ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Виходить 4 рази на рік

№ 66

КИЇВ – 2019

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – № 66. – 132 с.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень та побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації - серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до Наказу МОН України від 16.05.2016 № 515 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до переліку наукових фахових видань із технічних наук, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук.

Затверджено на засіданні вченої ради ВІКНУ від 19.12.2019р., протокол № 5.

Відповідальні за макет:
Ряба Л.О., Солодєєва Л.В.

Адреса редакції: 03189, м. Київ, вул. Ломоносова,81 тел./факс +38 (044) 521 – 33 – 82
Наклад 300 прим.
Ел.адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: http://miljournals.knu.ua/

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ЗАГАЛЬНІ ПИТАННЯ

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

INFORMATION TECHNOLOGIES

GENERAL QUESTIONS

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

УДК 621.396.96

д.т.н, проф. **Дружинін В.А.** (КНУ)
к.т.н. **Цьопа Н.В.** (КПІ)
к.т.н., с.н.с. **Жиров Г.Б.** (КНУ)
к.т.н., доц. **Четверіков І.О.** (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-01

СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ РАДІОЛОКАЦІЙНИХ СИСТЕМ АВІАЦІЙНО-НАЗЕМНОГО БАЗУВАННЯ ІЗ ЗМІННОЮ В ЧАСІ ВІДНОСНОЮ ПРОСТОРОВОЮ КОНФІГУРАЦІЄЮ

Робота присвячена розгляду сучасного стану та тенденції розвитку радіолокаційних систем авіаційно-наземного базування із змінною в часі відносною просторовою конфігурацією. Актуальність розгляду стану та тенденцій розвитку радіолокаційних систем авіаційно-наземного базування із змінною в часі відносною просторовою конфігурацією обумовлена практичною необхідністю отримання радіолокаційних зображень об'єктів в передній зоні огляду системи з урахуванням зростаючих вимог до оперативності й точності визначення (виявлення) зображень об'єктів спостереження в реальному масштабі часу в умовах складної сигнально-завадової обстановки.

Наведена загальна структура побудови наведених в роботі систем та визначені основні перспективи їх практичного застосування при вирішенні завдань класифікації радіолокаційних об'єктів та моніторингу джерел радіовипромінювання.

Наведено оцінки основних якісних характеристик зображень радіолокаційних об'єктів при застосуванні розглянутих систем та оцінки точності визначення координат джерел радіовипромінювання на підставі апробованого математичного апарату.

Визначені пріоритетні напрями наукових досліджень щодо подальшого розвитку теорії багатопозиційного прийому радіолокаційної інформації в умовах інформаційної невизначеності при застуванні систем із змінною в часі відносною просторовою конфігурацією.

Ключові слова: радіолокаційні системи авіаційно-наземного базування із змінною в часі відносною просторовою конфігурацією, радіолокаційний об'єкт, радіолокаційне зображення, роздільність за азимутом, радіомоніторинг, радіометричне розділення, динамічний діапазон.

Вступ та аналіз останніх досліджень. Актуальність розгляду стану та тенденцій розвитку радіолокаційних систем авіаційно-наземного базування із змінною в часі відносною просторовою конфігурацією обумовлена практичною необхідністю отримання радіолокаційних зображень (РЛЗ) об'єктів в передній зоні огляду системи з урахуванням зростаючих вимог до оперативності й точності визначення (виявлення) зображень об'єктів спостереження в реальному масштабі часу в умовах складної сигнально-завадової обстановки.

Слід зазначити, що в останній час спостерігається активне впровадження технологій робототехніки в різні галузі практичної діяльності. Використання безпілотних радіокерованих літальних апаратів - один з основних напрямків робототехніки. Дистанційно пілотовані літальні апарати (ДПЛА) вже застосовуються для вирішення таких важливих технічних завдань, як картографія та моніторинг місцевості.

Сучасні бортові радіотехнічні системи (БРТС) спостереження за земною поверхнею та навколоземним простором, що встановлюються на літальних апаратах (ЛА), мають ряд переваг (у порівнянні з оптичними системами), а саме: незначну залежність від метеорологічних умов, спроможність роботи в будь-який час, можливість вимірювань дальності поряд із кутовими координатами, що дозволяє отримувати тривимірні зображення. Всі ці переваги надають актуальність розробкам радіолокаційних систем авіаційно-наземного базування із змінною в часі відносною просторовою конфігурацією.

Актуальність запропонованої тематики підтверджується сучасними науковими і технічними тенденціями. У працях [1,2] розглянуті основи побудови багатопозиційної системи із СА. У [3,4] розглянуті основи радіомоніторингу з точки зору виконання вимог електромагнітної сумісності різних систем зв'язку, санітарних норм і законодавчих обмежень. У [5-11] розглянуті основи синтезу апертур для вирішення практичних завдань щодо підвищення роздільної здатності радіолокаційних об’єктів.

Разом з цим існує ряд практично важливих науково-технічних проблем, пов'язаних з отриманням радіозображень (РЗ) високого розділення в різних режимах спостереження, в тому числі в передній зоні огляду, та використанням даної інформації для виконання практичних завдань у процесі виявлення, розпізнавання та супроводу об'єктів спостереження.

Постановка завдання. Сучасні концепції розвитку даних систем орієнтовані на створення багатофункціональних засобів спостереження за поверхнею і повітряною обстановкою з підвищеною детальністю зображень за лінією польоту і якістю зображень, необхідних для інформаційного забезпечення польотів ЛА та споживачів такої інформації. У контексті визначених концепцій гостро стоїть питання щодо вдосконалення методів отримання і обробки зображень поверхні та повітряної обстановки в різних режимах польоту носіїв радіолокаційних засобів систем авіаційно-наземного базування. Таким чином, у роботі розглядаються питання зі створенням відповідного методичного і алгоритмічного апарату для існуючих і перспективних бортових радіолокаційних засобів (БРЛЗ) і обробки РЛЗ, який повинен охоплювати основні режими спостереження за поверхнею і повітряною обстановкою за курсом польоту ЛА на базі визначеної системи.

Основна частина. На даний час закордонними та вітчизняними фахівцями велика увага приділяється використанню теорії синтезованих апертур для вирішення практичних завдань щодо підвищення роздільної здатності радіолокаційних об’єктів [5-11].

Згідно теорії синтезованих апертур мінімальну ділянку розділення реалізує напівактивний режим моніторингу елементів місцевості, за умов: $\vec{V}_{ПРД} = \vec{V}_{ПРМ}$; $\theta_{ПРД} = \theta_{ПРМ}$; $R_н = R_п$ - відстань від об'єкту моніторингу до «підсвітлювача» набагато більша відстані від об'єкту до приймальної позиції перед початком синтезування апертури (рис. 1).

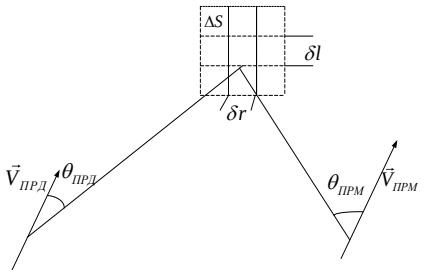


Рисунок 1 – Орієнтація векторів руху Н РЛВ відносно елементів місцевості

Структурна побудова НА РЛС АНБ, згідно з якою кожний бортовий радіолокаційний вимірювач (БРЛВ) реалізує цифрову передачу РЛІ (рис. 2), яка має наступні переваги: високу точність її трансляції й відображення, практично недосяжну при сучасній технології в аналогових системах; високу завадостійкість, можливість багаторазової ретрансляції й перезапису інформації; малу питому витрату смуги частот та зручність використання часового розподілу каналів.

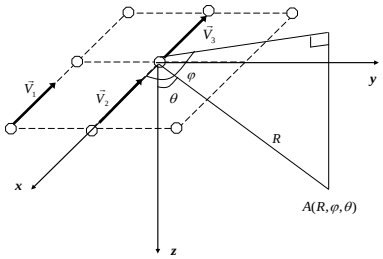


Рисунок 2 – Ескіз синтезованої прямокутної АР при керуванні польотом групи НРЛВ

Реалізація схеми ЦФ ДС на прийом у НА СРБ передбачає розробку відповідного алгоритмічного апарату, а саме: радіокерування групою (РК) НРЛВ на необхідних інтервалах часу для синтезування апертури (СА); синхронізації радіолокаційних складових системи моніторингу; спільної обробки отриманої РЛІ.

Відомо [1,2], що основою побудови багатопозиційної системи із СА є реалізація оптимальних алгоритмів спільної обробки інформації. Так спільна обробка здійснюється при наборі спостережень, вимірів або може бути змішаною.

Структура формування траєкторного сигналу та формування траєкторного сигналу при прямолінійній траєкторії згідно запропонованої методики покращення якісних характеристик зображення об'єкту моніторингу наведені на рис. 3 та рис. 4.

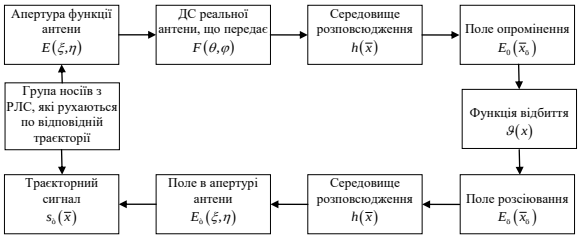


Рисунок 3 – Структура формування траєкторного сигналу

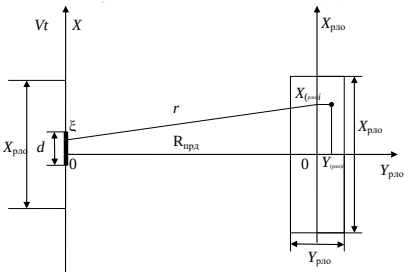


Рисунок 4 – Формування траєкторного сигналу при прямолінійній траєкторії

Поле на синтезованій апертурі, при запропонованій структурі НА РЛС АНБ, має наступний вигляд:

$$E_{CA}(t)=\left(\frac{jk}{2\pi}\right)\exp\{-j2kR_{ПРД}\}\times$$

$$\times\int\limits_{X_{РЛО}}\int\limits_{Y_{РЛО}}\vartheta(x_{РЛО},y_{РЛО})\exp\{-j2ky_{РЛО}\}\exp\left\{-jk\frac{(x_{РЛО}-(V_1+V_2+...+V_n)t)^2}{2R_{\text{н}}}\right\}F^2\left(\frac{x_{\text{ц}}-(V_1+V_2+...+V_n)t_{CA}}{2R_{ПРД}}\right)dx_{РЛО}dy_{РЛО} \tag{1}$$

Вимірювальна частина даної інформаційної системи складається з набору приймачів $i=1...Rc$ і передавача $j=1$, що рухаються за власними траєкторіями і характеризуються просторовими координатами $r_i=r_i(t),\ r_j=r_j(t)$.

При когерентному додаванні сигналів (рис. 5,6) проводиться підстроювання фази сигналу, прийнятого *m*-м веденим БРЛВ, під фазу сигналу, прийнятого i-м ведучим БРЛВ.

В ОП НПЗОІ розраховуються фази прийнятих сигналів ведучого й веденого БРЛВ за формулами

$$\varphi_i=\operatorname{arctg}\left(|u_{Si}|/|u_{Ci}|\right); \tag{2}$$

$$\varphi_m = \operatorname{arctg}\left(\left|u_{Sm}\right| / \left|u_{Cm}\right|\right). \tag{3}$$

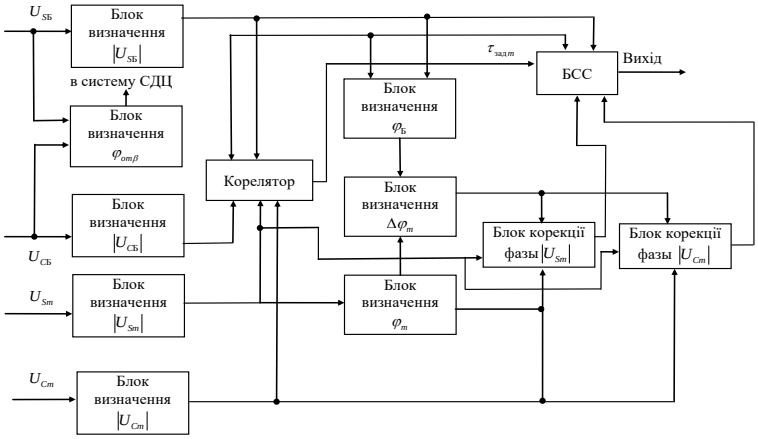


Рисунок 5 – Структурна схема ОП в режимі когерентного додавання

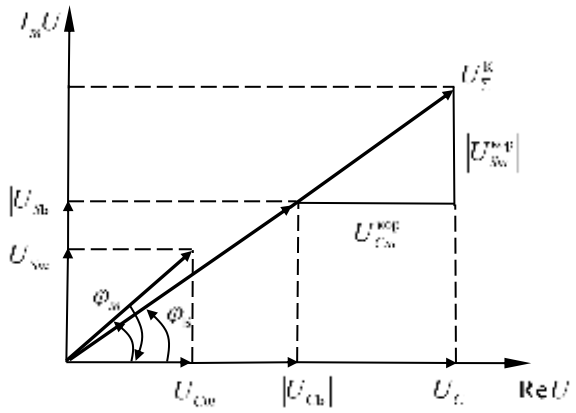


Рисунок 6 – Геометричні співвідношення при когерентному додаванні сигналів

Обчислюється фазовий зсув між сигналами, прийнятими *i*-м ведучим й *m*-м веденим БРЛВ,

$$\Delta\varphi_m = \varphi_i - \varphi_m, \tag{4}$$

який використовується в блоках корекції фази й для підстроювання фази сигналу u_m під фазу сигналу u_i за такими співвідношеннями

$$\left|u_{Sm}^{\text{кор}}\right| = \left|u_{Cm}\right|\cos\Delta\varphi_m - \left|u_{Sm}\right|\sin\Delta\varphi_m, \tag{5}$$

$$\left|u_{Cm}^{\text{кор}}\right| = \left|u_{Sm}\right|\cos\Delta\varphi_m + \left|u_{Cm}\right|\sin\Delta\varphi_m. \tag{6}$$

Коректовані модулі синусної $\left|u_{Sm}^{\text{кор}}\right|$ й косинусної $\left|u_{Cm}^{\text{кор}}\right|$ квадратурних складових подаються в БСС, де складаються у фазі із сигналом ведучого БРЛВ в момент часу, що задається блоком кореляційної прив'язки прийнятих сигналів за дальністю. Результуючий сигнал на виході БСС описується формулами:

$$u_{Sk} = \left|u_{Si}\right| + \sum_{m=2}^{M}\left|u_{Sm}^{\text{кор}}\right|, \tag{7}$$

$$u_{Ck} = \left|u_{Ci}\right| + \sum_{m=2}^{M} \left|u_{Cm}^{\text{кор}}\right|, \tag{8}$$

$$u_{\Sigma}^{\text{к}} = u_{C\text{к}} + j u_{S\text{к}} \ . \tag{9}$$

Виконання визначених процедур дозволяє реалізувати напівактивний режим, що здатний забезпечити мінімальну ділянку розділення та збільшення елементів розділення поверхні РЛО. Як відомо збільшення елементів розділення призводить до підвищення імовірності класифікації радіолокаційних об'єктів (рис. 7).

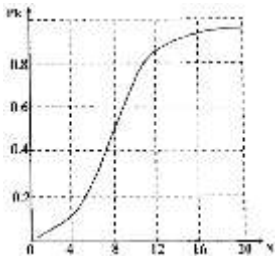
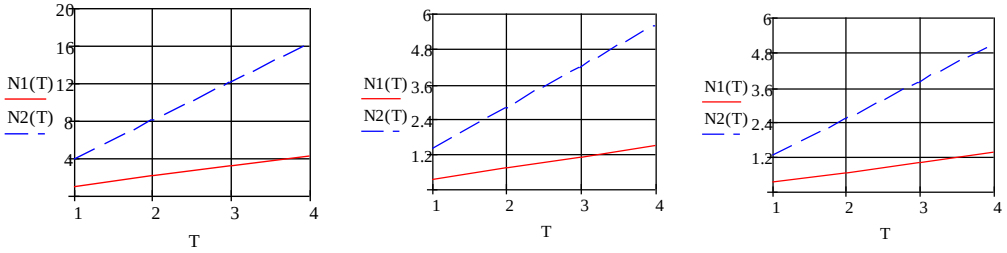


Рисунок 7 – Імовірність правильної класифікації радіолокаційного об'єкту від кількості елементів розділення радіолокаційного об'єкту

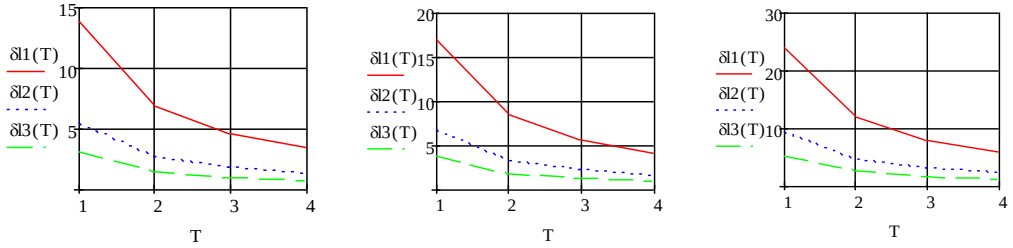
Проведена оцінка приросту кількості елементів розділення поверхні РЛО від часу СА при різних значеннях кута нагляду РЛО відносно шляхової швидкості носія θ (рис. 8). Аналіз графіків отриманих результатів показав, що запропонований в роботі режим моніторингу дозволяє значно збільшити приріст елементів розділення поверхні РЛО.



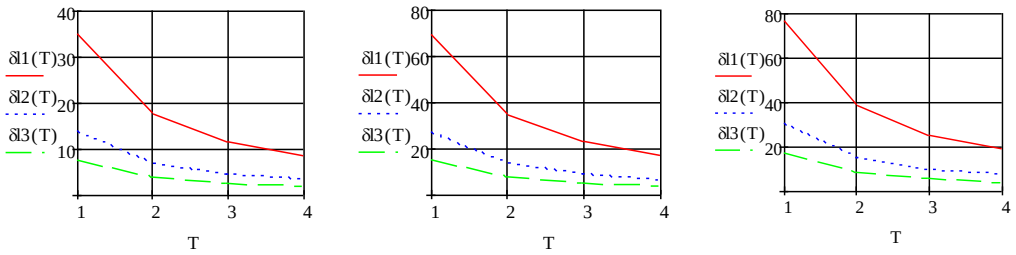
г) θ=π/9 д) θ=π/18 е) θ=π/20

Рисунок 8 – Результати оцінки приросту кількості елементів розділення поверхні РЛО від часу СА для випадків: 1 – моніторинг з однопозиційним СА (N1(T)); 2 – напівактивний режим (N2(T))

Шляхом математичного моделювання була проведена оцінка роздільної здатності за азимутом, радіометричного розділення та динамічного діапазону РЛЗ при застосуванні розробленої методики покращення якісних характеристик зображень, на підставі апробованого математичного апарату. Графіки результатів оцінки даних показників наведені на рис.9-11.

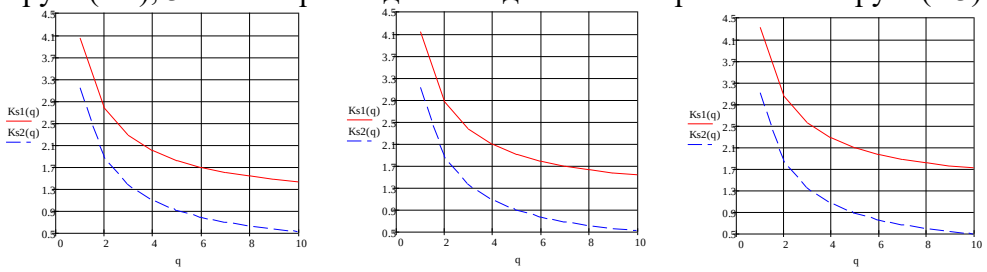


а) $\theta=\pi/3$ б) $\theta=\pi/4$ в) $\theta=\pi/6$

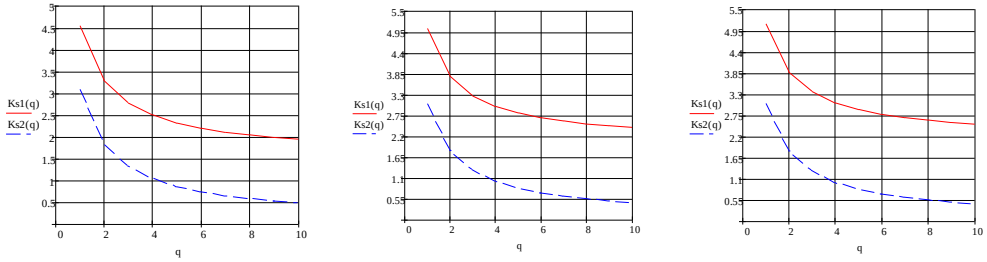


г) θ=π/9 д) θ=π/18 е) θ=π/20

Рисунок 9 – Результати оцінки лінійної роздільності НА СРБ за азимутом для випадків: 1 – моніторинг здійснює один носій (δl1); 2– моніторинг здійснює один носій в приймальній групі (δl2); 3– моніторинг здійснює два носія в приймальній групі (δl3)

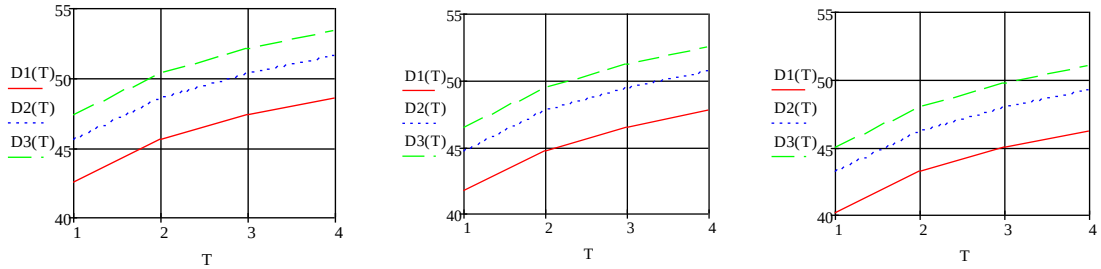


а) θ=π/3 б) θ=π/4 в) θ=π/6

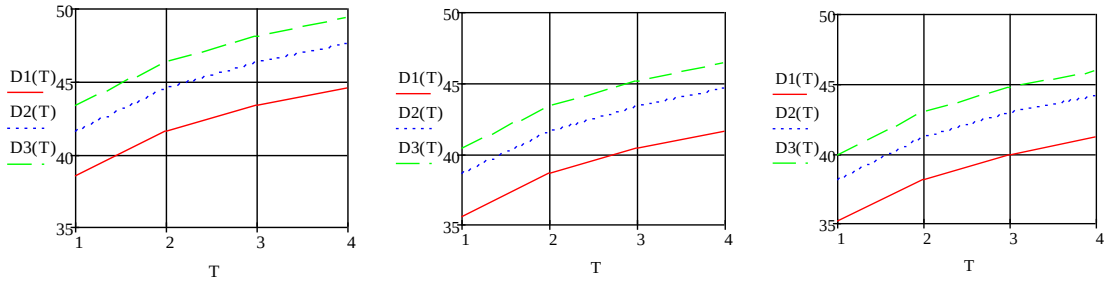


г) θ=π/9 д) θ=π/18 е) θ=π/20

Рисунок 10 – Результати оцінки радіометричного розділення радіолокаційного зображення для випадків при: 1 – однопозиційному СА (Ks1(q)); 2 – використанні запропонованого режиму моніторингу СА (Ks2(q))



а) θ=π/3 б) θ=π/4 в) θ=π/6



г) θ=π/9 д) θ=π/18 е) θ=π/20

Рисунок 11 – Результати оцінки динаміки зміни динамічного діапазону РЛЗ (після стиснення сигналу) в залежності від часу синтезування апертури для випадків: 1 – моніторинг здійснює один носій (D1(T)); 2– моніторинг здійснює два носія в приймальній групі (D2(T)); 3– моніторинг здійснює 3 носія в приймальній групі (D3(T))

Одним із перспективних завдань, які вирішуються за використанням ДПЛА, є радіомоніторинг. Розвиток бездротових інфокомунікаційних технологій призвело до суттєвого ускладнення радіоелектронної обстановки. Поряд з істотним збільшенням штатних телевізійних і радіомовних передавачів, стільникових систем зв'язку, спостерігається зростання числа несанкціонованих джерел радіовипромінювання зі зростаючою кількістю паразитних випромінювань, які не відповідають допустимим нормам. Ця обставина вимагає удосконалення технічних і організаційних засобів радіоконтролю.

