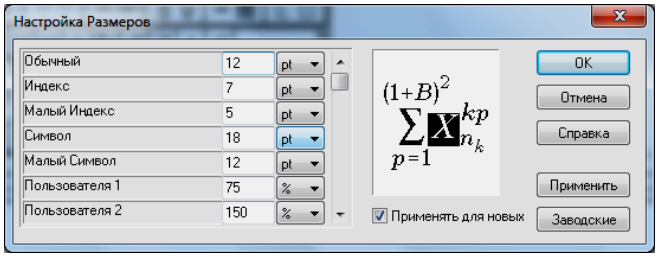
2. Ініціали та прізвища авторів – у правому куті (без наукового ступеня та вченого звання, шрифт напівжирний, без нахилу і підкреслювань).

3. Назва статті друкується великими літерами (шрифт напівжирний, без нахилу і підкреслювань) по центрі аркуша без переносів і відокремлюється від тексту одним вільним рядком зверху та знизу.

4. Анотація українською мовою з ключовими словами друкується курсивом під назвою статті й відокремлюється від заголовка та тексту одним вільним рядком. Її обсяг разом із ключовими словами має становити не менше 1800 друкованих знаків (разом із пробілами).

5. Формули в статтях повинні бути надруковані за допомогою редактора формул ***Equation Editor***. Усі параметри мають повністю відповідати наведеним нижче формам.





Усі формули розміщують у таблиці без обрамлення, по центрі, без абзацу. Номер формули зазначається посередині висоти другої колонки з виключкою вправо. Усі буквені позначення у формулах та рисунках, а також у тексті статті повинні бути однаковими за розміром і гарнітурою. Допускаються виділення напівжирним шрифтом, курсивом та підкреслювання за бажанням автора.

6. Рисунки до статті потрібно виконувати в редакторі Microsoft Word за допомогою функції «Створити малюнок». Не допускаються рисунки, оформлені як растрові зображення, або такі, що не піддаються редагуванню. Усі текстові написи на рисунках слід робити тільки в кадрах або текстових рамках. Розміри рисунка не повинні виходити за межі полів.

7. Стандартні таблиці слід виконувати в редакторі Microsoft Word. Вони повинні мати короткий заголовок.

8. Відповідно до постанови президії ВАК України від 15 січня 2003 року № 7-05/1 «Про підвищення вимог до фахових видань, внесених до переліку ВАК України» наукові статті, що подаються до друку, повинні містити такі необхідні елементи з їх зазначенням: постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями; аналіз останніх досліджень і публікацій, у яких започатковано вирішення даної проблеми та на які спирається автор, а також обов'язково виділення не вирішених раніше частин загальної проблеми, яким присвячена стаття; постановка завдання (формулювання цілей статті); виклад основного матеріалу дослідження з обґрунтуванням отриманих наукових результатів; висновки з даного дослідження і перспективи подальших розробок у даному напрямку. Список літератури (не менше 5 джерел) розміщується після статті в порядку згадування або в алфавітному порядку; посилання на літературу в тексті слід давати в квадратних дужках, наприклад, [1]. Бібліографічний опис оформлюється згідно з ДСТУ 8302:2015 «Бібліографічне посилання. Загальні положення та правила складання».

9. Після списку літератури наводиться REFERENCES, оформлений у стилі APA.

10. Далі подаються англійською мовою: прізвища авторів, назва статті, анотація та ключові слова (обсягом не менше ніж 1800 знаків разом із пробілами).

Редакція не несе відповідальності за викладену в статті інформацію. Автори відповідають за точність наведених у публікації даних, цитат, статистичних матеріалів тощо. Матеріали, оформлені з відхиленням від зазначених вимог, редколегія не розглядає.

Публікація в збірнику наукових праць безкоштовна та не передбачає отримання автором (авторами) гонорару та авторського примірника. Установа, представником якої є автор (автори) статті, включається до списку організацій, яким розсилається збірник наукових праць.

Статті приймаються за адресою: Житомирський військовий інститут імені С. П. Корольова (науково-організаційне відділення), просп. Миру, 22, м. Житомир, 10004.

Телефон для довідок: (0412) 48-30-19 (дод. 48-632, 46-675).

E-mail: nov.zvir@gmail.com

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 18

Видавничий оригінал виготовлений
у науково-організаційному відділенні ЖВІ

Редактор: **Л. М. Марищук**
Комп'ютерна верстка та макетування **Л. М. Марищук**

Свідоцтво про реєстрацію № 877 від 21 жовтня 2013 року.
Підписано до друку 12.01.2021. Формат 60 × 84 / 8.
Ум. друк. арк. 15,81. Тираж 100 прим. Зам. 15 офс.

Безкоштовно
Друкарня ЖВІ

10004, м. Житомир, просп. Миру, 22