Перевагою використання ДПЛА, як носіїв технічних засобів радіомоніторингу є: висока мобільність; можливість оперативного нарощування технічних засобів в заданому районі; низька вартість в порівнянні з розгортанням наземної інфраструктури; зниження кількості технічного персоналу для обслуговування визначеної системи моніторингу.

Основним завданням радіомоніторингу є контроль обстановки з метою виконання вимог електромагнітної сумісності різних систем зв'язку, санітарних норм і законодавчих обмежень [3]. Процес радіомоніторингу надається у вигляді послідовності наступних етапів: пошук радіосигналів в широкій смузі частот; виявлення радіосигналу; оцінка його характеристик; аналіз радіосигналу; прийняття рішення про відповідність випромінювання необхідним нормам. На етапі аналізу сигналу одним із основних завдань є ідентифікація джерела радіовипромінювання (ДРВ). Залежно від того до якої системи або стандарту зв'язку відноситься це ДРВ, до нього застосовуються ті чи інші обмеження щодо потужності випромінювання, паразитних випромінювань і т.і.

При розміщенні технічних засобів радіомоніторингу на мобільних носіях можливо два основні варіанти організації процесу.

У першому випадку на носії розміщується апаратура для здійснення пошуку, виявлення, реєстрації та вимірювання параметрів сигналу. Далі, отримані дані передаються на наземний пункт збору та обробки інформації (НПЗОІ), де і відбувається аналіз радіосигналу і прийняття рішення про його відповідність або невідповідність нормам. У другому варіанті, аналіз і прийняття рішення про радіосигнал здійснюється безпосередньо в апаратурі мобільного носія, а на наземний пункт передається інформація про прийняте рішення.

При використанні в якості мобільного носія технічних засобів радіомоніторингу ДПЛА, як правило, вибирається перший варіант реалізації процесу. Дана обставина обумовлена тим, що на масу корисного навантаження ДПЛА накладаються певні обмеження. Однак, постійне вдосконалення елементної бази сучасних обчислювальних пристроїв як за масогабаритними характеристиками, так і за енергоспоживанням дозволяє забезпечити розміщення апаратури аналізу і прийняття рішення на борту малорозмірних ДПЛА. Задачі ідентифікації ДРВ присвячено досить багато робіт вітчизняних і закордонних дослідників [12-15].

Застосування РЛС АНБ дозволяє значно підвищити точність оцінки координат розташування ДРВ у умовах пасивного режиму отримання інформації.

Накопичення просторово-часового сигналу від ДРВ при прямолінійному русі бортового радіолокаційного засобу мобільної системи радіоспостереження, на інтервалі часу радіомоніторингу, дозволяє підвищити точність оцінки азимуту джерела випромінювання:

$$\sigma_\beta = \left(k \left[0,88 \frac{\lambda}{\sqrt{\gamma^*}\vartheta t_M} \right]^2 + \left(\beta \frac{0,001\vartheta}{\vartheta} \right)^2 + 10^{-10} \right)^{\frac{1}{2}}, \qquad (10)$$

де: k - коефіцієнт пропорційності, який залежить від форми ДСА та способу виміру кутової координати β ; λ- довжина хвилі; β - азимут НДРВ; ϑ - швидкість руху НРПрМ; t_M - інтервал часу синтезування апертури (СА); γ^* - параметр виявлення радіовипромінювання з ймовірністю правильного виявлення $P_{ПВ} = 0,8$ при заданій імовірності хибної тривоги $P_{ХТ} = 0,1$.

Відповідним чином організована конфігурація РЛС АНБ на інтервалах часу радіоспостереження надає змогу підвищити точність оцінки координат дислокації

несанкціонованих ДРВ при умові реалізації просторово-часовою синхронізації функціонування рухомих радіолокаційних вимірювачів вище визначеної системи моніторингу.

Висновки. Визначена в роботі структурна побудова радіолокаційної системи авіаційно-наземного базування має вагомі переваги при практичному використанні, а саме: високу точність трансляції й відображення радіолокаційної інформації, практично недосяжну при сучасній технології в аналогових системах; високу завадостійкість запропонованої радіосистеми, можливість ретрансляції й перезапису інформації; малу питому витрату смуги частот та зручність використання часового розподілу інформаційних каналів системи.

Аналіз наведених в роботі результатів показав, що застосування розглянутих радіолокаційних систем авіаційно-наземного базування дозволяє:

- покращити радіометричне розділення зображення в середньому на 12-31 % одним бортовим радіолокаційним засобом у складі запропонованої системи спостереження в залежності від кута нагляду радіолокаційного об'єкту;

- підвищити динамічний діапазон зображення радіолокаційних об'єктів в середньому від 7% (при здійсненні моніторингу двома носіями в приймальній групі) до 12 % (при моніторингу трьома носіями в приймальній групі).

Перспективним завданням, які вирішуються за використанням дистанційно керованих літальних апаратів в якості радіокерованих носіїв локаційних вимірювачів параметрів джерел випромінювання є радіомоніторинг.

Підвищення ефективності радіолокаційних систем авіаційно-наземного базування при вирішенні розглянутих завдань потребує подальшого розвитку науково-методичного апарату аналізу та обробки просторово-часових сигналів від об'єктів моніторингу.

ЛІТЕРАТУРА:

1. Дружинін В. А. Проблеми формування та обробки радіолокаційної інформації в системах радіобачення: монографія. Київ: Логос, 2013. 230 с.

2. Дружинін В. А., Толюпа С.В., Наконечний В.С., Цьопа Н.В., Батрак Є.В. Методи та алгоритми обробки і захисту інформації в радіолокаційних системах із змінною просторовою конфігурацією: монографія. Київ: Логос, 2014. 251 с.

3. Дружинін В. А., Бойко Ю.М., Толюпа С.В. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів у радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад: монографія. Київ: Логос, 2018. 227 с.

4. Дружинін В.А., Наконечний В.С., Толюпа С.В., Лукова-Чуйко Н.В., Пархоменко І.І. Методи та засоби підвищення ефективності функціонування радіотехнічних систем розпізнавання багатопозиційного базування: монографія. Київ: Формат, 2019. 237 с.

5. Chaturvedi S. K. (2019), "Study of synthetic aperture radar and automatic identification system for ship target detection", Journal of Ocean Engineering and Science. pp. 173–182.

6. L. Gavrilovska, P. Latkoski, V. Atanasovski (2017), "Radio Spectrum: Evaluation Approaches, Coexistence Issues and Monitoring", Computer Networks. №121, pp. 1–12.

7. Q. N. Lu, J. J. Yang, Z. Y. Jin (2017), "State of the Art and Challenges of Radio Spectrum Monitoring in China", Radio Science. Vol.52, Issue 10, pp. 1261–1267.

8. V. V. Pavlikov, K. N. Van, O. M. Tymoshchuk (2016), "Algorithm for Radiometric Imaging by Ultrawideband Systems of Aperture Synthesis", 2016 IEEE Radar Methods and Systems Workshop (RMSW). pp. 103–106. DOI: 10.1109/RMSW.2016.7778561.

9. V. Pavlikov, V. Volosyuk, S. Zhyla (2017), "UWB active aperture synthesis radar the operating principle and development of the radar block diagram" 2017 IEEE Microwaves, Radar and Remote Sensing Symposium. pp. 27–30. DOI: 10.1109/MRRS.2017.8075018.

10. V. Pavlikov, V. Volosyuk, S. Zhyla (2017), "A New Method of Multi-Frequency Active Aperture Synthesis for Imaging of SAR Blind Zone Under Aerospace Vehicle", CADSM 2017, pp.118–120.

11. Y. Wang, Z. Gong, R. Zhang (2017), "An improved phase correction algorithm in extended towed array method for passive synthetic aperture", Proceedings of Meetings on Acoustics. pp. 1–14. https://doi.org/10.1121/2.0000643.

12. Хрипунов С.П., Чиров Д.С., Благодарящев И.В. Военная робототехника: современные тренды и векторы развития. *Тренды и управление*. Москва. 2015. № 4. С. 410-422.

13. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг: задачи, методы, средства. – 4-е изд., испр. Москва: Горячая линия - Телеком, 2015. 640 с.

14. Аджемов С.С., Кленов Н.В., Терешонок М.В., Чиров Д.С. Использование искусственных нейронных сетей для классификации источников сигналов в системах когнитивного радио. *Программирование*. Москва: РАН. 2016. № 3. С. 3-11.

15. Attar A.R., Sheikhi A., AbiriH. and Mallahzadeh A. A (2006), "New Method for Communication System Recognition", Iranian Journal of Science &Technology, Transaction B, Engineering, Vol. 30, No. B6, pp. 775-778.

REFERENCES:

1. Druzhinin V. A. Problemi formuvannja ta obrobki radiolokacijnoї informacії v sistemah radiobachennja: monografija. Kiїv: Logos, 2013. 230 p.

2. Druzhinin V. A., Toljupa S.V., Nakonechnij V.S., C'opa N.V., Batrak Є.V. Metodi ta algoritmi obrobki i zahistu informacії v radiolokacijnih sistemah iz zminnoju prostorovoju konfiguracієju: monografija. Kiїv: Logos, 2014. 251 p.

3. Druzhinin V. A., Bojko Ju.M., Toljupa S.V. Teoretichni aspekti pidvishhennja zavadostijkosti j efektivnosti obrobki signaliv u radiotehnichnih pristrojah ta zasobah telekomunikacijnih sistem za najavnosti zavad: monografija. Kiїv: Logos, 2018. 227 p.

4. Druzhinin V.A., Nakonechnij V.S., Toljupa S.V., Lukova-Chujko N.V., Parhomenko I.I. Metodi ta zasobi pidvishhennja efektivnosti funkcionuvannja radiotehnichnih sistem rozpiznavannja bagatopozicijnogo bazuvannja: monografija. Kiїv: Format, 2019. 237 p.

5. Chaturvedi S. K. (2019), "Study of synthetic aperture radar and automatic identification system for ship target detection", Journal of Ocean Engineering and Science. pp. 173–182.

6. L. Gavrilovska, P. Latkoski, V. Atanasovski (2017), "Radio Spectrum: Evaluation Approaches, Coexistence Issues and Monitoring", Computer Networks. №121, pp. 1–12.

7. Q. N. Lu, J. J. Yang, Z. Y. Jin (2017), "State of the Art and Challenges of Radio Spectrum Monitoring in China", Radio Science. Vol.52, Issue 10, pp. 1261–1267.

8. V. V. Pavlikov, K. N. Van, O. M. Tymoshchuk (2016), "Algorithm for Radiometric Imaging by Ultrawideband Systems of Aperture Synthesis", 2016 IEEE Radar Methods and Systems Workshop (RMSW). pp. 103–106. DOI: 10.1109/RMSW.2016.7778561.

9. V. Pavlikov, V. Volosyuk, S. Zhyla (2017), "UWB active aperture synthesis radar the operating principle and development of the radar block diagram" 2017 IEEE Microwaves, Radar and Remote Sensing Symposium. pp. 27–30. DOI: 10.1109/MRRS.2017.8075018.

10. V. Pavlikov, V. Volosyuk, S. Zhyla (2017), "A New Method of Multi-Frequency Active Aperture Synthesis for Imaging of SAR Blind Zone Under Aerospace Vehicle", CADSM 2017, pp.118–120.

11. Y. Wang, Z. Gong, R. Zhang (2017), "An improved phase correction algorithm in extended towed array method for passive synthetic aperture", Proceedings of Meetings on Acoustics. pp. 1–14. https://doi.org/10.1121/2.0000643.

12. Hripunov S.P., Chirov D.S., Blagodarjashhev I.V. (2015), "Voennaja robototehnika: sovremennye trendy i vektory razvitija", Trendy i upravlenie. Moskva, № 4,pp. 410-422.

13. Rembovskij A.M., Ashihmin A.V., Koz'min V.A. Radiomonitoring: zadachi, metody, sredstva. – 4-e izd., ispr. Moskva: Gorjachaja linija - Telekom, 2015. 640 p.

14. Adzhemov S.S., Klenov N.V., Tereshonok M.V., Chirov D.S. (2016), "Ispol'zovanie iskusstvennyh nejronnyh setej dlja klassifikacii istochnikov signalov v sistemah kognitivnogo radio", Programmirovanie, Moskva: RAN, № 3. pp. 3-11.

15. Attar A.R., Sheikhi A., AbiriH. and Mallahzadeh A. A (2006), "New Method for Communication System Recognition", Iranian Journal of Science &Technology, Transaction B, Engineering, Vol. 30, No. B6, pp. 775-778.

д.т.н., проф. Дружинин В.А., к.т.н. Цьопа Н.В.,
к.т.н., с.н.с. Жиров Г.Б., к.т.н., доц. Четвериков И.А.

СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ РАДИОЛОКАЦИОННЫХ СИСТЕМ АВИАЦИОННО-НАЗЕМНОГО БАЗИРОВАНИЯ С ПЕРЕМЕННОЙ ВО ВРЕМЕНИ ОТНОСИТЕЛЬНОЙ ПРОСТРАНСТВЕННОЙ КОНФИГУРАЦИЕЙ

Работа посвящена рассмотрению современного состояния и тенденций развития радиолокационных систем авиационно-наземного базирования с переменной во времени относительной пространственной конфигурацией. Актуальность анализа состояния и тенденций развития радиолокационных систем авиационно-наземного базирования с переменной во времени относительной пространственной конфигурацией обусловлена практической необходимостью получения радиолокационных изображений объектов в передней зоне обзора системы с учетом возрастающих требований к оперативности и точности определения (обнаружения) изображений объектов наблюдения в реальном масштабе времени в условиях сложной сигнально-помеховой обстановки.

Приведена обобщенная структура построения рассмотренных в работе систем и определены основные перспективы их практического применения при решении задач классификации радиолокационных объектов и мониторинга источников радиоизлучения.

Приведены оценки основных качественных характеристик изображений радиолокационных объектов при применении при применении рассмотренных систем и оценки точности определения координат источников радиоизлучения на основании апробированного математического аппарата.

Определены приоритетные направления научных исследований по дальнейшему развитию теории многопозиционного приема радиолокационной информации в условиях информационной неопределенности при использовании систем с переменной во времени относительной пространственной конфигурацией.

Ключевые слова: радиолокационные системы авиационно-наземного базирования с переменной во времени относительной пространственной конфигурацией, радиолокационный объект, радиолокационное изображение, разрешение по азимуту, радиомониторинг, радиометрической разделения, динамический диапазон.

doctor of sciences Druzhynin V., Ph.D Tsopa N., Ph.D Zhyrov H., Ph.D Chetverikov I.

CURRENT STATUS AND DEVELOPMENT TRENDS OF RADAR SYSTEMS AIRBORNE BASED WITH TIME-VARYING RELATIVE SPATIAL CONFIGURATION

The work is devoted to the review of the current state and development trends of airborne-based radar systems with a time-varying relative spatial configuration. The relevance of consideration of the state and tendencies of development of radar systems of aviation-ground based with time-varying relative spatial configuration due to the practical need to obtain radar images (radars) of objects in the front area of the system review, taking into account the growing requirements for promptness and accuracy of image detection of real-time surveillance in a complex signal-interference environment.

The generalized structure of the construction of the systems considered in the work is presented and the main prospects for their practical application in solving the problems of classifying radar objects and monitoring radio emission sources are determined.

Estimates are given of the main qualitative characteristics of the images of radar objects when applied when using the systems considered and the accuracy of determining the coordinates of radio emission sources is estimated based on an approved mathematical apparatus.

The priority areas of scientific research on the further development of the theory of multi-positional reception of radar information in the conditions of information uncertainty when using systems with a time-variable relative spatial configuration are determined.

Keywords: airborne-based radar systems with time-varying relative spatial configuration, radar object, radar image, azimuth resolution, radio monitoring, radiometric separation, dynamic range.

УДК 355.43:623.61
д.т.н., проф. **Зацерковний В.І.** (ННІ «Інститут геології» КНУ)
к.т.н., доц. **Пампуха І.В.** (ВІ КНУ)
к.т.н., доц. **Савков П.А.** (ВІ КНУ)
Синявська І.К. (ВІ КНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-02

КОНЦЕПТУАЛЬНІ ЗАСАДИ СТВОРЕННЯ СУЧАСНИХ СИСТЕМ УПРАВЛІННЯ ЗБРОЙНИМИ СИЛАМИ

Зважаючи на стрімкий розвиток інформаційних технологій (ІТ) у сфері безпеки і оборони та в цілому, управління збройними силами потребує принципово нових підходів до вирішення поставлених завдань. Мережецентрична війна (МЦВ), як форма ведення конфліктів із застосуванням мережевих форм організації, доктрини, стратегій і технологій, що пристосовані до сучасної інформаційної доби дає змогу підвищити бойові можливості різнорідних сил та засобів за рахунок синергетичного ефекту та скорочення циклу управління.

Головним елементом моделі ведення мережецентричної війни є інформація, в першу чергу розвідувальна (місце дислокації військ, стратегічні об'єкти, динаміка зміни оперативної обстановки в зоні ведення бойових дій, наземні, надводні, повітряні цілі). Загальною концепцією МЦВ є формування єдиного інформаційно-комунікаційного простору, що забезпечує всебічну інтеграцію систем управління, розвідки, зв'язку, що і буде первинним елементом на шляху досягнення синергетичного ефекту.

Функціональною особливістю концепції МЦВ є безперервність та здатність адаптуватися до динамічної обстановки і переносити функції бойового та оперативного управління на будь-який рівень по вертикалі і горизонталі відповідно до виникаючих потреб оперативного планування та управління військами.

Об'єктом дослідження являється інформаційно-технологічна складова сучасної розбудови збройних сил (ЗС), що містить в собі питання про роль ІТ у військових стратегіях розвинених країн, перед усім США, Росії та переходу на мережецентричні технології, а саме аспекти використання ІТ, мережевих технологій у плануванні і веденні сучасного бою.

Метою статті є дослідження ролі ІТ в сучасних збройних конфліктах і військових стратегіях держав, обґрунтування необхідності переходу на технології мережецентризму.

Ключові слова: високоточна зброя, інформаційні технології, мережецинтричні війни.

Вступ. Стрімкий розвиток озброєння та військової техніки, заснованої на нових фізичних, роботехнічних, біологічних та інших принципах, інформаційних і космічних технологій обумовлює постійні зміни у формах і способах ведення бойових дій.

Характерними рисами сучасних бойових дій сьогодні є широке застосування високоточної зброї (ВТЗ) повітряного (повітряно-космічного), морського і наземного базування, зростання масштабів інформаційної та радіоелектронної боротьби; набуття операціями об'ємного (повітряно-наземного) та високоманевреного характеру з одночасним проведенням взаємопов'язаних дій різних видів Збройних Сил (ЗС), родів військ на суші, у повітрі, космосі і на морі; підвищення уваги до захисту від нападу з повітря і космосу як стратегічного завдання ЗС; зростання ролі початкового періоду війни, його напруженості та можливості заподіяння противнику важких незворотних втрат, захоплення стратегічної ініціативи, а за сприятливих умов – досягнення основних воєнних цілей збройної боротьби; розгляд як першочергових об'єктів одночасного ураження масованими ракетно-авіаційними ударами не тільки розгорнутих угруповань військ (сил) противника, але й найважливіших центрів державного і воєнного управління, ключових елементів економічної та воєнної інфраструктури, районів формування стратегічних резервів тощо; підвищення здатності до швидкого переміщення на значні відстані значних угруповань військ (сил) та їх розгортання у найстисліші терміни (стратегічна мобільність); поява у зв'язку з цим у складі ЗС держав таких функціональних елементів, як сили швидкого реагування; зростання тенденції до коаліційних воєнних дій держав і створення з цією метою міжнаціональних військових формувань

(зокрема сил швидкого реагування). підтвердили тенденцію стосовно удосконалення основних форм і способів сучасної збройної боротьби [1].

Широкомасштабне та неочікуване для супротивника застосування ВТЗ на первісному етапі військових дій створює сприятливі умови не тільки для ведення обмеженої, а й загальної війни звичайними засобами. Істотне скорочення до кількох хвилин часу підготовки польотних завдань для ВТЗ та її носіїв дозволяє організувати постійний потужне вогневе ураження супротивника завдяки переходу від масованих ударів по попередньо запланованих цілях до динамічного розподілу зусиль по об'єктах ураження безпосередньо в процесі ведення бойових дій. Характерною тенденцією військових конфліктів є залучення для проведення операцій багатонаціональних сил.

Інформатизація сучасних засобів збройної боротьби дозволила створити глобальні системи розвідки, зв'язку і навігації, інтегрувати їх у єдине інформаційно-мережеве середовище, що викликало синергетичний ефект від сукупної дії бойових можливостей ВТЗ. Розвиненими країнами світу інтенсивно проводиться оптимізація та структурна перебудова своїх ЗС, головною метою якої є трансформація різноцільових сил та засобів збройної боротьби в більш гнучкі та мобільні військові формування з сучасними системами зв'язку та автоматизованими інформаційно-управлінськими системами, вдосконаленими засобами розвідувального інформаційного забезпечення та ВТЗ.

В умовах інтеграції зброї в єдиний інформаційний простір була висунута концепція *мережецентричної війни* (МЦВ) як стратегічного погляду на ведення війни в сучасних умовах. Застосування мережевих технологій під час ведення збройної боротьби дає можливість підрозділам ЗС інтенсивно маневрувати, оперативно вирішувати службово-бойові завдання на підставі безперервного отримання якісної розвідувальної інформації ефективно використовувати всі наявні бойові можливості. Концепція не обмежується розробкою нових способів застосування зброї, а передбачає докорінні зміни організаційних форм ЗС і способів ведення воєнних дій всіх масштабів, при яких практичний ефект вже досягається не стільки за рахунок підвищення вогневих, маневрових та ряду інших характеристик індивідуальних платформ озброєння, а головним чином за рахунок скорочення циклу бойового управління й прийняття рішень на основі інформаційної складової бойового простору.

Актуальність дослідження. Забезпечення національної безпеки держави є складним комплексом заходів, спрямованого на підвищення ефективності боротьби з міжнародним тероризмом, попередженням регіональних і локальних військових конфліктів, зміцненням обороноздатності країни тощо. Саме комплексність сучасних загроз ускладнює вирішення проблем старими методами управління військами. У зв'язку з цим актуальним і пріоритетним напрямком реформування ЗС більшості провідних розвинених країн є всебічна інтеграція бойових формувань і підвищення рівня їх взаємодії за рахунок всебічної інформатизації управлінських рішень, реалізації принципів нових «мережецентричних» концепцій та інтеграції систем управління, зв'язку, розвідки, ураження. Аналіз підходів щодо удосконалення ЗС цих країн, використання ІТ в управлінні військами та збройних конфліктах дає можливість визначити пріоритети будівництва ЗС України.

Аналіз останніх досліджень. Окремі аспекти удосконалення ЗС, ведення інформаційних війн та інформаційного протиборства досліджували А. Куліков, Г. Почепцов, О. Литвиненко, С. Расторгуєв, Р. Барнет, Р. Фольгеман, Б. Люїс, Д. Кюель А. Александров, В. Вепринцев, С. Базан, У. Бернхардт, М. Лейті, В. Лефевр, В. Медсен, Н. Монро, І. Панарін, Р. Роджерс, С. Саад, А. Тесфа, Т. Томас, Дж. Трауб, а також вітчизняні дослідники О. Гузько, М. Кондратюк, Ю. Кучеренко, В. Медведєв, С. Смолець та ряд інших.

Незважаючи на велику кількість публікацій присвячених цій темі, залишаються недостатньо дослідженими проблеми пов'язані з визначенням ролі ІТ у військовій справі та військових конфліктах майбутнього, необхідністю застосування геоінформаційних систем (ГІС), технологій ДЗЗ в підготовці та веденні сучасного бою.

Виклад основного матеріалу. Розвиток військового мистецтва і зміна парадигм збройної боротьби протягом усієї історії людства визначалися головним чином дальністю

ураження супротивника і кількістю ворогів, яких можна було знищити за одиницю часу. Спочатку використовувались булави і мечі, потім списи і луки, вогнепальна зброя індивідуального застосування та первинна артилерія, згодом автоматична зброя, далекобійна і реактивна артилерія, авіація дальньої дії і, врешті-решт, ракетна зброя, первісно середньої дальності, а через певний час і міжконтинентальні балістичні ракети, оснащені ядерними боєприпасами. Розвиток військової техніки постійно йшов у напрямку створення і вдосконалення бойових платформ.

Завдяки успіхам в автоматизації розвиток отримали розвідувально-ударні, розвідувально-вогневі комплекси, морські авіаносні ударні групи, які на мали озброєнні різні програмно-апаратні засоби розвідки цілей, розрахунку цілевказівки і автоматизованого або автоматичного управління засобами ураження цілей.

На сучасному етапі пріоритетними напрями розвитку ЗС розвинених країн стали:

− розвиток високоточної зброї (ВТЗ), зокрема великої дальності. Крилаті ракети повітряного, морського і наземного базування за вражаючим ефектом наблизились до зброї масового ураження, а їх застосування стало можливим через зони, що знаходяться поза досяжністю засобів протидії супротивника. Технології останніх десятиліть дозволили створити дійсно потужні, ефективні і смертоносні зразки військової техніки;

− розвиток індивідуальної зброї. Сучасний боєць, озброєний стрілецькою зброєю із запасом патронів, підствольним гранатометом і ручними гранатами, із засобами спостереження і зв’язку для обміну інформацією, по суті, також вважається бойової платформою, правда з обмеженою вогневою міццю;

− інтенсивний розвиток отримали технічні засоби розвідки, перед усім космічної та розвідки БПЛА. Супутники оптичної, інфрачервоної, радіо і радіотехнічної розвідки вже дозволяють вести безперервне і всепогодне спостереження за територією супротивника, передавати розвідувальні дані на центри їх обробки практично в реальному масштабі часу. Різного роду радіолокаційні станції (РЛС), у тому числі наземні і повітряні станції дальнього радіолокаційного виявлення систем протиракетної оборони і протиповітряної оборони (ППО), дозволяють ідентифікувати засоби ураження супротивника на великих відстанях, зокрема за горизонтом.

Одночасно з розвитком ВТЗ і засобів розвідки відбувався розвиток систем зв’язку та управління військами і озброєнням. Автоматизація і інформатизація все глибше стали проникати в армійські штаби і на командні пункти всіх рівнів.

При використанні традиційних підходів вся інформація збиралась і передавалась нагору в штаби, де опрацьовувалась і спускалась униз до підрозділів у формі наказів, директив тощо. Швидкість реагування такої системи залежала від пропускної здатності каналів зв'язку і швидкості роботи командування. Тобто, управління було централізоване, а при знищенні штабу або каналу зв'язку подібна система повністю «зависала». Крім того, час від моменту отримання розвідувальних даних, їх наступної обробки, передачі органам управління для подальших обчислень і корегування цілевказівок і до моменту одержання ударними засобами даних про цілі, був незрівнянно великим порівняно з очікуваною динамікою бойових дій, обумовленою технічними можливостями нового озброєння і військової техніки, в першу чергу швидкістю переміщення в просторі. Наскільки реальний такий висновок, дозволяє судити елементарне порівняння різних технічних засобів передачі інформації на полі бою − стандартного польового телефонного апарата ТА-57 (рис. 1) і сучасного персонального ноутбука ITRONIX GoBook MR-1 (рис. 2), що стоїть на озброєнні американської армії.

Рисунок 1 – Телефонний апарат ТА-57

Рисунок 2 – Персональний ноутбук ITRONIX GoBook MR-1

Якщо при використанні телефону процес передачі координат цілі є серйозною проблемою, то при використанні єдиної інформаційної системи (ІС) це вирішується миттєво: цілі відображуються синхронно на екранах усіх комп'ютерів, об'єднаних в одну мережу.

Отже, наявність великої кількості різноманітних даних про супротивника та його засоби ураження, даних про свої військові угруповання, бойові платформи на різних рівнях управління, потребують подальшого удосконалення розвитку систем і засобів збору і збереження даних з наступною їх інтерпретацією.

Для аналізу, оцінки і моделювання розвитку сценаріїв військових подій, підготовки варіантів для прийняття управлінських рішень з метою ефективного управління наявними силами і засобами ЗС потрібна інтеграція наявних різнорідних автоматизованих систем управління (АСУ) військами і зброєю в єдину систему, при цьому строго централізований і ієрархічний шлях проходження розвіданих про супротивника на цьому шляху, стає на цьому шляху серйозною проблемою, незважаючи на те, що швидкість передачі і обробки даних значно збільшилась. Це в значному ступені зводило нанівець потенційні ударні можливості різного роду бойових платформ і бойової техніки.

Підсумовуючи наведене, можна зробити висновки, що удосконалення й реформи ЗС, які передбачали підвищення ефективності управління військами і бойовими платформами не досягли своєї мети через низку проблем, а саме [2]:

− наявність неповної а іноді й неточної інформації про супротивника і про свої війська;

− необхідність термінового прийняття управлінських рішень, які б забезпечували виконання поставленої задачі в найкоротші терміни і з мінімально припустимими втратами;

− величезний обсяг інформації, що отримується і передається всіма рівнями управління військами при недостатній пропускній здатності ієрархічних «стволових» систем автоматизації управління і зв'язку;

− протиріччя між необхідністю жорсткої централізації управління військами і зброєю (особливо ВТЗ великої дальності і руйнівної сили) при одночасній потребі надання підпорядкованим командирам максимальної ініціативи на місця (концепція «влада на передній край»);

−стислість форми наказу (бойового розпорядження) та його змісту для його оперативного доведення до підпорядкованих сил, які повинні точно відбивати усю складність обстановки і ясність бойових задач;

− визначення пріоритетності у виборі цілей, а також засобів і способів їх ураження (знищення).

Як наслідок, якісні і кількісні зміни озброєння і військової техніки, засобів розвідки і спостереження за супротивником, засобів автоматизації управління, зв'язку і передачі даних, виявились недостатніми для проведення ефективних військових операцій. Розуміння цього врешті-решт привели до усвідомлення необхідності зміни форм і методів управління бойовими платформами при проведенні військових операцій, шляхом інтеграції систем

управління, зв'язку, розвідки та електронної боротьби на базі інформатизації та комп'ютеризації ЗС.

Першою з'явилась концепція реформування системи управління військами США С2 (Command and Control, або скорочено С2). Системи управління що відносяться до класу «С2», спроможні виконувати взаємне розпізнавання об'єктів, що входять у систему за принципом «свій-чужий», а також виконувати ідентифікацію цілей та видачу в автоматичному режимі цілевказівок наявним в системі засобам вогневого ураження. Система дозволяла командиру швидше довести прийняте їм рішення до підлеглих та проконтролювати хід його виконання. При цьому функції оцінки обстановки та прийняття рішень як і колись, повністю покладалися на «природний комп'ютер» – мозок командира. Крім того, така система дозволяла будь-якому об'єкту управління (крім безпосереднього командира) отримувати інформацію про стан і положення сусідніх підрозділів і частин.

Наступним кроком модернізації ЗС стала поява наприкінці 70-х рр. XX ст. концепції «Інтеграція систем управління і зв'язку» (С3 – Command, Control and Communications), яка передбачала систем і засобів зв'язку, які б дозволяли організувати ефективний обмін даними між різними АСУ. За рахунок реалізації цієї концепції було досягнуто потрібний рівень технічної інтеграції, розробки єдиних форматів стандартів повідомлень, безперервність і оперативність управління.

У середині 80-х рр. XX ст. її змінила нова концепція «Інтеграція систем управління, зв'язку і розвідки» (С3І – Command, Control, Communications and Intelligence), яка охоплювала вже не тільки АСУ, але й широке коло функціональних сфер діяльності та оперативного (бойового) забезпечення. Зокрема були розроблені єдині форми і способи подання даних, накопичення й відображення розвідувальної інформації поточної обстановки, створення центрів обробки і логічного аналізу з метою розподілу узагальненої інформації всім органам управління в реальному масштабі часу.

Початок 90-х рр. XX ст. ознаменувався прийняттям концепції «Інтеграція систем управління, обчислювальної техніки, зв'язку і розвідки» (С4І – Command, Control, Communications, Computers and Intelligence). В рамках її реалізації був створений єдиний комплекс інформаційно-обчислювальних мереж зі стандартним програмним і апаратним забезпечення, була досягнута високий ступінь автоматизації процесів місця розташування, цілевказівок і розподілу інформації різного виду, в тому числі через електронну пошту і телеконференцзв'язок. Були впроваджені експертні системи, засоби моделювання бойових дій, а також високопродуктивні комп'ютери.

Пропонувались і запроваджувались й інші концепції, які впроваджували планомірний процес об'єднання розрізнених засобів управління, зв'язку й розвідки, невід'ємним елементом яких була інформаційна мережа.

Концепція «мережецентризму» з'явилась наприкінці 90-х рр. XX ст. і отримала назву NCW – Network-centric Warfare і мала на меті максимальне використання можливостей усіх наявних засобів розвідки і бойових платформ. У літературі разом з цим терміном доволі часто вживаються терміни «мережецентричної», «мережево-центричної», «мережевої» війни або «мережецентричних бойових дій», «мережецентричних операцій», «мережецентричної протидії», «мережецентрування», застосування «універсальних мережецентричних засобів» тощо, упритул до «оборонного мережецентризму». При цьому різні автори часом вкладають в ці поняття зміст і значення, які сильно різняться [3-11].

Реальна інтеграція засобів розвідки і спостереження, бойових платформ, засобів автоматизації управління і зв'язку в єдину систему почала втілюватись у життя наприкінці 90-х рр. XX ст. у ЗС силах США.

Концепція МЦВ була опублікована в 1988 р. у статті віце-адмірала Артура Себровскі і наукового співробітника Міністерства США Джона Гарстка «Мережецентична війна: її походження та майбутнє» в журналі «Proceedings», які представили модель МЦВ як систему, що складається з трьох решіток-підсистем: інформаційної, сенсорної (розвідувальної) та бойової (рис. 3).

Основу цієї система складає інформаційна решітка, яка забезпечує доступ до всієї необхідної інформації. На інформаційну решітку накладаються сенсорна та бойова, які взаємно перетинаються (рис. 4).

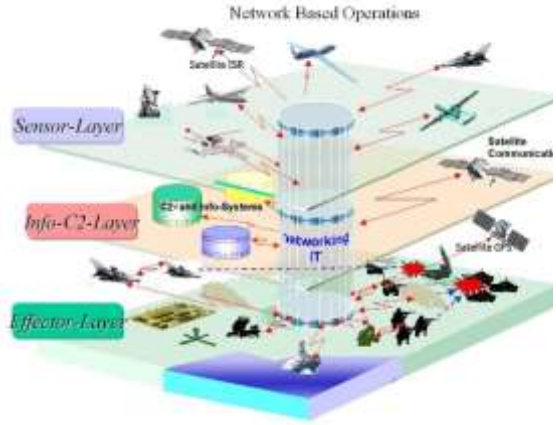


Рисунок 3 – Подання простору воєнних дій у вигляді пов’язаної мережі трьох решіток-підсистем: інформаційної, сенсорної (розвідувальної) та бойової

Рисунок 4 – Графічна інтерпретація логічної моделі "мережецентричної війни", за Себровски і Гарстка

Інформаційна решітка повністю пронизує всю систему. Елементами сенсорної решітки є "сенсори" (засоби розвідки), а елементами бойової −"стрілки" (засоби ураження). Ці дві групи елементів об’єднуються в єдине ціле органами управління і командування.

Основу інформаційно-комунікаційного простору складає Global Information Grid (GIG) − "Глобальна інформаційна решітка" (ГІР), яка являє собою потужне угруповання розвідувальних, комунікаційних і навігаційних космічних літальних апаратів на навколоземній орбіті (рис. 5).

Рисунок 5 – Глобальна інформаційна решітка

Саме ГІР пов’язує воєдино всі сили і засоби ЗС США та їх союзників по НАТО і забезпечує їх усією інформацією, необхідною для ведення війни. В результаті, реальна "картинка" бою, що відбувається в джунглях Амазонки або пісках Ближнього Сходу, миттєво висвічується на екранах військових комп’ютерів на іншому кінці світу у Вашингтоні.

Завдяки створенню єдиного інформаційно-комунікаційного простору досягається інформаційна перевага (інформаційне домінування) на полі бою, що дозволяє набагато разів ефективніше і оперативніше реалізувати бойовий потенціал угруповань військ (сил) в ході військових дій. З’являється можливість упереджувати супротивника на всіх етапах підготовки і ведення бойових дій. Протилежна сторона позбавляється можливості вжити хоч якихось відповідних кроків, у решті-решт, як вважають західні фахівці, впаде у стан повного шоку.

Компоненти інформаційних операцій для отримання інформаційного домінування представлені на рис. 6.

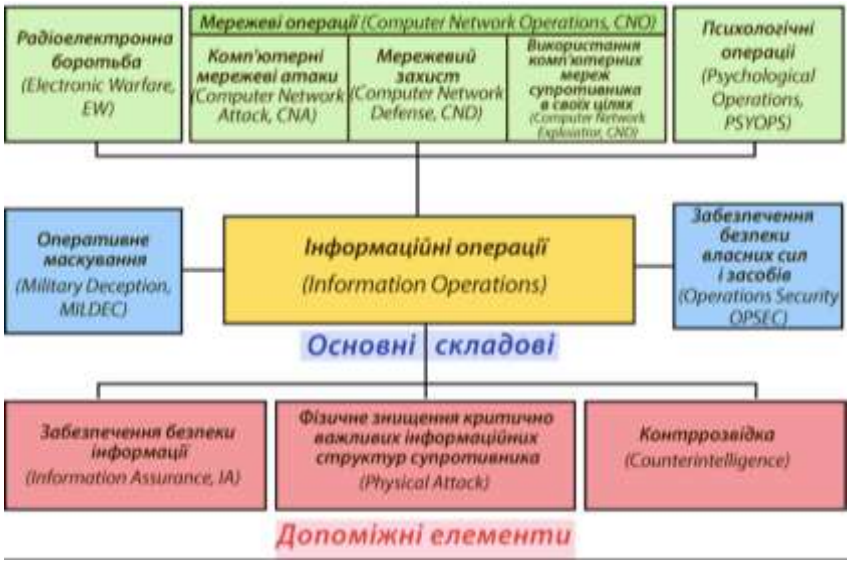


Рисунок 6 – Компоненти інформаційних операцій у ході проведення МЦВ

Взаємовідносини між усіма елементами підсистем і самими підсистемами доволі складні і багатопланові, що дозволяє, наприклад, "стрілкам" уражати цілі відразу при одержанні інформації від "сенсорів" або при одержанні наказу від органів управління, або в деяких випадках самостійно (рис. 7).

Рисунок 7 – Гнучкі алгоритми роботи бойових платформ

Концепцією МЦВ, передбачається використання розгалуженої мережі добре інформованих, географічно розосереджених сил. У військово-практичному сенсі, МЦВ дозволяє перейти від війни на виснаження до більш швидкоплинної і більш ефективної форми, для якої характерні дві основних характеристики: *швидкість управління* і *принцип самосинхронізації*.

Швидкість управління на думку американських експертів передбачає три аспекти:

− війська досягають інформаційної переваги, під якою розуміється не надходження інформації у величезних обсягах, а більш високий ступінь усвідомлення і більш глибоке розуміння ситуації на полі бою. В технологічному плані це передбачає впровадження нових систем управління, стеження, розвідки, контролю, комп'ютерного моделювання;

− завдяки своїм інформаційним перевагам війська втілюють у життя принцип масування результатів, а не масування сил;

− супротивник позбавляється можливості проводити будь-який курс дій і впадає в стан певної бездіяльності або ступору.

Як повинна працювати військова машина в умовах "мережецентричної війни", А. Себровскі і Дж. Гарстка представили так. На початковій стадії виводиться із ладу вся система ППО супротивника: командні пункти і пункти управління, центри зв'язку, позиції РЛС, бойові позиції зенітних ракет та авіації ППО. За твердженнями авторів, коли на початку конфлікту супротивник втрачає 50% чогось дуже важливого для себе, це неминуче позначається на його стратегії. Це може зупинити війну – а в цьому як раз і полягає сутність мережецентричної війни.

Принцип самосинхронізації у відповідності із теорією складних систем, стверджує, що явища і структури найкращим чином зорганізуються за принципом «знизу-вгору», тобто військові структури повинні самоорганізовуватись знизу, а не змінюватись у відповідності з указівками зверху. Організаційна структура частин і підрозділів, форми і методи виконання ними бойових задач, на думку американських фахівців, будуть змінюватись на полі бою, але у відповідності з потребами вищого командування.

Застосування системи самосинхронізації позволяє досягти переваги над супротивником у швидкості і несподіваності дій. Зникають тактичні і оперативні паузи, якими супротивник міг би скористатися, всі процеси управління і самі бойові дії стають більш динамічними, активними і результативними. Військові дії набувають не форму послідовних боїв і операцій з відповідними паузами між ними, а форму безперервних високошвидкісних дій (операцій, акцій) з рішучими цілями.

МЦВ може вестись на всіх рівнях ведення військових дій – тактичному, оперативному і стратегічному. Принципи її ведення жодним чином не залежать від географічного регіону, бойових задач, складу і структури залучених військ (сил).

Реалізація концепції МЦВ спричинила відповідні перетворення в системі підготовки військ і в їх організаційно-штатній структурі.

Концепція МЦВ лежить в основі діючих програм розвитку і вдосконалення ЗС США і передбачає глибоку інтеграцію інформаційно-телекомунікаційних, військових та соціальних мереж. При цьому, при всій важливості інформаційно-телекомунікаційних мереж, що становлять своєрідну "кровоносну систему" будь-якого військового організму, все більш важливу роль відіграють контакти і зв'язки між різними категоріями військовослужбовців: воєначальниками, що приймають рішення; начальниками і підлеглими; бойовими і підтримуючими частинами на полі бою; рядовими солдатами на полі бою. Не останню роль відіграє міжвидовий, міжвідомчий і міжнародний (коаліційний) характер таких військових "соціальних" мереж (рис. 8).

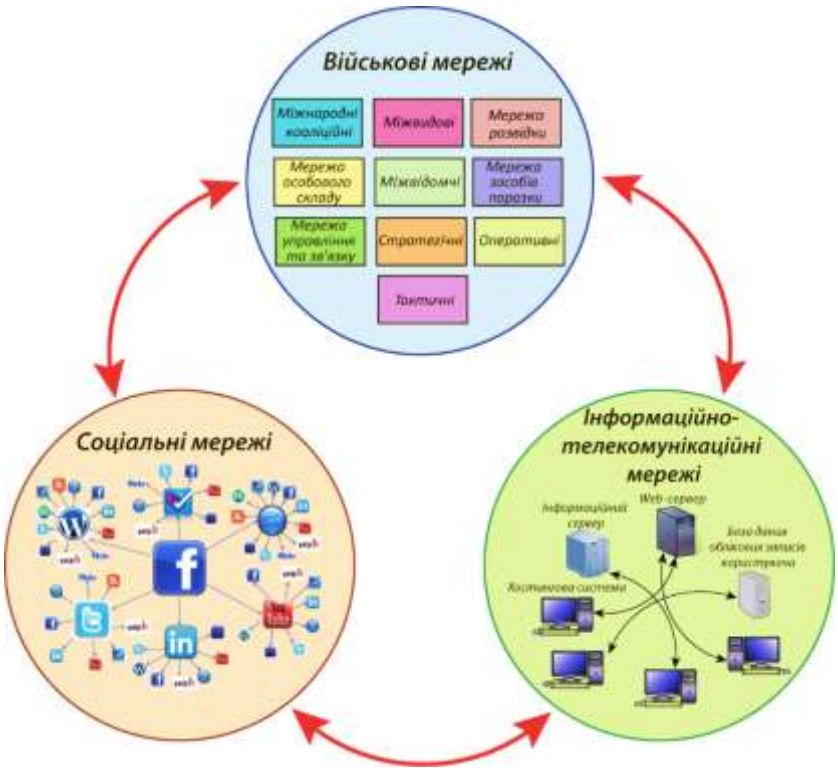


Рисунок 8 – Інтеграція інформаційно-телекомунікаційних, військових та соціальних мереж

Алгоритм ведення МЦВ, як свідчить досвід останніх війн і військових конфліктів, буде проходити в два етапи.

На першому етапі будуть наноситись високоточні повітряно-космічні удари на всю глибину території країни. Можливості ЗС США дозволяють їм застосовувати до 1 тис. крилатих ракет на добу. І це без авіації ВПС і ВМС. Потенційними цілями знищення будуть обрані критично важливі об’єкти держави супротивника. Перелік пріоритетів об’єктів ураження складаються заздалегідь, у мирний час, виходячи з концепції так званих "п’яти кілець полковника Уордена", яка розглядає супротивника як систему, що складається з п’яти радіальних кілець (рис. 9).

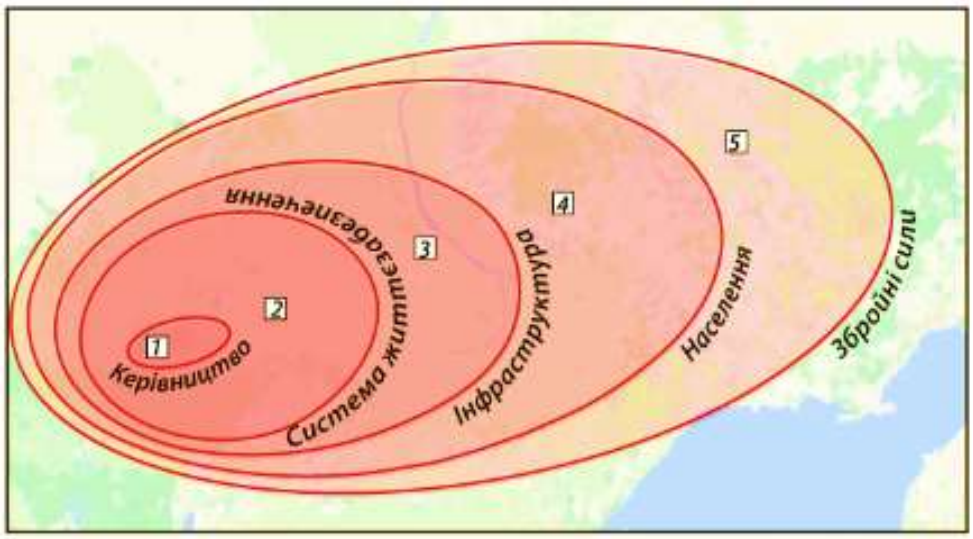


Рисунок 9 – Пріоритети об’єктів ураження (п’ять кілець полковника Уордена)

У центрі −політичне керівництво, потім йдуть системи забезпечення життєдіяльності; інфраструктура; населення і, лише в останню чергу, ЗС.

До речі, саме за цим алгоритмом розвивався збройний конфлікт між НАТО і Югославією в 1999 р.

Одночасно будуть здійснюватися масовані і скоординовані операції інформаційної війни −радіоелектронна боротьба (РЕБ), мережеві (електронне пригнічення і знищення системи державного, економічного, фінансового і військового управління, зв'язку, розвідки, РЕБ) і психологічні операції тощо.

Метою першого етапу агресії є повна дезорганізація системи державного, економічного, військового управління; "осліплення" системи розвідки і ППО країни; деморалізація населення, паніка і шок; дезорганізація військових заходів держави-жертви.

Другий етап агресії – наземне вторгнення, яке починається тільки тоді, коли буде досягнута мета першого етапу і якщо це буде визнано необхідним! По суті, це буде зачистка місцевості. Характерною особливістю другого етапу агресії є те, що угруповання військ супротивника не будуть вести класичні військові (бойові) дії. Вони будуть усіляко прагнути до того, щоб виключити навіть найменшу можливість вступу до бою [3].

Характерні риси цього етапу ведення МЦВ:

– сторона, що нападає буде випереджати супротивника на всіх етапах: збору, оцінки інформації, прийняття рішень і дії;

– не буде зосередження, висування військ, розгортання в бойовий порядок, власне атаки, переслідування або відходу на нові рубежі;

– не буде рубежів, смуг, не буде флангів, фронту та тилу;

– нападаюча сторона буде інформаційно домінувати на полі боя –бачити кожного солдата супротивника;

– жорстка ієрархічна система військового управління зміниться гнучкою мережевою: підпорядковані війська отримають свободу в виборі методів дій, а організаційно-штатна структура військ буде постійно змінюватись, "пристосовуючись" до вимог обстановки;

– широке використання нападаючою стороною тактичних наземних і повітряних робототехнічних комплексів (рис. 10), які будуть "повзати" в тилу супротивника, знищуючи осередки військового опору, що залишились.

Все це кореним чином змінює уявлення про майбутню війну, виводячи її за межі фізичної сфери в сферу інформаційну. Реальністю стає безконтактна війна. І тут вже досвід другої світової війни з організації і проведення стратегічних наступальних операцій може виявитися абсолютно марним і навіть шкідливим.

У концепції МЦВ є ще й своєрідна психологічна складова: у того, хто активно використовує переваги мережецентричних підходів, формується абсолютна впевненість у собі. Загроза життю конкретного військовослужбовця на полі боя стає мінімальною. Військові дії з поєдинку не на життя, а на смерть перетворюються в комп'ютерну гру за принципом: "Я тебе бачу, а ти мене - ні". Це, на думку авторів концепції, повинно привести до дезорганізації й деморалізації особового складу протилежної сторони ще до вступу в бойове зіткнення. Сторона, яка не використовує переваги МЦВ, в найкоротший строк повністю втрачає управління і, врешті-решт, прирікає себе на неминучу поразку.

Таким чином практична реалізація концепції «мережецентричної» війни неможлива без ефективного вирішення питань створення чотирьох ключових компонентів [13]:

− *наднадійного* (в англомовних джерелах - ultreliable) *комунікаційного середовища*, яке б забезпечувало ефективне функціонування на його основі комп'ютерних мереж ЗС та їх інтеграцію в глобальну інформаційну мережу;

− *розподіленого в просторі угруповання керованих, інформативних, надійних, довговічних і малопомітних для супротивника сенсорів*, які поєднуються в комп'ютерні мережі збройних угруповань;

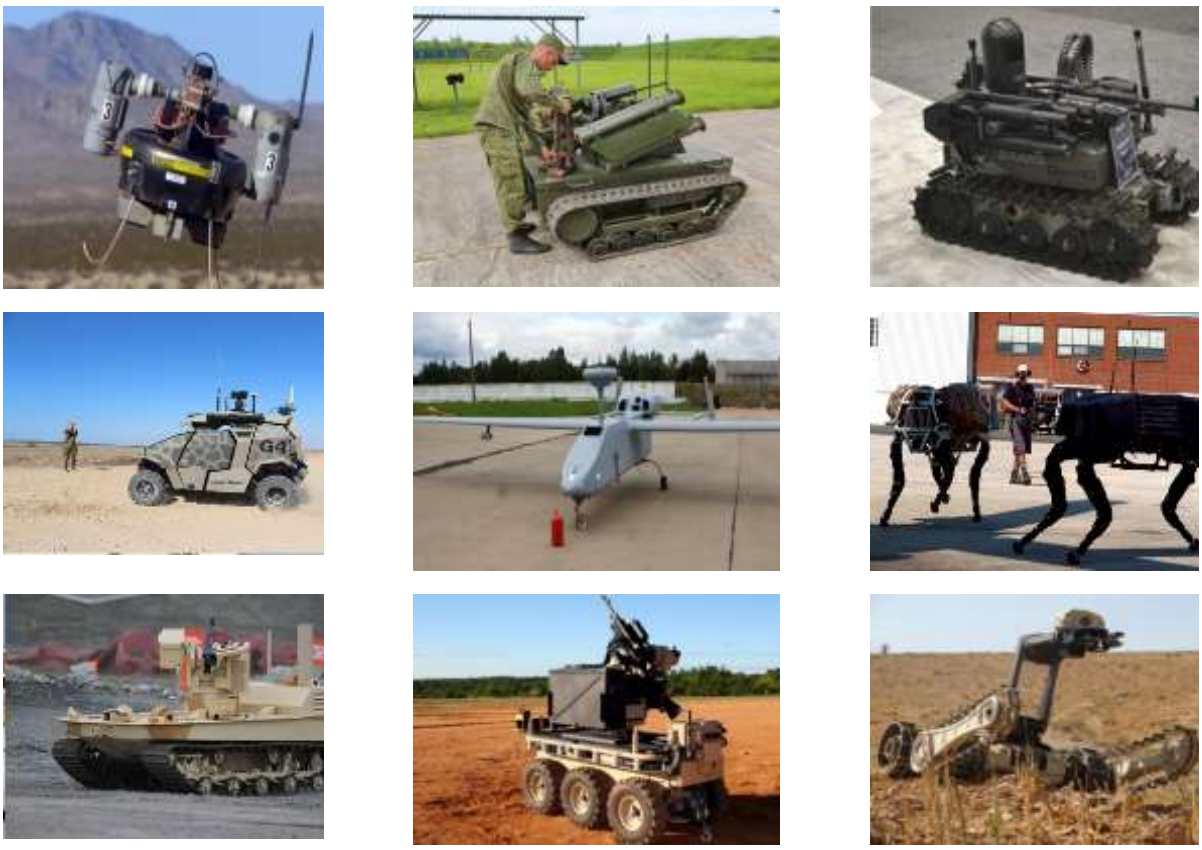


Рисунок 10 – Приклади тактичних наземних і повітряних робототехнічних комплексів

− *розподіленого програмного середовища*, яке б забезпечувало в реальному часі комплексну багаторівневу інтелектуальну обробку потоків малоінформативних в окремості (а найчастіше ще й суперечливих) первинних відомостей про прояви об’єктів, а також яке б дозволяло при необхідності оперативно змінювати логіку цієї обробки по мірі змін складу і можливостей сенсорів, отримання нових знань про контрольоване угруповання тощо;

- *кластеризації інформаційного простору* для формування заданих кластерів з метою систематизації інформації для її ефективного застосування;

Створення єдиної інформаційної мережі здатне в кілька разів збільшити потужність ЗС без збільшення їх чисельності. Мережецентрична війна дозволяє піднятися на новий рівень ефективного управління військами, значно зменшуючи час прийняття рішень.

У США та інших країнах НАТО приділяється дуже серйозна увага впровадженню ІТ і мережецентричних підходів у практику будівництва і застосування ЗС. Тільки Сухопутними військами США на досягнення цих цілей вже витрачено понад 230 млрд. доларів США. Принципи мережецентричних операцій практично відпрацьовувались ЗС США в бойових умовах в Афганістані та Іраку. При цьому, як вважають за океаном, концепція МЦВ універсальна і її можна застосувати для боротьби з супротивником будь-якого типу: регулярним і іррегулярнім, сучасним і традиційним.

Нині власні доктрини МЦВ розробляють Швеція (Network Based Defence), Великобританія (Network Enabled Capability), Сінгапур, Китай, Австралія та ряд інших країн (рис. 11).

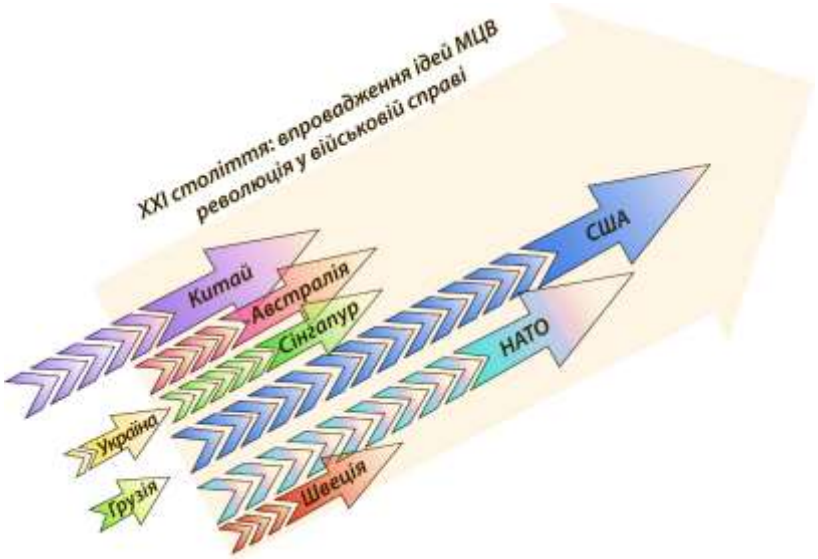


Рисунок 11 – Приклади країн, що впроваджують мережевоцентричні технології

Відбувається комп'ютеризація наукоємних озброєнь на базі космічних і лазерних технологій, кібер-військ, оновлення ракетно-космічних військ, осучаснюються усі види бойової авіації та наземних військ, здійснюється озброєння мініатюрними високоточними боєприпасами майбутнього та вже триває заміна солдатів-людей роботами-воїнами й безпілотною космічною авіацією, виявляються можливості поєднати повітряну, наземну, надводну і навіть космічну техніку в рамках цілісних бойових комплексів тощо.

Висновки. Україна має робити все можливе для входження її до переліку ЗС до кола найсильніших і найсучасніших ЗС світу з новітнім науково-технологічним військово-промисловим комплексом, набуття статусу одного з провідних військово-геополітичних гравців на євразійському просторі поряд з НАТО (чи у його складі).

МЦВ направлені на забезпечення максимального скорочення термінів циклів управління своїми військами та засобами по відношенню до противника та отримання ними повної і об'єктивної усвідомленості ситуації в зоні ведення бойових дій. З цього поняття витікає той факт, що: для реалізації положень концепції застосування високотехнологічних МЦВ необхідно мати дуже потужну економіку держави, здійснювати широкомасштабне застосування новітніх інформаційних технологій, мати потужний вітчизняний промисловий комплекс та науковий потенціал, що здатний здійснювати розробку перспективних зразків озброєння та військової техніки

Виходячи з цього можна стверджувати, що реалізація концепції «мережецентричної» війни неможлива без застосування вищенаведених ключових компонентів: наднадійного комунікаційного середовища, розподіленого в просторі угруповання керованих, інформативних, надійних, довговічних і малопомітних для супротивника сенсорів, розподіленого програмного середовища, та кластеризації інформаційного простору для формування заданих кластерів з метою систематизації інформації для її ефективного застосування. Всі ці компоненти формують єдину систему, що дозволяє здійснювати безперервну, здатну до адаптації систему управління збройними силами.

ЛІТЕРАТУРА:

1. Затуливетер Ю., Семёнов С. Ориентир – достаточная оборона. «Национальная оборона». 2012 № 11. С.12-18.

2. Ковалёв В.И., Матвиенко Ю.А. Является ли концепция «сетецентрическая» война новой парадигмой вооружённой борьбы? «Информационные войны» 2013. №1 (25). С. 21-23.

3. Кондратьев А. Сетецентрический фронт. Боевые действия в едином информационном пространстве. «Национальная оборона» 2011. № 2.

4. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию. – М.: «Евразийское движение», 2011. – 130 с.

5. «Сетевые войны: угроза нового поколения». Сборник докладов участников конференции «Сетевые войны». – М.: «Евразийское движение», 2009.

6. «Сетецентрическая война. Дайджест по материалам открытых изданий и СМИ». – М. ВАГШ ВС РФ, 2010.

7. Сидорин А.Н., Рябченко И.А., Герасимов В.П. и др. Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств: інформаційно-аналитический сборник– М.: Воениздат, 2011.

8. Слипченко В. И. Войны нового поколения: дистанционные и бесконтактные, М., «ОЛМА-ПРЕСС образование», 2004 г.

9. Слюсаренко А.В. Досвід ведення бойових дій у локальних війнах кінця XX – початку XXI століть, та його використання у підготовці ЗС України. [Електронний ресурс] Режим доступу до джерела: http://ena.lp.edu.ua/bitstream/ntb/30909/1/30.pdf

10. Шеремет И.А. Концепция «сетецентричной войны» и особенности её практической реализации [Електронний ресурс] 2005. Режим доступу до джерела: http://nvo.ng.ru/concepts/2005-11-11/4_computers.html.

11. Department of Defense. The Implementation of Network-Centric Warfare. Washington, D.C., 2005, p. 4.

REFERENCES:

1. Zatuliveter Yu., Semyonov S. 2012. Orientyr – dostatochnaya oborona. “Natsyonalnaya oborona”. № 11. C.12-18.

2. Kovalev V.I., Matvienko Yu.A. 2013. Yavlyaetsa ly kontceptcya “setecentricheskaya” voina novoy paradygmoy vooruzhennoy borby? “Infornatsyonnye voiny” №1 (25).P.21-23

3. Kondratiev A. 2011. Setetsentrycheskiy front. Boevye deistvia v edynom informatsyonnom prostranstve. “Natsyonalnaya oborona”. №2.

4. Savyn L.V. 2011. Setetsentrycheskaya & setevaya voina. Vvedenie v kontseptsiy. “Yevrasiiskoe dvizhenie”.130 p.

5. “Setevyue voiny: ygroza novogo pokolenia”. 2009. Sbornyk dokladov uchastnykov konferencyi “Setevyue voiny”. “Yevrasiiskoe dvizhenie”.

6. “Setecentrycheskaya voina. Dayjest po materialam otkrytyh izdaniy & SMI”.2010. VAGASH VS RF.

7. Sydoryn A.N., Ryabchenko I.A. Gerasymov V.P. 2011. Informatsionnye, spetsialnye, vozdushno-desantnye & aeromobilnye operatsyi vedushchyh zarubezhnyh gosudarstv: informatsyonno-analiticheskyi sbornik. Voenizdat.

8. Slyphenko V.I. Voiny novogo pokolenia: distantsyonnye & bescontaktnye. 2004.”OLMA – PRESS obrazovanie.

9. Slusarenko A.V. Dosvid vedennya boyovyh diy u localnyh viynah kintsya XX – pochatky XXI stolit, ta yogo vykorystannia u pidgotovtsi ZS Ukrainy. http://ena.lp.edu.ua/bitstream/ntb/30909/1/30.pdf

10. Sheremet I.A. 2005. Kontseptsia “setetsentrycheskoi voiny” & osobennosti eyo praktycheskoi realizatsyi. http://nvo.ng.ru/concepts/2005-11-11/4_computers.html.

11. Department of Defense. The Implementation of Network-Centric Warfare. Washington, D.C., 2005, p. 4.

д.т.н., проф. Зацерковный В.И., к.т.н., доц. Пампуха И.В.,
к.т.н., доц. Савков П.А., Синявская И.К.

АНАЛИЗ ПОДХОДОВ ПО СОЗДАНИЮ СОВРЕМЕННЫХ СИСТЕМ УПРАВЛЕНИЯ ВООРУЖЕННЫМИ СИЛАМИ

Несмотря на стремительное развитие информационных технологий в сфере безопасности и обороны и в целом, управление вооруженными силами требует принципиально новых подходов к решению поставленых задач. Сетецентрическая война, как форма ведения конфликтов с применением сетевых форм организации, доктрины, стратегий и технологий, которые приспособлены к современной информацинной эпохи позволяет повысить боевые возможности разнородных сил и средств за счет синергетического эффекта и сокращения цикла управления.

Главным елементом модели ведения сетецентрической войны является информация, в первую очередь разведывательная (место дислокации войск, стратегических объектов, динамика изменения оперативной обстановки в зоне ведения боевых действий, наземные, надводные, воздушные цели. Общий концепцией сетецентрических воен является формирование единого информационного-коммуникационного пространства обеспечивающего всестороннюю интеграцию систем управления, разведки, связи, и будет первичным елементом на пути достижения синергетического ефекта.

Функциональною особенностью концепции сетецентрических воен является непрерывность и способность адаптировается к динамической обстановке и переносить функции боевого и оперативного управления на любой уровень по вертикали и горизонтали в соответствии с возникающими потребностями оперативного планирования и управления войсками. Целью статьи является обоснование необходимости применения сетецентрической формы ведения конфликтов.

Обьектом исследования является информационно-технологическая составляющая современного развития вооруженных сил (ВС), содержащая в себе вопрос о роли ИТ в военных стратегиях развитых стран, прежде всего США, Росии и переходи не сетецентрические технологии в планировании и ведении современного боя.

Целью статьи является исследования роли ИТ в современных вооруженных конфликтах и военных стратегиях государств, обоснование необходимости перехода на технологии сетецентризма.

Ключевые слова: высокоточное оружие, информационные технологии, сетецентрические войны.

Doctor of Engineering sciences Zatserkovnyi Vitalii, PhD Pampukha Igor,
PhD Savkov Pavlo, Syniavska Iryna

ANALYSIS OF APPROACHES TO CREATE MODERN ARMED FORCE MANAGEMENT SYSTEM

Despite the development of information technology in the security and defense sector, the management of the Armed Forsec requires a fundamentaly new approach to meeting the challenges set. Network-centric warfare, as a form of conflict management with the use of network-based forms of organization, doctrine, strategies and technologies, adapted to the modern information age, allows to increase the combat capabilities of heterogeneous forces and means at the expense of synergistic effect and shortening of the management cycle.

The main element of the network-centric warfare model is information, primarily intelligence (location of troops, strategic object, dynamic of change of operational environment in the area of warfare, land, surface, air targets). The overall concept of network-centric wars is to create a single information and communication spase that provide comprehensive integration of management, intelligence, communications, wich will be a primary element in the path to achieving a synergistic effect.

A functional feature of the network-centric concept is the continuitly and ability to adapt to a dynamic environment and to transfer combat and operational control funcktions to any level vertically and horizontally in accordance to the emerging needs of operational planning and command of the troops. The poorpose of the article is to substantiate the feasibility and necessity of using a network-centric form of conflict management.

The object of research is the information and technological component of modern armed forces (AF), wich contains questions about the role of IT in the military strategies of developed countries, especially the US, Russia and the transition to network-centric technologies, namely aspects of the use of IT, network technologies in the planning and conduct of modern combat.

The purpose of the article is to research the role of IT in the current armed conflicts and military strategies of the states, rationale for the transition to network centric technology.

Key words: hight-precision weapons, information technology, network-centric wars.

УДК 528.1

к.т.н. **Кольцов Р.Ю.** (ВІКНУ)
Ванієв П.Ш. (ВІКНУ)
Індутний Д.Г. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-03

АНАЛІЗ СТАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ, ЯКІ БУЛИ СТВОРЕНІ ЗА ЧАС ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ НА СХОДІ УКРАЇНИ

У статті представлено аналіз безпілотних літальних апаратів, які були створені за час проведення антитерористичної операції на території Донецької та Луганської областей. В основі статті лежить опис особливостей використання безпілотних літальних апаратів на території Донецької та Луганської областей. Також в статті розглянуто переваги застосування безпілотних літальних апаратів під час виконання бойових або спеціальних завдань. Визначено провідні концепції створення безпілотних літальних апаратів та комплекс чинників, які обумовлюють успішність забезпечення безпілотними літальними апаратами Збройні Сили України. Було узагальнено досвід використання та забезпечення безпілотними літальними апаратами та безпілотними авіаційними комплексами за час проведення антитерористичної операції на території Донецької та Луганської областей. Наведено шляхи удосконалення традиційних способів створення безпілотних літальних апаратів та визначено для яких завдань за час проведення антитерористичної операції використовувалися безпілотні літальні апарати. У статті наведено типи безпілотних авіаційних комплексів які використовувалися в зоні Операції Об'єднаних Сил (антитерористичної операції) на території Донецької та Луганської областей українськими військовими, спецпризначенцями та гвардійцями.

В результаті проведеного у роботі дослідження розкриті особливості визначення оперативно-тактичних вимог до безпілотних літальних апаратів для їх ефективного використання на території Донецької та Луганської областей. Запропоновано раціональні шляхи створення безпілотних літальних апаратів для їх використання в інтересах бойового застосування.

Вихідними матеріалами для проведення аналізу стали деякі сучасні публікації стосовно створення та застосування безпілотних літальних апаратів для військових цілей та керівні документи. Вихідні матеріали перевірялись на предмет відповідності критеріям, поставленим керівними документами.

Ключові поняття: оперативно-тактичні вимоги, безпілотні літальні апарати та безпілотні авіаційні комплекси.

Вступ. Безпілотні літальні апарати сьогодні стали чи не головною ознакою сучасного війська. За їх кількістю та якістю у бойових порядках можна легко визначити технологічний рівень армії тієї чи іншої держави. Безпілотні авіаційні комплекси (БпАК) спроможні вирішувати широкий спектр завдань у мирний та кризовий час. Особливу вагу та значення БпАК набувають у ході бойових дій. За час проведення антитерористичної операції на сході України безпілотні авіаційні комплекси продемонстрували високу ефективність у виконанні розвідувальних завдань в інтересах усіх родів військ і завдань інтересах Ракетних військ та артилерії. Це суттєво підвищило інтерес усіх силових відомств України до оснащення своїх частин та підрозділів різними типами БпАК з урахуванням специфіки застосування. Виходячи з цього виникає задача проаналізувати безпілотні літальні апарати, які були створені за час проведення антитерористичної операції на сході України.

В ході написання статті було виявлено, що застосування безпілотних літальних апаратів на сході України відбувалося під впливом трьох основних груп факторів: особливостей умов ведення збройної боротьби, науково-технічного прогресу та воєнно-економічних чинників. На застосування безпілотних літальних апаратів найсуттєвіше впливали зміни характеру збройної боротьби, які сталися в зазначений період, та складні фізико-географічні умови районів

ведення бойових дій. Складний рельєф, кліматичні та метеорологічні умови районів конфліктів, переміщення бойових дій на міські вулиці істотно зменшували, а іноді робили неможливим застосування наземної розвідки та пілотованої розвідувальної авіації. Протягом кожного з визначених етапів розвитку встановлені характерні риси та особливості застосування безпілотних літальних апаратів. Загальними характерними рисами усього періоду стали: активне ведення розвідки за допомогою безпілотних літальних апаратів задовго до початку виникнення конфлікту; прерогатива розвідувальних даних, які добували безпілотні літальні апарати, перед традиційною кількісною перевагою в силах і засобах над противником.

Аналіз останніх досліджень та публікацій. Фундаментальною працею у питанні впливу безпілотних літальних апаратів на перебіг та результати ведення бойових дій є [1], розкрите питання визначення безпілотних літальних апаратів у працях [2], [3]. Працею, що має практичну реалізацію аналізу створення безпілотних літальних апаратів є [4], але в теперішній час можливо значно удосконалити методику, наведену в статті.

Мета статті. Метою статті є наведення найоптимальніших шляхів створення безпілотних літальних апаратів в зоні проведення антитерористичної операції.

Виклад основного матеріалу. Безпілотний літальний апарат – це літальний апарат без людини на борту, призначений для вирішення спеціальних завдань, керований дистанційно, за програмою або комбіновано і являє собою складну систему елементів випромінювання. БПЛА у бойовій обстановці вже зараз є ефективними при вирішенні завдань тактичної повітряної розвідки, цілевказання, коригування вогню артилерії, радіаційної розвідки та вирішення інших завдань. Одним із важливих завдань використання БПЛА є топографічне аерознімання для опрацювання великомасштабних планів, що, як підтвердив досвід бойових дій, вже необхідні для роботи з ними відповідним складом. Але цей процес доволі складний, оскільки потрібно дотримуватись багатьох вимог для виконання знімання: забезпечити висоту знімання для масштабності аерознімків, стабілізацію літака, щоб зменшити кути нахилу та швидкість для утримання повздовжнього перекриття тощо. Всі ці чинники дають змогу швидко виявити об’єкт та знищити його.

Основними перевагами застосування БПЛА є [5]:

- відносно невеликі розміри та малопомітність;
- низька вартість технічного обслуговування та експлуатації БПЛА;
- економія значних коштів на підготовку операторів та технічного персоналу у порівнянні з підготовкою пілотів бойових літаків;
- істотно нижча собівартість виробництва у порівняні зі звичайними літаками.

Маючи значний потенціал, Україна відставала від багатьох країн у питаннях розробки і створення безпілотної авіації. В такій ситуації без кооперації з іншими країнами розробка і серійний випуск БПАК було відкладено на досить значний час. Разом з тим з боку МО України робились деякі спроби забезпечити армію. Актуальність розробки безпілотної авіації, у першу чергу для ЗС України була обумовлена світовим досвідом воєнних конфліктів.

З початком антитерористичної операції в південно-східному регіоні України, що розпочалася з квітня 2014 р. (з кінця квітня 2018 р. – операція Об’єднаних сил), потреба в наявності на озброєнні ЗС України безпілотних авіаційних апаратів, спочатку розвідувальних, а потім і ударних, стала невідворотною. З початком війни на фронті в різні періоди використовувалося близько 30 типів найрізноманітніших, більшість із числа саморобних, безпілотних апаратів, зібраних руками волонтерів для ведення розвідки та коректування вогню.

На сьогодні в ЗС України відсутні будь-які керівні документи, які б регламентували призначення, завдання та порядок застосування ударних БПЛА [6]. Так, тільки наприкінці 2015 року, розпочалися закупівлі БПЛА вітчизняного виробництва, але тільки для ведення повітряної розвідки.

Підприємство-виробник безпілотних літальних комплексів “Меридіан”, 26 січня 2016 року передало Міноборони перший серійний зразок комплексу власного виробництва “Spectator”. Комплекс складається з трьох БПЛА і системи управління. Крім

того, у ЗС України почали поступати БПЛА типа “Фурія”, які можуть вести повітряну розвідку на дальностях до 30 км. Всього поставлено для проведення випробувань 5 комплексів по 3 БПЛА в кожному.

В той же час аналіз відкритих INTERNET-ресурсів показує, що ряд передових країн світу вже мають на озброєнні та розпочали активні роботи по розробці ударних БПЛА. Тому, існує нагальна проблема розробки програми створення ударних БПЛА, їх виробництва та відповідно затвердження керівництв з їх бойового застосування.

У зоні АТО українськими військовими, спецпризначенцями та гвардійцями використовувались безпілотні авіаційні комплекси, які можна розділити на три групи:

1. Комплекси вітчизняного виробництва, які були закуплені за державним оборонним замовленням у 2015 р. і нині знаходяться на підконтрольній експлуатації в зоні АТО, або перебувають у арсеналах військових частин. У подальшому ці комплекси можуть бути прийняти на озброєння (постачання) Збройних сил.

2. Комплекси зарубіжного виробництва, які були закуплені силовими відомствами за державні гроші, або поставлені в рамках військово-технічної допомоги.

3. Безпілотні апарати і комплекси, які були виготовлені, закуплені і передані в силові відомства волонтерами та спонсорськими організаціями.

Враховуючи обмежені ресурси держави, пріоритетність у розробці, виробництві та подальшому розвитку БПЛА повинна все ж таки надаватися тим типам, що спроможні виконувати завдання саме в інтересах бойового застосування військових частин та підрозділів, особливо ракетних та артилерійських.

За часів незалежної України були проведені як теоретичні дослідження, так і науково-дослідні (дослідно-конструкторські) роботи з обґрунтуванням доцільності виробництва та застосування БПЛА в інтересах бойового застосування військ (сил) та визначення оперативно-тактичних і тактико-технічних вимог для використання їх саме в інтересах ракетних військ і артилерії [7]. Але, відсутність державного замовлення на виробництво військового БПЛА, що пов’язане у першу чергу, з обмеженим фінансуванням Збройних Сил України призвело до їх практичної відсутності на озброєнні військ (сил). Огляд вітчизняних розробок БПЛА, що проведений в [7], показав, що такі установи як НДІ проблем фізичного моделювання (“Беркут-1”, “Сапсан”), КБ “Зліт” (“Ремез-3”, “Альбатрос-4к”, “Яструб”), Українська авіаційна компанія UA Via (R-100, R400), державне підприємство “Завод № 410 цивільної авіації” (“Моноліт”), Чугуївський авіаремонтний завод (“Стрепет”) та інші, виробляють (пропонують) декілька зразків планерів БПЛА для цивільного використання, що можуть бути модернізовані для їхнього використання в інтересах військ. Зазначені вище та інші науково-виробничі підприємства під час проведення АТО, змогли частково пристосувати деякі моделі БПЛА цивільного призначення до застосування у військах. Наприклад, БПЛА НВП “Атлон-Авіа” (“Стрепет”, “Фурія”), практично використовуються для розвідки та коригування артилерійського вогню. Разом з тим застосування БПЛА в інтересах військ не має системного характеру, відсутність штатних підрозділів, на озброєнні яких є БПЛА, унеможливлює врахування їх можливостей з ведення розвідки під час її планування [8].

Незважаючи на безумовну доцільність використання БПЛА для розвідки об’єктів противника як в тактичній, так і оперативній глибині їх застосування має безсистемний характер і є скоріше результатом роботи ентузіастів. Отже, авіаційний науково-виробничий комплекс України, за певних організаційних заходів та фінансування, здатний самостійно або у кооперації з іншими країнами (в питаннях оснащення відповідними приладами) створити БПЛА військового призначення, у тому числі в інтересах бойового застосування ракетних військ і артилерії [9]. Для пристосування вітчизняних планерів БПЛА до вимог щодо їх застосування у військових цілях доцільно здійснити їх оснащення відповідними сучасними засобами: оптичної розвідки; визначення координат у реальному масштабі часу; передачі даних (закритими каналами), що дадуть змогу здійснювати не тільки пошук цілей з повітря, а коригування застосування засобів вогневого ураження [10]. За попередніми оцінками, пристосування вітчизняних цивільних БПЛА до військових потреб на основі обґрунтованих

оперативно-тактичних вимог до них, призведе не тільки до скорочення часу на розроблення та виробництво БПЛА військового призначення, а й в першу чергу, дасть змогу визначити шляхи їх модернізації.

Враховуючи наведене вище, необхідно зазначити, що організація процесу прогнозування та планування розвитку БПЛА, як і будь-якої системи озброєння буде мати певні особливості. Ці особливості у більшості будуть визначатися існуючими підходами, що прийняті у практиці науково-дослідної діяльності та підходами, що використовують відповідні органи планування у ЗС України.

На наш погляд, планування розвитку БПЛА, як складної системи озброєння, повинне здійснюватися з урахуванням основних положень методології прогнозування розвитку систем озброєння. Важливим є дотримання принципу комплексності досліджень, що полягає у єдності науково-технічного, оперативно-тактичного та економічного прогнозування розвитку БПЛА [11].

Враховуючи ситуацію на Сході країни, ми не можемо розраховувати в цьому питанні лише на допомогу різних волонтерських організацій та рухів, оскільки такий підхід не вирішить загальної проблеми [12]. Таким чином, першочерговим завданням є розроблення єдиних вихідних даних оперативно-тактичного та воєнно-технічного характеру, що є базовим для вирішення решти питань з визначенням загального обліку БПЛА. Оперативно-тактичне обґрунтування доцільно здійснити шляхом визначення: оперативно-тактичних вимог до БПЛА [13]; організаційної структури їх можливих формувань (підрозділів); потрібної кількості у бойовому складі військ (сил) [14]. Виконання цих завдань доцільно здійснити у найкоротший термін, що необхідно для планування розвитку БПЛА і складання державного оборонного замовлення. У подальшому обов'язково необхідно здійснити оцінку потреби в різних видах ресурсів (витрат) для приведення існуючих цивільних зразків БПЛА, що взяті за основу, для подальшої їх модернізації у відповідності до визначених оперативно-тактичних і технічних вимог.

Висновки і перспективи подальших досліджень. В результаті дослідження, було виявлено, що для використання в інтересах бойового застосування угруповань військ (сил) ЗС України доцільно мати універсальні оперативно-тактичні і тактичні БПЛА. При створенні БПЛА для їх використання в інтересах бойового застосування доцільно спиратися на досвід провідних країн світу щодо виробництва БПЛА військового призначення (їх оснащення відповідним обладнанням) та вітчизняних розробників щодо розроблення та виробництва планерів БПЛА цивільного призначення.

Перспективним напрямом досліджень є проведення досліджень щодо оцінки впливу застосування БПЛА в ході бойового застосування, розроблення доцільних способів застосування БПЛА в комплексі з іншими засобами розвідки противника та обґрунтування їх раціональної кількості у бойовому складі оперативного (оперативно-тактичного) угруповання військ (сил). У подальших дослідженнях доцільно обґрунтувати вимоги до оснащення універсального оперативно-тактичного (тактичного) БПЛА відповідним обладнанням з урахуванням як існуючої, так і перспективної елементної бази.

ЛІТЕРАТУРА:

1. Безпілотна авіація у військовій справі: С.П. Мосов, М.В. Погорецький, С.М. Салій, О.В. Сєлюков, А.Л. Фещенко; за ред. проф. С.П. Мосова. – Київ: Інтерсервіс, 2019. 324 с.

2. Глотов В., Гуніна А., Телещук Ю. Аналіз можливостей застосування безпілотних літальних апаратів для військових цілей / Сучасні досягнення геодезичної науки та виробництва. – 2017. – Вип. 1. – С. 139-146.

3. Гребеников А. Г. Аналіз структури та варіантів побудови безпілотних авіаційних комплексів / Гребеников А. Г., Проценко М. М. // Вісник ЖДТУ, 2012. – Вип. 2. – С. 113–117.

4. Дубов Д. В. Нові покоління технологій подвійного призначення, як інноваційні детермінанти розвитку сфери Національної безпеки та оборони / Д. В. Дубов // Стратегічні пріоритети. – К., 2014. – Вип. 4 (33). – С.106–113.

5. Даник Ю.Г. Вимоги до оптичної системи та процесу обробки цифрових зображень

апаратурою безпілотного літального апарата / Ю. Г. Даник, М. М. Проценко // Вісник ЖДТУ, 2013. – Вип. 1. – С. 42–47.

6. Сальник Ю.П. Направление обеспечения мониторинга местности перспективной аппаратурой БПЛА / Ю. П. Сальник // Системи обробки інформації. – 2007. – № 3 (61). – С. 106–108.

7. Мосов С.П. Беспилотная разведывательная авиация стран мира. – К.: Издательский дом "Румб". – 2008. С. 160-165.

8. Радецький В.Г., Руснак І.С., Даник Ю.Г. Безпілотна авіація в сучасній збройній боротьбі : монографія. Київ : НАОУ, 2008. С. 224-229.

9. Луцький М. Г. Розвиток міжнародного регулювання та нормативної бази використання БПЛА / МГ. Луцький, В. П. Харченко, Д.О. Бугайко // Аерокосмічні системи моніторингу та керування: вісник ЖДТУ, 2011. – Вип. 2. – С. 5–14.

10. Слюсар В.И. Передача данных с борта БПЛА: стандарты НАТО / В.И. Слюсар // Электроника: наука, технология, бизнес. – 2010. – № 3. – С. 80–86.

11. Сальник Ю.П., Матала І.В. Аналіз технічних характеристик і можливостей безпілотних авіаційних комплексів оперативно-тактичного та тактичного радіуса дії армій розвинених країн : Військово-технічний зб. 2013. С. 74-77.

12. Proceedings of International Conference "Unmanned Aircraft Systems Towards Civil Applications". 2009. Graz, Austria [Електронний ресурс]. Режим доступу: http://www.fhjoanneum.at/aw/home/Studienangebot/fachbereich_information_design_technologien/lav/News_Events/lav_events/~bshr/lavevhttp://www.fhjoanneum.at/aw/home/Studienangebot/fachbereich_information_design_technologien/lav/News_Events/lav_events/~bshr/ lav-ev-/?lan=de

13. Барсов В. І. Підвищення ефективності функціонування системи обробки інформації та управління безпілотних літальних апаратів на основі застосування модулярної системи числення / В. І. Барсов, Є. О. Сотник, В. О. Жадан та ін. // Збірник наукових праць Харківського університету Повітряних сил. – 2011. – № 3 (29) – С. 90–95.

14. Proceedings of 12th International Conference & Exhibition UAS, Paris, France. 2010 [Електронний ресурс]. – Режим доступу: http://www.uas2011.org/.

REFERENCES:

1. Mosov, S.P., Pogoreckij, M.V., Salij, S.M., Syelyukov, O.V., Feshenko A.L., (2019), "Bezpilotna aviaciya u vijskovij spravi" za red. prof. Mosova, S.P., [Unmanned Aviation in Military Affairs] - Kyiv: Interservis, p. 324

2. Glotov, V., Gunina, A., Teleshuk, Yu. (2017), "Analiz mozhlivostej zastosuvannya bezpilotnih litalnih aparativ dlya vijskovih cilej" [Analysis of the possibility of using unmanned aerial vehicles for military purposes] Suchasni dosyagnennya geodezichnoyi nauki ta virobnictva. – Ed. 1. – pp. 139-146.

3. Grebenikov, A.G., (2012), "Analiz strukturi ta variantiv pobudovi bezpilotnih aviacijnih kompleksiv" [Analysis of structure and variants of construction of unmanned aerial complexes], Visnik ZhDTU, Ed. 2. – pp. 113–117.

4. Dubov, D.V., (2014), "Novi pokolinnya tehnologij podvijnogo priznachennya, yak innovacijni determinanti rozvitku sferi Nacionalnoyi bezpeki ta oboroni" [New Generations of Dual-Use Technology as Innovative Determinants of National Security and Defense]/ Strategichni prioriteti, Ed. 4 (33). – Pp.106–113.

5. Danik, Yu.G., Procenko, M.M., (2013), "Vimogi do optichnoyi sistemi ta procesu obrobki cifrovih zobrazhen aparaturoyu bezpilotnogo litalnogo aparata" [Requirements for the optical system and the process of processing digital images by unmanned aerial vehicle equipment] // Visnik ZhDTU, – Ed. 1. – pp. 42–47.

6. Salnik, Yu.P., (2007), "Napravlenie obespecheniya monitoringa mestnosti perspektivnoj apparaturoj BPLA" [Direction of providing terrain monitoring with perspective UAV equipment] / Salnik, Yu.P. // Sistemi obrobki informaciyi. – Ed. 3 (61). – pp. 106–108.

7. Mosov, S.P., (2008) "Bespilotnaya razvedyvatelnaya aviaciya stran mira" [Unmanned reconnaissance aircraft of the world] Izdatelskij dom "Rumb". pp. 160-165.

8. Radeckij, V.G., Rusnak, I.S., Danik, Yu.G. (2008) "Bezpilotna aviaciya v suchasnij zbrojnij borotba" [Unmanned Aviation in the modern armed struggle] monografiya. Kyiv: NAOU, pp. 224-229.

9. Luckij, M.G. (2011), "Rozvitok mizhnarodnogo regulyuvannya ta normativnoyi bazi vikoristannya BPLA" [Development of international regulation and regulatory framework for the use of UAVs] / Luckij, M.G., Harchenko, V.P., Bugajko D.O. // Aerokosmichni sistemi monitoringu ta keruvannya: visnik ZhDTU, Ed. 2. – pp. 5–14.

10. Slyusar, V. I. (2010), "Peredacha dannyh s borta BPLA: standarty NATO" [UAV Transmission: NATO Standards] / V. I. Slyusar // Elektronika: nauka, tehnologiya, biznes. Ed. 3. – pp. 80–86.

11. Salnik, Yu.P., Matala, I.V. (2013), “Analiz tehnichnih harakteristik i mozhlivostej bezpilotnih aviacijnih kompleksiv operativno-taktichnogo ta taktichnogo radiusa diyi armij rozvinenih krayin” [Analysis of technical characteristics and capabilities of unmanned aerial complexes of operational-tactical and tactical range of armies of developed countries] //Vijskovo-tehnichnij zb.// pp. 74-77.

12. Proceedings of International Conference “Unmanned Aircraft Systems Towards Civil Applications”. 2009. Graz, Austria [Електронний ресурс]. Режим доступу: http://www.fhjoanneum.at/aw/home/Studienangebot/fachbereich_information_design_technologien/lav/News_Events/lav_events/~bshr/lavevhttp://www.fhjoanneum.at/aw/home/Studienangebot/fachbereich_information_design_technologien/lav/News_Events/lav_events/~bshr/ lav-ev-/?lan=de

13. Barsov, V.I. (2011), “Pidvishennya efektivnosti funkcionuvannya sistemi obrobki informaciyi ta upravlinnya bezpilotnih litalnih aparativ na osnovi zastosuvannya modulyarnoyi sistemi chislennya” [Improving the efficiency of the information processing and control system of unmanned aerial vehicles based on the use of a modular numbering system] / V. I. Barsov, Ye. O. Sotnik, V. O. Zhadan ta in. // Zbirnik naukovih prac Harkivskogo universitetu Povitryanih sil. Ed. 3(29). – pp. 90–95.

14. Proceedings of 12th International Conference & Exhibition UAS, Paris, France. 2010 [Електронний ресурс]. – Режим доступу: http://www.uas2011.org/.

к.т.н. Кольцов Р.Ю., Ваниев П.Ш., Индутный Д.Г.

АНАЛИЗ СОСТОЯНИЯ ОБЕСПЕЧЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ, КОТОРЫЕ БЫЛИ СОЗДАНЫ В ХОДЕ АНТИТЕРРОРИСТИЧЕСКОЙ ОПЕРАЦИИ НА ВОСТОКЕ УКРАИНЫ

В статье представлен анализ беспилотных летательных аппаратов, которые были созданы за время проведения антитеррористической операции на территории Донецкой и Луганской областей. В основе статьи лежит описание особенностей использования беспилотных летательных аппаратов на территории Донецкой и Луганской областей. Также в статье рассмотрены преимущества применения беспилотных летательных аппаратов при выполнении боевых задач. Определены ведущие концепции создания беспилотных летательных аппаратов и комплекс факторов, обуславливающих успешность обеспечения беспилотными летательными аппаратами Вооруженные Силы Украины. Было подытожено опыт использования и обеспечения беспилотными летательными аппаратами и беспилотными авиационными комплексами за время проведения антитеррористической операции на востоке Украины. Приведены пути совершенствования традиционных способов создания беспилотных летательных аппаратов и определено для каких задач за время проведения антитеррористической операции использовались беспилотные летательные аппараты. В статье приведены типы беспилотных авиационных комплексов, которые использовались в зоне проведения Операции Объединенных Сил (антитеррористической операции) на территории Донецкой и Луганской областей украинскими военными, спецназовцами и гвардейцами.

В результате проведенного в работе исследования раскрыты особенности определения оперативно-тактических требований к беспилотным летательным аппаратам для их эффективного использования на востоке Украины. Предложено рациональные пути создания беспилотных летательных аппаратов для их использования в интересах боевого применения.

Исходными материалами для проведения анализа стали некоторые современные публикации по созданию и применению беспилотных летательных аппаратов для военных целей и руководящие документы. Исходные материалы проверялись на предмет соответствия критериям, предъявляемым руководящими документами.

Ключевые понятия: оперативно-тактические требования, беспилотные летательные аппараты и беспилотные авиационные комплексы.

Ph.D Ruslan Koltsov, Pulat Vaniyev, Dmitry Indutniy

ANALYSIS OF THE STATE OF THE PROVISION OF DRONES THAT WERE CREATED DURING THE COURSE OF THE ANTI-TERRORIST OPERATION IN THE EAST OF UKRAINE

The article presents the analysis of unmanned aerial vehicles that were created during the conduct of the anti-terrorist operation in eastern Ukraine. The article is based on the description of the features of the use of unmanned aerial vehicles in eastern Ukraine. The article also discusses the advantages of using unmanned aerial vehicles when performing combat missions. The leading concepts of creating unmanned aerial vehicles and a set of factors that determine the success of providing unmanned aerial vehicles with the Armed Forces of Ukraine are defined. The experience of using and providing unmanned aerial vehicles and unmanned aviation complexes during anti-terrorist operation in eastern Ukraine was generalized. Ways to improve the traditional methods of creating unmanned aerial vehicles and identify for which tasks unmanned aerial vehicles were used during the anti-terrorist operation. The article describes the types of unmanned aerial complexes used in the area of anti-terrorist operation by Ukrainian military, special forces and guards.

As a result of the research the peculiarities of determining operational-tactical requirements for unmanned aerial vehicles for their effective use in the east of Ukraine are revealed. The rational ways of creation of unmanned aerial vehicles for their use in the interests of combat use are offered.

The starting point for the analysis was some recent publications on the creation and use of drones for military purposes and guidance documents. The source materials were checked for compliance with the criteria set out in the guidance documents.

Key concepts: operational and tactical requirements, unmanned aerial vehicles and unmanned aerial complexes.

УДК 519.24

д.т.н., проф. **Кошевой Н.Д.** (НАКУ «ХАИ»)
д.т.н., проф. **Костенко Е.М.** (Полтавская государственная аграрная академия)
Муратов В.В. (НАКУ «ХАИ»)

DOI: https://doi.org/10.17721/2519-481X/2020/66-04

ПРИМЕНЕНИЕ МЕТОДА ПРЫГАЮЩИХ ЛЯГУШЕК ДЛЯ ОПТИМИЗАЦИИ ТРЕХУРОВНЕВЫХ ПЛАНОВ МНОГОФАКТОРНОГО ЭКСПЕРИМЕНТА

Планирование эксперимента позволяет решить задачу получения математической модели при минимальных стоимостных и временных затратах. На стоимость реализации эксперимента существенное влияние оказывает порядок чередования уровней изменения факторов. Таким образом, требуется найти порядок реализации опытов, обеспечивающий минимальную стоимость (время) проведения многофакторного эксперимента. Эта задача становится особенно актуальной при исследовании длительных и дорогостоящих процессов. Целью данной статьи является дальнейшее развитие методологии оптимального по стоимостным (временным) затратам планирования эксперимента, которая включает в себя комплекс методов оптимизации планов эксперимента и программно-аппаратные средства для их реализации. Объект исследования: процессы оптимизации по стоимостным затратам трехуровневых планов многофакторных экспериментов. Предмет исследования: метод оптимизации по стоимостным и временным затратам планов экспериментов, основанный на применении метода прыгающих лягушек. Экспериментальные методы исследования широко применяют для оптимизации производственных процессов. Одной из главных целей эксперимента является получение максимального количества информации о влиянии исследуемых факторов на производственный процесс. Далее строится математическая модель исследуемого объекта. При этом получить эти модели необходимо при минимальных стоимостных и временных затратах. Планирование эксперимента позволяет получать математические модели при минимальных стоимостных и временных затратах. Для этого были разработаны метод и программное обеспечение для оптимизации трехуровневых планов с использованием метода

прыгающих лягушек. Трехуровневые планы используют при построении математических моделей исследуемых объектов и систем. Проведен анализ известных методов синтеза оптимальных по стоимостным и временным затратам трехуровневых планов. Работоспособность алгоритма проверялась при исследовании шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов МЭМС. Показана его эффективность в сравнении со следующими методами: роя частиц, табу-поиска, ветвей и границ. С помощью разработанного метода и программного обеспечения для оптимизации трехуровневых планов с использованием метода прыгающих лягушек можно достичь высоких результатов выигрышей по сравнению с начальным планом эксперимента, оптимальных или близких к оптимальным результатов в сравнении с методами роя частиц, табу-поиска, ветвей и границ, а также высокого быстродействия решения задачи оптимизации в сравнении с разработанными ранее методами оптимизации трехуровневых планов эксперимента.

Ключевые слова: оптимальный план, метод прыгающих лягушек, оптимизация, планирование эксперимента, стоимость, время, выигрыш.

Введение. Планирование эксперимента позволяет решить задачу получения математической модели при минимальных стоимостных и временных затратах [1]. На стоимость реализации эксперимента существенное влияние оказывает порядок чередования уровней изменения факторов [2]. Таким образом, требуется найти порядок реализации опытов, обеспечивающий минимальную стоимость проведения многофакторного эксперимента. Эта задача становится особенно актуальной при исследовании длительных и дорогостоящих процессов [1].

Разработаны метод и программа оптимизации многофакторных планов эксперимента с варьированием факторов на трех уровнях с помощью алгоритма прыгающих лягушек [3]. Работоспособность метода оптимизации прыгающих лягушек доказана на примерах исследования метода измерения плотности тока гальванических ванн с использованием мерных датчиков и шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов микро электромеханических систем (МЭМС). Работоспособность и эффективность подтверждается совпадением или приближением оптимальных планов, полученных этим методом и методом роя частиц. Показана его эффективность в сравнении с другими методами оптимизации многофакторных планов эксперимента.

Объект исследования: технологические процессы и системы, позволяющие осуществление на них активного эксперимента.

Предмет исследования: метод оптимизации по стоимостным (временным) затратам планов эксперимента, основанный на применении алгоритма прыгающих лягушек [3].

Цель исследования: разработка метода и программного обеспечения для оптимизации трехуровневых планов с использованием алгоритма прыгающих лягушек и проведение сравнительного анализа разработанного метода с методом роя частиц [4].

По результатам сравнения выдаются рекомендации для использования разработанного метода.

Анализ исследований и публикаций. Известны методы синтеза оптимальных по стоимостным и временным затратам планов экспериментов с варьированием факторов на трех уровнях [1], основанные на использовании следующих видов оптимизации: анализ перестановок строк матрицы планирования [1], случайный поиск, метод табу-поиска [5], метод ветвей и границ [6]. Эффективность разработанных методов доказана при исследовании ряда различных технологических процессов, приборов и систем [1]. Однако их недостатками являются: низкое быстродействие, не всегда находится оптимальное решение. Поэтому целесообразно проверить возможность применения метода прыгающих лягушек [7] для оптимизации планов многофакторного эксперимента процесса измерения плотности тока гальванических ванн с использованием мерных датчиков и шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов МЭМС с

варьированием факторов на трех уровнях и провести сравнительный анализ результатов с методами роя частиц, табу-поиска, ветвей и границ [3].

Основные материалы исследования. Для решения поставленной задачи разработаны метод и программа для оптимизации трехуровневых планов с использованием алгоритма прыгающих лягушек [3]. С использованием разработанного программного обеспечения оптимизировался план для исследования шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов МЭМС. Исходный план эксперимента 3^k, а также описание метода определения шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов МЭМС, приведены в работе [1]. При составлении плана эксперимента были учтены три входных фактора процесса, предположительно способных в наибольшей степени влиять на оптимизируемый параметр (среднее арифметическое отклонение профиля): X_1 – отношение длительности стадий пассивации и травления; X_2 – давление в реакторе, Па; X_3 – температура электрода-подложкодержателя, ^oC. Условия проведения эксперимента представлены в табл. 1. В табл. 2 представлены стоимости изменений значений уровней факторов.

Сущность метода прыгающих лягушек и программы, обеспечивающей его реализацию для оптимизации трехуровневых планов, заключается в следующем. В начале работы программы вводится количество факторов k, после чего осуществляется ввод стоимостей (времен) переходов между уровнями факторов и строится матрица планирования эксперимента трехуровневого плана. Затем осуществляется вычисление начальной стоимости (времени) проведения эксперимента и происходит генерация матрицы сумм стоимостей (времен) переходов между уровнями для каждого из факторов. Выполняется сортировка столбцов по индексам и генерация массивов индексов для сумм стоимостей (времен) переходов между уровнями для каждого из факторов. Затем происходят перестановки столбцов в соответствии с массивом индексов для сумм стоимостей (времен) переходов между уровнями для каждого из факторов. Выполняется построчный перебор между всеми блоками столбцов (мемеплексов, в которых перемещается лягушка) и определение начальной точки для дальнейшего перебора, исходя из наименьшей суммы стоимостей (времен) переходов между уровнями для каждого из факторов. Также программой выполняется поиск в рамках блока столбца, в котором находится лягушка по минимальному значению суммы стоимостей (времен) переходов между уровнями для каждого из факторов, после чего происходит переход на следующую строку матрицы планирования и сравнение с предыдущей. Осуществляется поиск в блоке столбца с наименьшим значением суммы стоимостей (времен) переходов между уровнями и установление соответствующего блока (перестановка местами в матрице планирования эксперимента). После реализации необходимых перестановок выполняются: построение оптимальной матрицы планирования эксперимента; расчет общей стоимости (времени) реализации эксперимента; расчет выигрыша B; расчет времени *t*, затраченного на оптимизацию трехуровневого плана многофакторного эксперимента с использованием метода прыгающих лягушек.

Таблица 1

Условия проведения эксперимента

Наименование параметров	Обозначение	Входные факторы		
		X_1	X_2	X_3
Нулевой уровень	0	0,2	3	20
Интервал варьирования	ΔX_i	0,1	1	10
Нижний уровень	-1	0,1	2	10
Верхний уровень	+1	0,3	4	30

Таблица 2

Стоимости изменения значений уровней факторов

Стоимости изменений, усл. ед.	Обозначение факторов		
	X_1	X_2	X_3
из «0» в «-1»	3	7	8
из «0» в «+1»	2	5	10
из «-1» в «+1»	4	10	20
из «+1» в «-1»	6	14	16
из «-1» в «0»	2	5	10
из «+1» в «0»	3	7	8

Режимы проведения процессов травления кремния задавали в соответствии с выбранным планом (табл. 3), который представлял собой полный факторный эксперимент для трех факторов при их одновременном варьировании на трех уровнях: «+1», «-1», «0». Оптимальный план эксперимента, полученный с использованием разработанного программного обеспечения, реализующего алгоритм прыгающих лягушек, также представлен в табл. 3.

Таблица 3

Исходный и оптимальный планы эксперимента

Исходный план				Оптимальный план (метод прыгающих лягушек)				Оптимальный план (метод роя частиц)			
Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов		
	X_1	X_2	X_3		X_1	X_2	X_3		X_1	X_2	X_3
1	-1	0	0	16	-1	-1	0	1	-1	0	0
2	-1	0	-1	26	0	-1	0	19	0	0	0
3	+1	-1	-1	18	+1	-1	0	10	-1	-1	+1
4	0	0	+1	6	+1	+1	0	22	0	-1	+1
5	+1	0	0	27	-1	+1	0	7	-1	+1	+1
6	+1	+1	0	24	0	+1	0	4	0	0	+1
7	-1	+1	+1	4	0	0	+1	13	-1	+1	-1
8	+1	0	+1	19	0	0	0	25	+1	0	-1
9	+1	+1	+1	1	-1	0	0	16	-1	-1	0
10	-1	-1	+1	20	-1	0	+1	26	0	-1	0
11	+1	+1	-1	5	+1	0	0	2	-1	0	-1
12	0	0	-1	8	+1	0	+1	20	-1	0	+1
13	-1	+1	-1	14	+1	-1	+1	23	0	+1	+1
14	+1	-1	+1	22	0	-1	+1	5	+1	0	0
15	0	+1	-1	10	-1	-1	+1	15	0	+1	-1
16	-1	-1	0	13	-1	+1	-1	6	+1	+1	0
17	0	0	-1	7	-1	+1	+1	18	+1	-1	0
18	+1	-1	0	23	0	+1	+1	3	+1	-1	-1
19	0	0	0	15	0	+1	-1	27	-1	+1	0
20	-1	0	+1	9	+1	+1	+1	9	+1	+1	+1
21	-1	-1	-1	11	+1	+1	-1	17	0	0	-1
22	0	-1	+1	25	+1	0	-1	8	+1	0	+1
23	0	+1	+1	2	-1	0	-1	11	+1	+1	-1
24	0	+1	0	12	0	0	-1	14	+1	-1	+1
25	+1	0	-1	17	0	0	-1	12	0	0	-1

Исходный план				Оптимальный план (метод прыгающих лягушек)				Оптимальный план (метод роя частиц)			
Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов		
	X_1	X_2	X_3		X_1	X_2	X_3		X_1	X_2	X_3
26	0	-1	0	21	-1	-1	-1	21	-1	-1	-1
27	-1	+1	0	3	+1	-1	-1	24	0	+1	0

Оптимизированный план эксперимента имеет значение стоимости реализации, равное 181 усл.ед., в то время как исходный план – 417 усл.ед. Выигрыш по стоимости составил 2,31 раза, в то время как при использовании метода ветвей и границ выигрыш составлял 1,28 раза. При этом на оптимизацию плана необходимо затратить 0,03 с, в то время как на реализацию метода ветвей и границ – 137 мин, а на реализацию метода роя частиц – 0,33 с. С использованием разработанного программного обеспечения исследовали метод измерения плотности тока гальванических ванн с мерными датчиками. Исходный план эксперимента 3^k, а также описание метода измерения плотности тока гальванических ванн с использованием мерных датчиков, приведены в работе [1]. Методом прыгающих лягушек проведена оптимизация исходного плана по критерию суммарной стоимости реализации эксперимента. Стоимости изменений значений уровней факторов приведены в табл. 4. Порядок проведения опытов оптимального по стоимости реализации плана эксперимента представлен в табл. 5. Стоимость реализации эксперимента по этому плану составляет 87 усл. ед., тогда как стоимость реализации исходной матрицы планирования – 174 усл. ед. Таким образом, достигнут выигрыш по стоимости реализации в 2 раза по сравнению с исходным планом проведения эксперимента.

Таблица 4

Стоимости изменений значений уровней факторов

Стоимости изменений, усл. ед.	Обозначение факторов		
	X_1	X_2	X_3
из «0» в «-1»	3	3	3
из «0» в «+1»	2	2	2
из «-1» в «+1»	5	5	5
из «+1» в «-1»	5	5	5
из «-1» в «0»	3	3	3
из «+1» в «0»	2	2	2

Сравнение результатов при использовании усовершенствованного программного обеспечения по методу оптимизации прыгающих лягушек и ранее разработанных методов [3] приведено в табл. 6. Таким образом, доказана работоспособность метода прыгающих лягушек на примерах исследования шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов МЭМС и метода измерения плотности тока гальванических ванн с использованием мерных датчиков.

Таблица 5

Исходный и оптимальный планы эксперимента

Исходный план				Оптимальный план (метод прыгающих лягушек)				Оптимальный план (метод роя частиц)			
Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов		
	X_1	X_2	X_3		X_1	X_2	X_3		X_1	X_2	X_3
1	-1	0	0	6	+1	+1	0	1	-1	0	0
2	-1	0	-1	7	-1	+1	0	10	+1	+1	+1
3	+1	-1	-1	25	0	+1	0	19	+1	-1	0
4	0	0	+1	27	0	+1	0	20	0	0	0
5	+1	0	0	19	+1	-1	0	2	-1	0	-1

Исходный план				Оптимальный план (метод прыгающих лягушек)				Оптимальный план (метод роя частиц)			
Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов			Номер опыта	Обозначение факторов		
	X_1	X_2	X_3		X_1	X_2	X_3		X_1	X_2	X_3
6	+1	+1	0	17	-1	-1	0	3	+1	-1	-1
7	-1	+1	0	1	-1	0	0	21	-1	0	+1
8	-1	+1	+1	21	-1	0	+1	24	0	+1	+1
9	+1	0	+1	5	+1	0	0	6	+1	+1	0
10	+1	+1	+1	9	+1	0	+1	4	0	0	+1
11	-1	-1	+1	20	0	0	0	22	-1	-1	-1
12	+1	+1	-1	4	0	0	+1	13	0	0	-1
13	0	0	-1	23	0	-1	+1	14	-1	+1	-1
14	-1	+1	-1	11	-1	-1	+1	23	0	-1	+1
15	+1	-1	+1	15	+1	-1	+1	5	+1	0	0
16	0	+1	-1	12	+1	+1	-1	15	+1	-1	+1
17	-1	-1	0	10	+1	+1	+1	12	+1	+1	-1
18	0	-1	-1	8	-1	+1	+1	11	-1	-1	+1
19	+1	-1	0	14	-1	+1	-1	17	-1	-1	0
20	0	0	0	24	0	+1	+1	26	+1	0	-1
21	-1	0	+1	16	0	+1	-1	8	-1	+1	+1
22	-1	-1	-1	13	0	0	-1	9	+1	0	+1
23	0	-1	+1	2	-1	0	-1	27	0	+1	0
24	0	+1	+1	26	+1	0	-1	18	0	-1	-1
25	0	+1	0	3	+1	-1	-1	16	0	+1	-1
26	+1	0	-1	18	0	-1	-1	25	0	+1	0
27	0	+1	0	22	-1	-1	-1	7	-1	+1	0

Таблица 6

Результаты оптимизации планов эксперимента

Метод поиска	$C_{исх}$, усл.ед.	C_{min}, усл.ед.	Выигрыш по сравнению с исходным планом эксперимента
Метод прыгающих лягушек	174	87	2
Метод оптимизации роем частиц	174	85	2,05
Табу-поиск	174	97	1,79
Случайный поиск	174	147	1,2

В работе [7] были разработаны метод и программное обеспечение для оптимизации планов полного факторного эксперимента по стоимостным (временным) затратам с помощью алгоритма прыгающих лягушек. Программное обеспечение для оптимизации трехуровневых планов изменено в следующих модулях: генерация исходной матрицы планирования эксперимента, ввод стоимостей (времен) переходов между уровнями факторов и выполнение перестановок для получения трехуровневых планов методом прыгающих лягушек. Программное обеспечение реализовано на языке программирования C++. Все необходимые расчеты выполнялись на компьютере с процессором Intel Pentium G620 с частотой 2.60 GHz. Необходимый объем памяти – 32 МБ. Количество факторов и стоимости переходов уровней факторов вводятся с клавиатуры либо задаются в файле. Реализация метода прыгающих

лягушек требует небольшого объема памяти ЭВМ и имеет высокое быстродействие решения задачи. Разработанное программное обеспечение состоит из следующих модулей: ввод данных, построение исходной матрицы планирования эксперимента, построение матрицы сумм стоимостей (времен) изменения значений уровней факторов, оптимизация методом прыгающих лягушек, построение оптимальной матрицы планирования эксперимента, расчет выигрыша B.

Выводы. Разработаны метод и программное обеспечение, реализующие оптимизацию с применением алгоритма прыгающих лягушек многофакторных планов экспериментов с варьированием факторов на трех уровнях. Доказана его работоспособность и эффективность при исследовании метода измерения плотности тока гальванических ванн с мерными датчиками и шероховатости поверхности кремния при процессах глубокого плазмохимического травления элементов МЭМС.

Поиск оптимального или близкого к оптимальному плану эксперимента, полученного этим методом, реализуется за существенно меньшее время счета, чем при методе ветвей и границ и методе случайного поиска. Выигрыш в стоимости реализации планов экспериментов при использовании данного метода значительно больше, чем при методах случайного поиска и табу-поиска. Применение разработанного программного обеспечения, основанного на использовании алгоритма прыгающих лягушек, эффективно при количестве факторов $k \geq 3$. Показано, что для оптимизации трехуровневых планов целесообразно использование метода прыгающих лягушек.

ЛИТЕРАТУРА:

1. Кошевой Н.Д., Костенко Е.М. Оптимальное по стоимостным и временным затратам планирование эксперимента: монография. Полтава: изд. Шевченко Р.В., 2013. 317 с.

2. Koshevoy N. D., Kostenko E.M., Gordienko V.A., Syroklyn V.P. Optimum planning of an experiment in manufacturing the electronic equipment. Telecommunications and Radio Engineering. 2011. V.70, N 6. P. 731-734. https://doi.org/10.1615/TelecomRadEng.V70.i8.60.

3. Карпенко А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой: учебное пособие. М.: изд-во МГТУ им. Н.Э. Баумана, 2014. 446 с.

4. Кошевой Н.Д., Беляева А.А. Применение алгоритма оптимизации роем частиц для минимизации стоимости проведения многофакторного эксперимента. Радіоелектроніка, інформатика, управління. 2018. №1. С. 41 – 49. https://doi.org/10.15588/1607-3274-2018-1-5.

5. Кошевой Н.Д., Костенко Е.М., Беляева А.А. Сравнительный анализ методов оптимизации при исследовании весоизмерительной системы и терморегулятора. Радіоелектроніка, інформатика, управління. 2018. №4. С. 179-188. https://doi.org/10.15588/1607-3274-2018-4-17.

6. Кошевой Н. Д., Костенко Е.М., Чуйко А.С. Применение методов ветвей и границ и последовательного приближения для оптимизации моделирования процесса получения пористых материалов. Оптимізація виробничих процесів: зб. наук. пр. Севастопольського нац. техн. університету. 2011. Вип. 13. С. 69-74.

7. Кошевой Н.Д., Муратов В.В. Применение алгоритма прыгающих лягушек для оптимизации по стоимостным (временным) затратам планов полного факторного эксперимента. Радіоелектронні і комп'ютерні системи. 2018. №4. С. 53-61. https://doi.org/10.32620/reks.2018.4.05.

REFERENCES:

1. Koshevoy N. D., Kostenko E.M. Experimentally-optimal cost and time planning of the experiment: a monograph. Poltava: ed. Shevchenko R.V. 2013. 317 p.

2. Koshevoy N. D., Kostenko E.M., Gordienko V.A., Syroklyn V.P. Optimum planning of an experiment in manufacturing the electronic equipment. Telecommunications and Radio Engineering. 2011. V.70, N 6. P. 731-734.https://doi.org/10.1615/TelecomRadEng.V70.i8.60.

3. Karpenko A. P. Modern search engine optimization algorithms. Nature-inspired algorithms: a tutorial. M .: publishing house of MSTU. N.E. Bauman, 2014. 446 p.

4. Koshevoy N. D., Belyaeva A.A. Application of particle swarm optimization algorithm to minimize the cost of a multivariate experiment. Radio electronics, informatics, control. 2018. N. 1. S. 41 - 49. https://doi.org/10.15588/1607-3274-2018-1-5.

5. Koshevoy N.D., Kostenko E.M., Belyaeva A.A. Comparative analysis of optimization methods in the study of the weighing system and thermostat. Radio electronics, informatics, control. 2018. No4. S. 179-188.https: //doi.org/10.15588/1607-3274-2018-4-17.

6. Koshevoy N. D., Kostenko E. M., Chuyko A. S. The use of branch and bound methods and sequential approximation to optimize the modeling of the process of obtaining porous materials. Optimization of virological processes: zb. sciences. pr. Sevastopol national tech. to university. 2011. VIP. 13. – P. 69-74.

7. Koshevoi N.D., Muratov V.V. The use of the jumping frog algorithm for optimization of the cost (time) cost of plans for a full factorial experiment. Radio electronics and computer system. 2018. N4. Pp. 53-61.https: //doi.org/10.32620/reks.2018.4.05.

prof. Koshevoy N.D., prof. Kostenko E.M., Muratov V.V.

APPLICATION OF THE JUMPING FROGS METHOD FOR THE OPTIMIZATION OF THREE-LEVEL PLANS OF A MULTIPLE FACTOR EXPERIMENT

The planning of the experiment allows us to solve the problem of obtaining a mathematical model with minimal cost and time costs. The cost of implementing an experiment is significantly affected by the order of alternating levels of change in factors. Thus, it is required to find a procedure for the implementation of experiments that provides the minimum cost (time) for conducting a multivariate experiment. This task becomes especially relevant when studying long and expensive processes. The purpose of this article is the further development of the methodology of optimal planning of the experiment in terms of cost (time), which includes a set of methods for optimizing the plans of the experiment and hardware and software for their implementation. Object of study: optimization processes for the cost of three-level plans for multivariate experiments. Subject of research: optimization method for cost and time costs of experimental designs based on the use of the jumping frog method. Experimental research methods are widely used to optimize production processes. One of the main goals of the experiment is to obtain the maximum amount of information about the influence of the studied factors on the production process. Next, a mathematical model of the object under study is built. Moreover, it is necessary to obtain these models at the minimum cost and time costs. The design of the experiment allows you to get mathematical models with minimal cost and time costs. For this, a method and software were developed for optimizing three-level plans using the jumping frog method. Three-level plans are used in the construction of mathematical models of the studied objects and systems. An analysis is made of the known methods for the synthesis of three-level plans that are optimal in cost and time costs. The operability of the algorithm was tested when studying the roughness of the silicon surface during deep plasma-chemical etching of MEMS elements. Its effectiveness is shown in comparison with the following methods: swarm of particles, taboo search, branches and borders. Using the developed method and software for optimizing three-level plans using the jumping frog method, one can achieve high winnings compared to the initial experimental plan, optimal or close to optimal results compared to particle swarm, taboo search, branches and borders methods, and also high speed of solving the optimization problem in comparison with previously developed optimization methods for three-level experimental designs.

Keywords: optimal plan, method of jumping frogs, optimization, experiment planning, cost, time, payoff.

УДК 004.522

д.т.н., проф. **Ленков С.В.** (ВИКНУ)
д.т.н., проф. **Мясищев А.А.** (ХмНУ)
д.т.н., доц. **Комарова Л.А.** (ОНАЗ)
д.т.н., с.н.с. **Селюков А.В.** (ТОО «Укрспецколсалтинг»)

DOI: https://doi.org/10.17721/2519-481X/2020/66-05

ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ PID РЕГУЛЯТОРА ДЛЯ ПРОШИВОК БПЛА

В статье рассматривается практическая возможность настройки параметров PID регулятора для семейства прошивок cleanflight беспилотных летательных аппаратов (БПЛА) роторного типа и с неподвижным крылом во время полета. Показано, что для этого необходимо использование аппаратуры радиоуправления с минимальным количеством каналов равным восьми. Разработан беспилотный летательный аппарат (БПЛА) на базе полетного контроллера OMNIBUSF4V3 с встроенным гироскопом и акселерометром, барометром/высотомером BMP280. Разработана схема подключения 3-х осевого компаса HMC5883L по шине I2C и GPS приемника u-blox NEO-6M к порту контроллера UART6. В качестве прошивки использована INAV ver.2.2.1, поддерживающая навигационные функции. Спроектированный квадрокоптер (БПЛА) способен выполнять следующие полетные режимы: ANGLE - автоматическое выравнивание крена и тангажа с контролем угла горизонта, заданное значение которого не может превышаться, чем достигается устойчивый полет. Здесь задействованы гироскоп и акселерометр для удержания горизонта. NAV ALTHOLD - удержание высоты. Здесь использован барометр, который способствует удержанию высоты по давлению воздуха. NAV POSHOLD - выполняется удержание позиции. Использует GPS. NAV RTH (Return To Home) - возврат домой, в точку взлета. NAV WP - полет по заданной траектории, которая аппроксимирована путевыми точками. В этом случае в конфигураторе накладываются на выбранную карту местности путевые точки с такими параметрами, как высота, скорость ее пролета.

Для малых оборотов моторов показана возможность использования режима AIR MODE для увеличения эффективности работы PID регулятора. Показана возможность использования программы STM32 Flash loader demonstrator в качестве программатора для прошивки полетного контроллера OMNIBUSF4V3 любой прошивкой семейства Cleanflight. Установлено, что для настройки параметров P, I и D возможно использование трехпозиционного переключателя на одном из каналов управления и переменного резистора на другом канале. Если отградуировать резистор на три положения можно выполнить регулировку трех параметров, а на пять положений - 5 параметров. Рассмотрен вопрос настройки устойчивости полета коптера. При резком увеличении дроссельной заслонки возможен завал коптера в одну из сторон и его падение. Установлено, что для предотвращения этого необходимо использование одинаково подобранных ESC регуляторов, моторов и правильная настойка PID параметров в частности по YAW.

Ключевые слова: OMNIBUSF4V3, PID-регулятор, INAV, GPS приемник, AIR MODE, STM32F4, HMC5883L, NEO6MV2, MPU6000.

Введение и постановка задачи. Беспилотные летательные аппараты (БПЛА) роторного типа (квадрокоптеры, гексакоптеры и др.), с неподвижным крылом (самолеты, летающие крылья) для обеспечения удержания горизонтального полета используют классические PID регуляторы [1-4]. Для управления полетом перечисленных выше БПЛА наиболее часто используют полетные контроллеры на базе микроконтроллеров STM32F4, STM32F7 с прошивками betaflight, cleanflight, INAV [1,5,6]. Первые две прошивки используются в основном на небольших квадрокоптерах, очень динамичных и развивающих высокие скорости. Они не используют навигационное оборудование, такие как компас, барометр, GPS приемник для удержания позиции, возврата в точку старта и полета по точкам - заданной траектории. Прошивка INAV [1,6] используется и для больших коптеров, летающих крыльев, на которых установлено навигационное оборудование. В основном эта прошивка применяется для дальних полетов с использованием курсовой камеры (полет по FPV). Такие полеты опасны тем, что при потере связи с видеопередатчиком теряется информация о положении БПЛА и он

улетает в неопределенное местоположение. Для этого в прошивке INAV существует возможность использование навигационной аппаратуры, которая позволяет по GPS приемнику, магнитометру, барометру в случае потери радиосвязи вернуться в положение старта или на расстояние, доступное для радиосвязи. Однако для устойчивого полета БПЛА, особенно в ветреную погоду, на высоких скоростях с резкими изменениями траектории (динамичные маневры), должен быть идеально настроен PID [7-9] регулятор - подобраны его три параметра - P, I, D. В настоящее время не существует аналитического решения этой задачи для разной геометрии, веса БПЛА. Эта задача решается опытным путем в полёте для разных типов, размеров, веса, установленного оборудования БПЛА. В работе рассматривается, как это реализовано с помощью аппаратуры радио управления для перечисленных типов прошивок так как они имеют аналогичный PID регулятор. Перед настройкой регулятора рассматривается особенность построения четырёхмоторного БПЛА (квадрокоптера) на базе полетного контроллера OMNIBUSF4V3 [10] с прошивкой INAV Ver.2.2.1 [5], которая является последней на момент написания работы.

Анализ последних исследований и публикации. В настоящее время в периодической литературе мало представлено работ по построению, программированию и практическому исследованию поведения БПЛА для разных его геометрических параметров, используемых полетных контроллеров, прошивок, навигационных датчиков [1-3,9]. Так разное программное обеспечение полетных контроллеров (прошивки) [1-12] очень сильно влияет на устойчивость, стабильность, продолжительность полета. Навигационные датчики совместно с программным обеспечением позволяют придерживаться более или менее точного полета по заданным траекториям. Используемые математические модели фильтрации данных с датчиков (фильтр Кальмана, комплементарный фильтр и др.) оказывают сильное влияние на БПЛА во время полета и устойчивого маневрирования. Большое значение имеет подбор параметров для выбранной модели стабилизации и параметров для усиления классических параметров математических моделей, например, TPA, AIRMODE, Anti-Gravity [1,6] и др. Подбор программного обеспечения, полетных контроллеров, датчиков, геометрии БПЛА для максимально устойчивого полета БПЛА возможно лишь при проведении летных испытаний. Представленная работа посвящена практическому анализу представленным здесь техническим средствам и программному обеспечению.

Изложение основного материала работы. INAV является ответвлением известного проекта Cleanflight [1, 13] с акцентом на функции GPS для самолетов и мультироторных моделей. INAV активно развивается и в настоящее время - поддерживает режимы RTH (Return To Home) с предопределенной высотой набора высоты, удержание позиции, полета по путевым точкам, режим «Следуй за мной" (Follow-Me) и другие.

Особенностью прошивки INAV является возможность динамически регулировать усиление PID, поэтому высокий дроссель (ускоренный полет вперед или быстрый набор высоты) не вызывает высокочастотных колебаний квадрокоптера, характерных для высоких значений составляющей P в PID регуляторе. Для этого вводится параметр TPA [Throttle PID Attenuation]. TPA обеспечивает уменьшение значения PID по отношению к полному дросселю [1]. Он используется для гашения значений PID при достижении полного газа. Численно TPA равен проценту гашения, которое будет иметь место при полном открытии дроссельной заслонки. TPA Breakpoint – точка на кривой газа, с которой начнет применяться TPA. Ниже этой точки TPA не используется. Например, если возникают колебания, начинающиеся с 3/4 дросселя, необходимо установить TPA Breakpoint равное 1750 или ниже (предполагается, что диапазон изменения дросселя составляет 1000-2000), а затем медленно необходимо увеличить TPA, пока колебания квадрокоптера не исчезнут. На рис. 1 показан пример мультироторной кривой TPA.

Для динамической регуляции усиления PID очень важно установить режим AIRMODE. В стандартном режиме уменьшения дроссельной заслонки, когда рассчитываются крен, шаг и рыскание, все двигатели будут уменьшать обороты одинаково. При развороте некоторые двигатели могут даже отключаться. Это приводит к уменьшению усиления PID регулятора.

Поэтому при резком снижении квадрокоптера, резких поворотов из-за уменьшения воздействия PID регулятора на стабилизацию полета квадрокоптер падает. Airmode обеспечит полную коррекцию PID во время нулевого дросселя и дает возможность плавного полета и выполнения высшего пилотажа. Для построения опытного квадрокоптера использовались следующие компоненты:

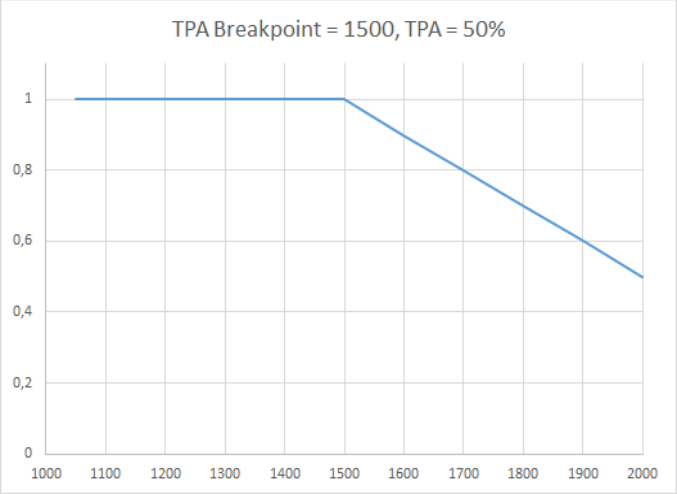


Рисунок 1 – Пример мультироторной кривой TPA

1. Рама размером 380мм
2. Моторы A2212/1000 с ESC регуляторами на 30A [14]
3. Пропеллеры 10x45 дюймов
4. Полетный контроллер OMNIBUSF4V3[9] на базе микроконтроллера STM32F405 [7] LQFP64 (168Mhz, 1M Flash, 192kB SRAM) с встроенным гироскопом, акселерометром MPU6000 [11] и барометром BMP280
5. Компас HMC5883L [2] подключенный к шине I2C
6. GPS приемник NEO6M [2]

Для питания моторов и электроники установлена батарея lipo 3S1P 1800mAh. Она обеспечивала полет в течении 11-13минут. Квадрокоптер должен уметь удерживать высоту (барометр), позицию (GPS приемник) и возвращаться домой и летать по заданной траектории (до 60 полетных точек).

На рис. 2 представлен полетный контроллер OMNIBUSF4V3 [11] с обозначением его основных выводов для подключения к датчикам, моторам, приемнику и видеопередатчику.

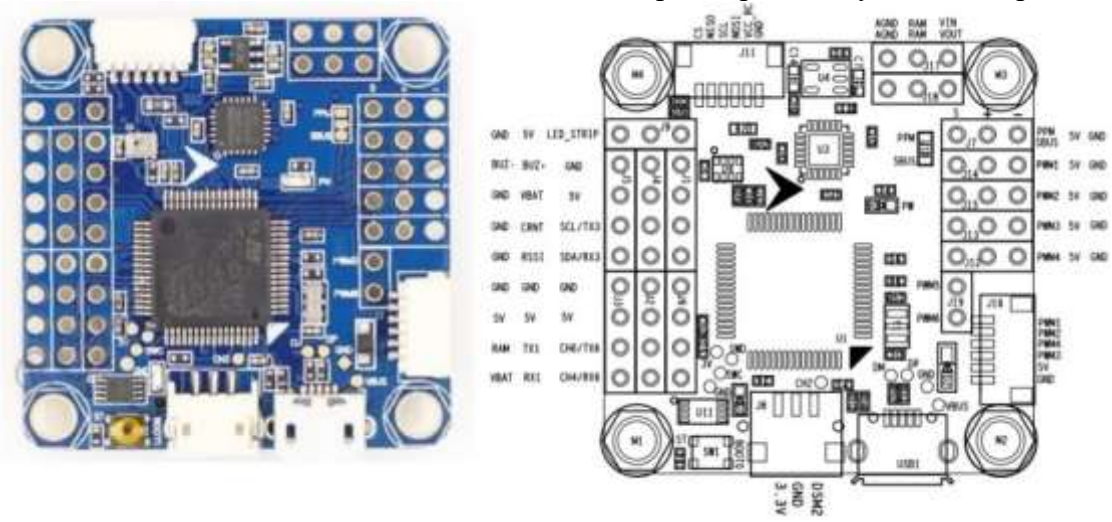


Рисунок 2 – Полетный контроллер OMNIBUSF4V3

Для решения задачи требуется прошивка контроллера, которая копируется с сайта https://github.com/iNavFlight/inav/releases/download/2.2.1/inav_2.2.1_OMNIBUSF4V3.hex, и конфигуратор inav ver. 2.2.1 -: https://github.com/iNavFlight/inav-configurator/releases/download/2.2.1/INAV-Configurator_win32_2.2.1.zip. Для прошивки OMNIBUSF4V3 использовалась программа STM32 Flash loader demonstrator [4] с сайта https://www.st.com/en/development-tools/flasher-stm32.html и конвертер USB to TTL на базе микросхемы CH340. Процедура прошивки описана в работе [1] для полетного контроллера cc3d, которая аналогична прошивке OMNIBUSF4V3. Подключение конвертера выполняется к выводам TX1, RX1 контролера OMNIBUSF4V3.

Подключение к OMNIBUSF4V3 компаса, GPS приемника, приемника управления по PPW, моторов показано на рис. 3. Компас должен находиться над плоскостью вращения пропеллеров на высоте не менее 15см для уменьшения помех при работе моторов. Подключение приемника радиоуправления возможно и по шине SBUS, однако это приведет к использованию дополнительного порта UART у микроконтроллера. Важно то, что необходима установка перемычки при выборе PPW или SBUS. Эта перемычка расположена в правой верхней части контроллера.

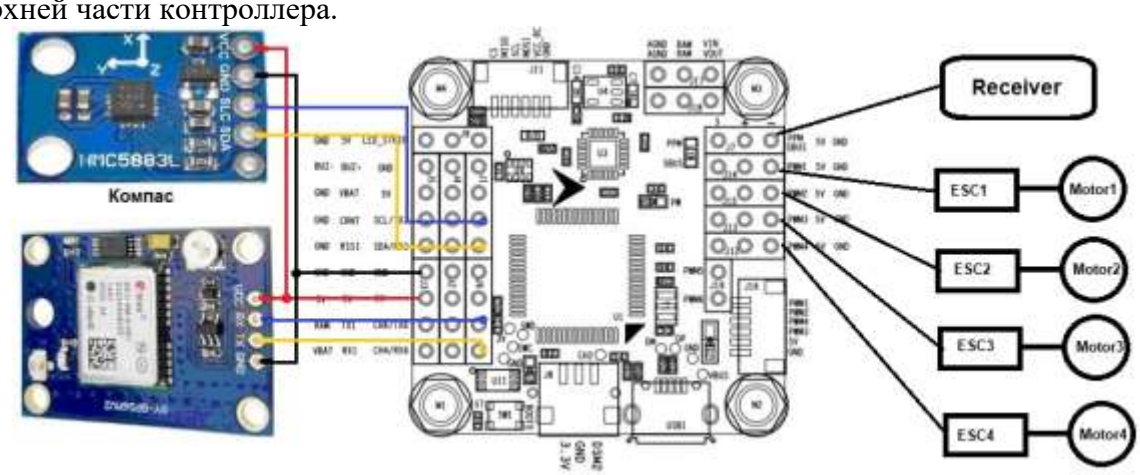


Рисунок 3 – Схема подключения к полетному контроллеру

После подключения согласно рис. 3 необходимо запустить конфигуратор INAV и последовательно заходить во вкладки и выполнять настройки параметров. Во вкладке Ports на строке UART6 в позиции Sensors устанавливается GPS со скоростью 38400. В вкладке Mixer выбирается Quad X и нажимается кнопка Load and apply. После выхода с каждой вкладки выполняется сохранение (кнопка save). Во вкладке Configuration в качестве Sensors должны быть установлены MPU6000 (Accelerometr), HMC5883 (Magnetometer), BMP280 (Barometer). В разделе Board and Sensor Alignment - устанавливается MAG alignment - CW 90. Это соответствует расположению компаса, повернутого на 90 градусов. Receiver Mode - PPM RX input - режим работы приемника. В разделе GPS включается GPS и устанавливается протокол UBLOX. В разделе ESC/Motor Features включается Enable motor and servo output. Устанавливается протокол, например, ONESHOT125 [15]. Во вкладке PID tuning предварительно устанавливаются параметра PID регулятора, как на рис. 4. Их настройка рассмотрена ниже.

Name	Proportional	Integral	Derivative	FeedForward
Basic/Acro				
Roll	47	13	39	0
Pitch	47	13	39	0
Yaw	120	60	0	0

Рисунок 4 – Параметры PID регулятора

Во вкладке Motors после включения выключателя "I understand the risks, propellers are removed - Enable motor control" необходимо проконтролировать, в какую сторону вращаются моторы в соответствии с рисунком. Если мотор вращается не в ту стороны, меняется подключение двух из трех проводов мотора к ESC регулятору. Во вкладке Receiver контролируется работа каналов приемника. Перемещение стиков и включение и выключение активных тумблеров на пульте управления должно отображаться во вкладке адекватно. Во вкладке Modes устанавливаются полетные режимы квадрокоптера в соответствии с работой [1]. В рассматриваемой версии INAV возможна настройка полетной миссии - Mission Control (полет по заданной траектории с указанием путевых точек, рис. 5). Здесь производится выбор участка карты. Должен быть доступ к Интернет. Указываются нажатием клавишей мышки путевые точки. Каждая путевая точка после второго нажатия на нее мышкой высвечивает свои координаты с параметрами высоты пролета над ней и скоростью. Эти значения необходимо отредактировать. Если необходимо вернуться в точку старта с автоматической посадкой - ставят галочку на RTH at the end of the mission и на Landing. Сформированный маршрут записывается командами Save mission to FC и Save Eeprom mission. Полет по точкам может быть выполнен, если во вкладке Modes будет установлен переключатель на пульте радиоуправления в полетный режим NAV WP.

Рисунок 5 – Формирование полетной миссии по путевым точкам

Во вкладке Calibration необходимо выполнить калибровку Accelerometra и Compass. Схема калибровка Accelerometra показана на рисунке вкладки. Для этого предварительно нажимается кнопка Calibrate Accelerometr. При калибровке компаса квадрокоптер необходимо вращать по 6-ти осям. На эту процедуру выделяется 30 секунд. Калибровка в поле выполняется перемещением стиков на пульте управления по правилу: Левый стик вверх и вправо, правый стик вниз в течении 2-3секунд. После это коптер вращается по 6-и осям.

При полете коптера в автоматическом режиме настраиваются параметры во вкладке Advanced tuning. Обычно настройка ведется в двух основных разделах. Это Multirotor Navigation Settings и RTH and Landing Settings.

Раздел Multirotor Navigation Settings.

User Control Mode:

Altitude - В этом режиме коптер в меньшей степени отслеживает свое положение по спутникам. Например, включается полетный режим NAV POSHOLD - удержание позиции. Если стиком пульта дать перемещение вперед, координаты со спутника не будут восприниматься коптером. Но в случае возврата стика в нейтральное положение, коптер определит координаты со спутника и вернется в положение, когда стик занял нейтральную позицию. При большой скорости возможно перелетание позиции и коптер будет возвращаться обратно в точку нейтрального положения стика. Коптер в этом режиме более динамичен, чем в режиме Cruise и используется для малых коптеров.

Cruise - Здесь при перемещении стиков с нейтральной позиции коптер при полете постоянно контролирует свои координаты и в случае возвращения стиков в нейтральную

позицию коптер сразу останавливается. При этом режиме коптер мало динамичен, подходит для больших коптеров.

Max. navigatoin speed - это максимальная скорость в режиме навигации в см/с (установлен режим NAV POSHOLD).

Max. CRUISE speed - максимальная скорость в режиме круиза в см/с.

Max. navigator climp rate - максимальная скорость подъема в режиме навигации в см/с.

Max. ALTHOLD climp rate - максимальная скорость подъема в режиме удержания высоты в см/с.

Multirotor max. banking angle [degrees] - максимальный угол наклона коптера в градусах в режиме навигации.

Use mid. throttle for ALTHOLD - Если включен, режим удержания высоты установлен, когда стик газа находится в среднем положении.

Hover throttle - В этом окне указывается число, пропорциональное частоте вращения моторов при среднем стике газа. Если в среднем стике газа на пульте установить режим удержания высота и коптер будет резко набирать высоту или снижаться, необходимо точнее установить это число.

Раздел RTH and Landing Settings.

RTH altitude mode:

Current - возврат домой (в точку старта) выполняется на той же высоте на которой была потеряна связь с пультом управления или дана команда возврата.

Extra - при возврате коптер с текущей высоты подниметься на высоту, указанную в параметре RTH altitude.

Fixed - при возврате, если коптер имеет высоту срабатывания возврата домой ниже RTH altitude, то он поднимается на высоту возврата и далее на ней летит домой. Если коптер был выше высоты возврата, то по всей обратной траектории он медленно опускается до высоты возврата домой.

Max - коптер возвращается в точку старта на максимальной высоте, которую он зафиксировал во время полета. В этом случае, если коптер перелетал гору, а потом снижался, он при обратном возврате не столкнется с горой.

At least - возвращается в точку старта на высоте не меньше той, что указана в параметре RTH altitude. Если высота коптера была меньше RTH altitude при срабатывании RTH, то он поднимается на высоту возврата. Если больше, то возвращается на этой же высоте.

RTH altitude - высота возврата домой в см.

Climb befor RTH - сначала подняться до высоты RTH altitude, потом вернуться в точку старта.

Climb regardless of positions sensors health - подняться независимо от датчика, который потерял связь со спутниками. Если связь не восстановиться на высоте, коптер приземлиться в этом месте.

Tail first - возврат домой задом без разворота.

Land afte RTH - Always - всегда выполнять посадка в точке старта, Never - не выполнять посадку в точку старта, Only failsafe - выполнять посадку в случае потери связи с передатчиком.

Landing vertical speed - вертикальная скорость посадки.

Min. vertical landing speed at altitude - высота, на которой вертикальная скорость посадки замедляется.

Vertical landing speed slowdown at altitude - высота, начиная с которой коптер начинает притормаживать вертикальную скорость посадки.

Min. RTH distance - минимальное расстояние, начиная с которого коптер будет выполнять процедуру возврата домой. Если расстояние меньше и связь с аппаратурой управления нарушиться, коптер выполнит посадку в месте обрыва связи.

Рассмотрим возможности полетного контроллера и прошивки INAV по настройке PID регулятора. Известно, что PID регулятор (Пропорционально интегрально дифференцирующий

регулятор) это управляющий цикл с обратной связью, который очень часто используется во всевозможных управляющих системах. PID регулятор вычисляет значение «ошибки» как разницу между измеренным значением переменной и ее желаемым значением. Он пытается минимизировать ошибку воздействуя на управляемые входы.

PID регулятор берет данные, измеренные сенсорами полетного контроллера (гироскопы, акселерометры) и сравнивает их с ожидаемым значениями, чтобы изменить скорость моторов для компенсации любых отклонений и удержания баланса. Алгоритм вычислений в PID регуляторе включает в себя 3 постоянных параметра, пропорциональное, интегральное и дифференцирующее значения, обозначаемые P, I и D. Эвристически эти значения могут быть интерпретированы как значения во времени: P зависит от текущей ошибки, I – от накопившихся прошлых ошибок, D – это предсказание будущих ошибок, на основании скорости изменения. В зависимости от полетного контроллера PID регуляторы будут связаны с различными полетными режимами.

P – это основное значение, которое определяет стабильность. Например, если I и D будут равными 0, самолет будет удерживать горизонтальное положение. Поэтому значение P настраивается до значений I и D.

Чем больше значение P, тем резче оно пытается стабилизировать коптер. Но если P слишком большое, то коптер становится слишком чувствительным и слишком резко пытается корректировать свое положение, проскакивая требуемое положение (чрезмерно резкая и быстрая реакция), в этом случае возникнут колебания с большой частотой. Параметр P увеличивают до тех порка не появятся высокочастотные колебания, звуки которых легко можно различить. Далее P уменьшают примерно на 30%.

D – это противоположность P. При резком отклонении стиков по крену и тангажу при малых D коптер начинает раскачиваться, что приводит к его переворачиванию. В этом случае повышают D так, чтобы при резком отклонении стиков и возврате их в нейтральное положение коптер возвращался в горизонтальное состояние без колебаний. Значение I увеличивают до тех пор, пока не появятся низкочастотные колебания коптера. После этого I уменьшают до полного прекращения колебаний. Значение I уменьшает раскачку коптера во время быстрого снижения.

Рассмотрим настройки INAV для изменения параметров P, I и D во время полета. Для этого используется вкладка Adjustments. На пульте управления необходимо выбрать два канала - это трехпозиционный переключатель и "крутилка" - канал, связанный с переменным резистором, который может плавно изменять значения импульсов от 1000 до 2000. Изменение значений параметров выполняется с помощью трехпозиционного переключателя. Среднее положение соответствует состоянию, когда параметр не изменяется. Верхнее положение - уменьшению параметра. Нижнее - увеличению. К полетному контроллеру обязательно должен быть подключен зуммер. При уменьшении параметра на одну единицу он дает однократный сигнал с периодом примерно 0.5сек. При увеличении - двойной сигнал. Например, пять сигналов, - параметр от исходного значения уменьшился на 5 единиц и т.д. Для выбора параметра используется канал с резистором. Если поворот резистора разметить на 3 одинаковых части, то можно менять три параметра, установив резисторы в определенное положение. Рис. 6 вкладки иллюстрирует сказанное выше.

Рисунок 6 – Иллюстрация работы с вкладкой Adjustments

Канал CH6 использует переменный резистор. На канале CH5 установлен трехпозиционный переключатель. Если ручка резистора (CH6) находится в левом положении, то трехпозиционный переключатель изменяет параметр P по Pitch и Roll одновременно. При среднем положении ручки резистора одновременно меняются значения параметра I также по Pitch и Roll одновременно. Одновременное изменение возможно, так как коптер симметричный с центром тяжести в центре. Так будут изменяться параметры, представленные в таблице на рис. 4. Чтобы увидеть эти изменения необходимо нажать на кнопку refresh в вкладке PID tuning это в случае, если компьютер подключен к полетному контроллеру. При нажатии на кнопку save новые параметры будут сохранены. Во время полета для сохранения измененных параметров PID необходимо на пульте управления опустить вниз и развести в разные стороны стики пульта управления. Сигнал зуммера укажет, что значения PID регулятора записаны в EEPROM память контроллера. Для такой регулировки параметров необходимо иметь 8-ми канальную систему управления. Аналогично можно менять многие параметры полетного контроллера, которые можно выбрать в колонке then apply вкладки Adjustments. Чем больше каналов имеет система управления, тем большее количество параметров регулируется в тестовых полетах по настройки любого БПЛА.

При установке навигационного оборудования на коптер, арминг коптера можно выполнит только в случае подключения к такому количеству спутников, которые указаны во вкладке Advanced tuning в параметре Min. GPS satellites for a valid fix, например, 6 спутников. Для разрешения арминга без спутников используется команда set nav_extra_arming_safety = OFF, которую вводят в вкладке CLI с последующим вводом команды save. На рис. 7 представлено фото экспериментального БПЛА со снятыми пропеллерами. Компас вынесен за пределы корпуса GPS приемника для уменьшения сбоев его работы и зависания.

Рисунок 7 – фото экспериментального БПЛА со снятыми пропеллерами

Выводы. В статье показаны особенности определения параметров PID регулятора для прошива беспилотного летательного аппарата, а именно:

1. Показана возможность использования прошивок семейства Cleanflight на примере INAV для изменения параметров PID регулятора во время полета с помощью пульта управления.

2. Для малых оборотов моторов показана возможность использования режима AIR MODE для увеличения эффективности работы PID регулятора.

3. Исследована возможность использования прошивки INAV с полетным контроллером OMNIBUSF4V3 начиная с версии 1.9.2 для полета по заданной траектории, которую можно сформировать максимум из 60 путевых точек.

4. Рассмотрено подключение к полетному контроллеру магнитометра, GPS приемника, моторов, радиоприемника системы управления для построения бюджетного (до $100) полностью автоматического квадрокоптера для выполнения фото съемок местности по радиусу до 10км с литий ионными элементами емкостью 6000мАч.

5. Показана возможность использования программы STM32 Flash loader demonstrator в качестве программатора для прошивки полетного контроллера OMNIBUSF4V3 любой прошивкой семейства Cleanflight.

ЛИТЕРАТУРА:

1. Мясищев А.А. Возможности полетного контроллера cc3d с прошивкой inav. / Вісник ХНУ. Технічні науки. -Хмельницький: ХНУ, 2019. - №1. - С. 129-136.

2. Мясищев А.А. Использование платы ROBOTDYN MEGA2560 PRO для построения полетного контроллера гексакоптера / А.А. Мясищев // Вісник хмельницького національного університету. Технічні науки. – Хмельницький: ХНУ, 2018. – № 3. – С. 171–179.

3. В. Чигінь, П. Михайлишин. Експериментальний безпілотний авіаційний комплекс для фотозахоплення / Вісник ХНУ. Технічни науки. -Хмельницький: ХНУ, 2019. - №2. -С. 202-206.

4. FLASHER-STM32 [Electronic resource]. – 2016. – Mode of access: https://www.st.com/en/development-tools/flasher-stm32.html.

5. INAV Configurator 2.2.1. [Electronic resource]. – 2019. – Mode of access: https://github.com/iNavFlight/inav-configurator/releases/tag/2.2.1.

6. INAV [Electronic resource]. – 2018. – Mode of access: https://github.com/iNavFlight/inav/wiki.

7. F1, F3, F4 AND F7 FLIGHT CONTROLLER DIFFERENCES EXPLAINED. [Electronic resource]. – 2017. - Mode of access: https://oscarliang.com/f1-f3-f4-flight-controller

8. Карпов В.Э. ПИД-управление в нестрогом изложении. [Electronic resource]. – Москва, 2012. – Mode of access: http://robofob.ru/materials/articles/pages/Karpov_mobline1.pdf

9. QUADCOPTER PID EXPLAINED. [Electronic resource]. – 2019. – Mode of access: https://oscarliang.com/quadcopter-pid-explained-tuning/

10. OMNIBUS F4V3. [Electronic resource]. – 2017. – Mode of access: http://nic.vajn.icu/PDF/radio-controlled/OMNIBUS_F4_V3.pdf

11. Command Line Interface (CLI) [Electronic resource]. – 2019. – Mode of access: https://github.com/iNavFlight/inav/blob/master/docs/Cli.md.

12. Open-Source flight controller software for modern flight boards. [Electronic resource]. -2018. - Mode of access: http://cleanflight.com/.

13. Gyroscopes and Accelerometers on a Chip. [Electronic resource]. – 2013. – Mode of access: http://www.geekmomprojects.com/gyroscopes-and-accelerometers-on-a-chip/

14. Мясищев А.А. Программирование esc регуляторов SIMONK-30A И EMAX SIMON-12A через ARDUINO и полетный контроллер / Вісник ХНУ. Технічні науки. - Хмельницький: ХНУ, 2019. - №2.- С. 228-237.

15. Мясищев А.А. Построение БПЛА на базе полетного контроллера APM 2.6. / Вісник ХНУ. Технічни науки. -Хмельницький: ХНУ, 2016. - №5. - С. 225-230.

REFERENCES:

1. Myasishev A.A. Vozmozhnosti poletnogo kontrollera cc3d s proshivkoj inav. / Visnik HNU. Tehnichni nauki.-Hmelnickij: HNU, 2019. - №1. Pp. 129-136.

2. Myasishev A.A. Ispolzovanie platy ROBOTDYN MEGA2560 PRO dlya postroeniya poletnogo kontrollera geksakoptera / A.A. Myasishev // Visnik hmelnickogo nacionalnogo universitetu. Tehnichni nauki. – Hmelnickij : HNU, 2018. – № 3. – Pp. 171–179.

3. V. ChIGIN, P. Mihajlishin. eksperimentalnij bezpilotnij aviacijnij kompleks dlya fotozahoplennya. / Visnik HNU. Tehnichni nauki.-Hmelnickij: HNU, 2019. - №2. Pp. 202-206.

4. FLASHER-STM32 [Electronic resource]. – 2016. – Mode of access: https://www.st.com/en/development-tools/flasher-stm32.html.

5. INAV Configurator 2.2.1. [Electronic resource]. – 2019. – Mode of access: https://github.com/iNavFlight/inav-configurator/releases/tag/2.2.1

6. INAV [Electronic resource]. – 2018. – Mode of access: https://github.com/iNavFlight/inav/wiki.

7. QUADCOPTER PID EXPLAINED. [Electronic resource]. – 2019. – Mode of access: https://oscarliang.com/quadcopter-pid-explained-tuning/

8. F1, F3, F4 AND F7 FLIGHT CONTROLLER DIFFERENCES EXPLAINED. [Electronic resource]. – 2017. - Mode of access: https://oscarliang.com/f1-f3-f4-flight-controller

9. Myasishev A.A. Programmirovanie esc regulyatorov simonk-30a i emax simon-12a cherez arduino i poletnyj kontroller/ Visnik HNU. Tehnichni nauki.-Hmelnickij: HNU, 2019. - №2.-s. 228-237.

10. Open-Source flight controller software for modern flight boards. [Electronic resource]. 2018. - Mode of access: http://cleanflight.com/.

11. Command Line Interface (CLI) [Electronic resource]. – 2019. – Mode of access: https://github.com/iNavFlight/inav/blob/master/docs/Cli.md.

12. Karpov V.E. PID-upravlenie v nestrogom izlozhenii. [Electronic resource]. – Moskva, 2012. – Mode of access: http://robofob.ru/materials/articles/pages/Karpov_mobline1.pdf

13. OMNIBUS F4V3. [Electronic resource]. – 2017. – Mode of access: http://nic.vajn.icu/PDF/radio-controlled/OMNIBUS_F4_V3.pdf

14. Myasishev A.A. Programmirovanie esc regulyatorov simonk-30a i emax simon-12a cherez arduino i poletnyj kontroller/ Visnik HNU. Tehnichni nauki.-Hmelnickij: HNU, 2019. - №2. Pp. 228-237.

15. Myasishev A.A. Postroenie BPLA na baze poletnogo kontrollera APM 2.6. / VISNIK HNU. Tehnichni nauki.-Hmelnickij: HNU, 2016. - №5. Pp. 225-230.

д.т.н., проф. Лєнков С.В., д.т.н., проф. Мясіщев О.А.,
д.т.н., доц. Комарова Л.О., д.т.н., с.н.с. Сєлюков О.В.

ОСОБЛИВОСТІ ВИЗНАЧЕННЯ ПАРАМЕТРІВ PID РЕГУЛЯТОРА ДЛЯ ПРОШИВОК БПЛА

В роботі розглядається практична можливість налаштування параметрів PID регулятора для сімейства прошивок cleanflight безпілотних літальних апаратів (БПЛА) роторного типу і з нерухомим крилом під час польоту. Показано, що для цього необхідно використання апаратури радіоуправління з мінімальною кількістю каналів рівним восьми. Розроблено безпілотний літальний апарат (БПЛА) на базі польотного контролера OMNIBUSF4V3 з вбудованим гіроскопом і акселерометром, барометром / висотоміром BMP280. Розроблено схему підключення 3-х осьового компаса HMC5883L по шині I2C і GPS приймача u-blox NEO-6M до порту контролера UART6. Як прошивки використана INAV ver.2.2.1, що підтримує навігаційні функції. Спроектований квадрокоптер (БПЛА) здатний виконувати наступні польотні режими: ANGLE - автоматичне вирівнювання крену і тангажу з контролем кута горизонту, задане значення якого не може перевищуватися, чим досягається стійкий політ. Тут задіяні гіроскоп і акселерометр для утримання горизонту. NAV ALTHOLD - утримання висоти. Тут використано барометр, який сприяє утриманню висоти по тиску повітря. NAV POSHOLD - виконується утримання позиції. Використовує GPS. NAV RTH (Return To Home) - повернення додому, в точку зльоту. NAV WP - політ по заданій траєкторії, яка аппроксимирована точками. В цьому випадку в конфігураторі накладаються на обрану карту місцевості шляхові точки з такими параметрами, як висота, швидкість її прольоту.

Для малих оборотів моторів показана можливість використання режиму AIR MODE для збільшення ефективності роботи PID регулятора. Показана можливість використання програми STM32 Flash loader demonstrator як програматора для прошивки польотного контролера OMNIBUSF4V3 будь прошивкою сімейства Cleanflight. Встановлено, що для налаштування параметрів P, I, D можливе використання трипозиційного перемикача на одному з каналів управління і змінного резистора на іншому каналі. Якщо отградуировать резистор на три положення можна внести корективи трьох параметрів, а на п'ять положень - 5 параметрів.

Розглянуто питання настройки стійкості польоту коптера. При різкому збільшенні дросельної заслінки можливий завал коптера в одну зі сторін і його падіння. Встановлено, що для запобігання цьому необхідно використання однаково підібраних ESC регуляторів, моторів і правильна настоянка PID параметрів зокрема по YAW.

Ключові слова: OMNIBUSF4V3, PID-регулятор, INAV, GPS приймач, AIR MODE, STM32F4, HMC5883L, NEO6MV2, MPU6000

Prof. Lienkov S.V., Prof. Myasischev A.A.,
Prof Komarova L.O., Prof Selyukov A.V.

FEATURES OF DETERMINING THE PID REGULATOR PARAMETERS FOR UAV FIRMWARE

The paper considers the practical possibility of tuning the PID controller parameters for the cleanflight firmware family of unmanned aerial vehicles (UAVs) of a rotor type and with a fixed wing during flight. It is shown that this requires the use of radio control equipment with a minimum number of channels equal to eight. An unmanned aerial vehicle (UAV) has been developed based on the OMNIBUSF4V3 flight controller with a built-in gyroscope and accelerometer, BMP280 barometer / altimeter. The scheme of connecting the 3-axis compass HMC5883L via the I2C bus and the GPS receiver u-blox NEO-6M to the controller port UART6 is developed. The firmware used is INAV ver.2.2.1, which supports navigation functions. The designed quadrocopter (UAV) is capable of performing the following flight modes: ANGLE - automatic roll and pitch alignment with horizon angle control, the set value of which cannot be exceeded, thereby achieving stable flight. A gyroscope and an accelerometer are used here to hold the horizon. NAV ALTHOLD - hold height. A barometer is used here, which helps to maintain altitude by air pressure. NAV POSHOLD - a position is being held. Uses GPS. NAV RTH (Return To Home) - return home to the take-off point. NAV WP - flight along a given path, which is approximated by waypoints. In this case, waypoints with such parameters as altitude and its flight speed are superimposed on the selected terrain map in the configurator.

For low engine speeds, the possibility of using the AIR MODE mode to increase the efficiency of the PID controller is shown. The possibility of using the program STM32 Flash loader demonstrator as a programmer for flashing the flight controller OMNIBUSF4V3 with any Cleanflight family firmware is shown. It was found that for setting the parameters P, I, D it is possible to use a three-position switch on one of the control channels and a variable resistor on the other channel. If the resistor is calibrated to three positions, three parameters can be adjusted, and five parameters to five positions. The issue of tuning the flight stability of the copter is considered. With a sharp increase in the throttle, a crash of the copter in one of the sides and its fall is possible. It was established that in order to prevent this, it is necessary to use identically selected ESC controllers, motors and the correct setting of PID parameters, in particular according to YAW.

Keywords: OMNIBUSF4V3, PID controller, INAV, GPS receiver, AIR MODE, STM32F4, HMC5883L, NEO6MV2, MPU6000.

УДК 621.396.933 (043.2)

д.т.н., проф. **Барабаш О.В.** (ДУТ)
Галахов Є.М. (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-06

ДОСЛІДЖЕННЯ ФУНКЦІЇ ІНТЕНСИВНОСТІ КІБЕРАТАК ЗА ДОПОМОГОЮ СТЕПЕНЕВОГО *P*-ПЕРЕТВОРЕННЯ АНАЛІТИЧНОЇ ФУНКЦІЇ

Забезпечення заданого рівня кібербезпеки вимагає визначення суб'єктів загрози, їх мету, наміри нападів на інфраструктуру та слабкі місця інформаційної безпеки підприємства. Для досягнення цих цілей, підприємства потребують нових рішень інформаційної безпеки, які поширюються на області, які захищені традиційною безпекою. Представлено відповідно рівні еволюції та адаптованості вірусів, а також політики захисту кібербезпеки. Показано, що помилки прогнозування функцій інтенсивності кібератак на підприємство частково обумовлені підбором моделі при дослідженні показників кібератак. Представлено відомі методології аналізу інтенсивності кібератак на підприємство. Доведено, що проблематика дослідження інтенсивності кібератак та їх передбачення є мало дослідженою у науковій літературі, що пов'язано із непередбаченістю кібератак та відсутністю у багатьох випадках реальних даних, а також доступних методів їх прогнозування.

Представлено математичне моделювання часових рядів інтенсивності кібератак на підприємство для надання комплексних рішень і прогнозів посилення стійкості підприємства проти поточних цільових кіберзагроз. Розглядається нелінійне диференціальне рівняння першого порядку – рівняння Бернуллі, що описує процес часового ряду інтенсивності кібератак. Аналіз функції інтенсивності кібератак проводиться аналітично завдяки степеневого p-перетворення аналітичною функцією. Розглянуто статистичні дані кількості кібератак на підприємстві за умови того, що плановий аудит проводиться раз в квартал. Представлено види кібератак на ураження мережевої інфраструктури, пропрієтарних додатків, рівня виправлень і конфігурацій сервера, стандартного програмного забезпечення та їх кількість на підприємстві за певні часові періоди. Представлена геометрична візуалізація зміни крутизни логістичної кривої інтенсивності кібератак при різних значеннях параметра з рівномірним кроком за період часу між плановими аудитами при застосуванні p-перетворення.

Ключові слова: кібербезпека, інтенсивність кібератак, рівняння Бернуллі, ураження, логістична крива.

Вступ та постановка завдання. По мірі появи нових IT-технологій зростає інтенсивність нових кібератак на IT-системи підприємства. Традиційні заходи кібербезпеки не справляються запобіганню або стримуванню цих нападів через їх швидкість та частоту. Існує декілька систем таких, як, наприклад система IBM i2 Enterprise Insight Analysis, для контролю кіберзагроз, що можуть допомогти підприємствам слугувати захистом від множини кібератак.

На рис. 1 представлено відповідно рівні еволюції та адаптованості вірусів та політики захисту кібербезпеки [1]. Таким чином, зміцнення кібербезпеки вимагає визначення суб'єктів загрози, їх мету, наміри нападів на інфраструктуру та слабкі місця інформаційної безпеки підприємства. Для досягнення цих цілей, підприємства потребують нових рішень інформаційної безпеки, які поширюються на області, які захищені традиційною безпекою.

Таким чином, захист кіберпростору підприємства у площині його інформаційної безпеки починається з кіберрозвідки у реальному часі. В сучасних умовах постає необхідність у математичному моделюванні часових рядів інтенсивності кібератак на підприємство для надання комплексних рішень і прогнозів посилення стійкості підприємства проти поточних цільових кіберзагроз.

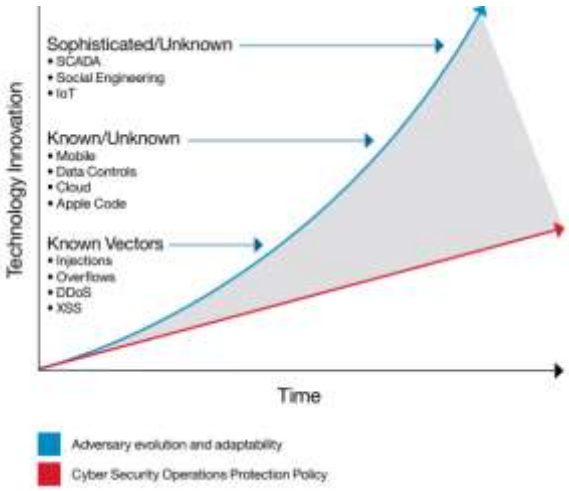


Рисунок 1 – Рівні еволюції та адаптованості вірусів та політики захисту у площині кібербезпеки [4]

Аналіз останніх досліджень і публікацій. Помилки прогнозування функцій інтенсивності кібератак на підприємство частково обумовлені підбором моделі при дослідженні показників кібератак [2]. Дослідження кібератак між плановими аудитами в технічній літературі називають смисловим розривом [3]. Автори у роботі [1] вивчають розрізнення відомих та невідомих атак. Ідентифікації характеристик зміни кібератак протягом певного часу присвячено праці [4-6].

Діаграми часових рядів інтенсивності кібератак на підприємство (кількість атак на годину) представлено на рис. 2 [7]. Горизонтальні лінії – це порогові значення, перевищення яких є небажаними для інформаційної безпеки підприємства.

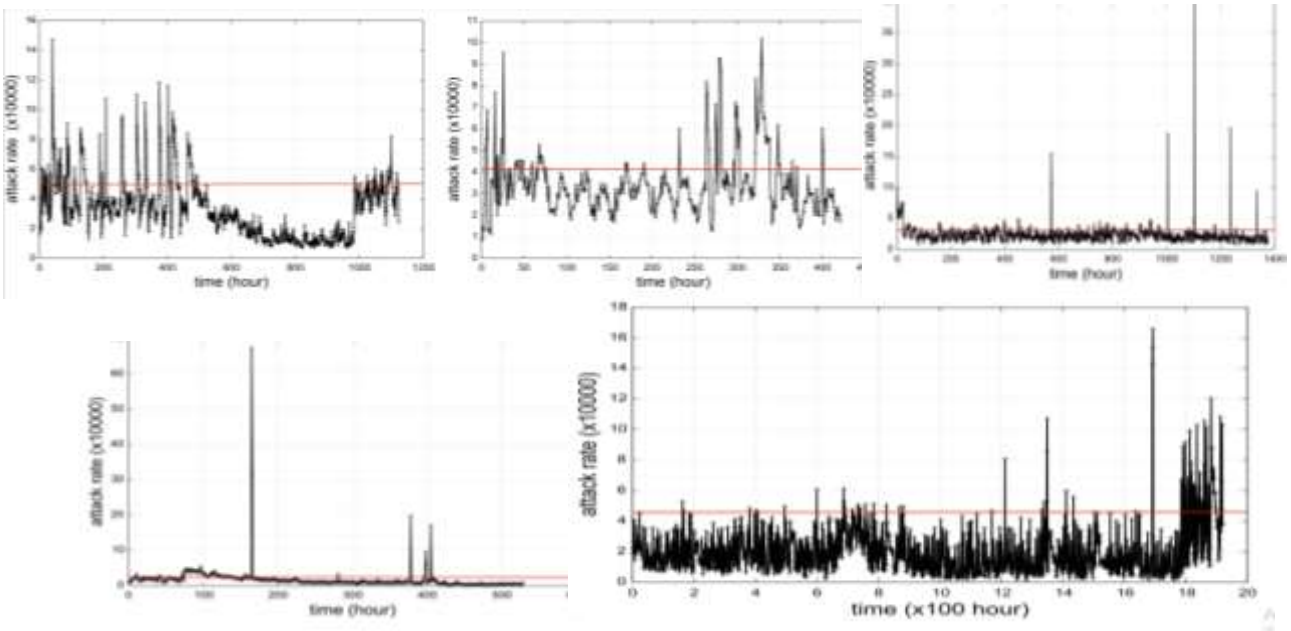


Рисунок 2 – Діаграми часових рядів частоти атак (кількість атак на годину) за 5 часових періодів між плановими аудитами [7]

У науковій праці [7] представлено нову методологію аналізу інтенсивності кібератак на підприємство. Методика аналізу використовує моделі EVT і TST, і має на меті точніше прогнозувати рівень кібератак. Застосування моделі FARIMA + GARCH дозволило прогнозувати швидкість атаки на 1 годину випередження з точністю, що можна вважати практичною. На рис. 3 представлено моделювання функції інтенсивності кібератак на підприємство на основі TST з порівнянням прогнозів на основі FARIMA + GARCH та FARIMA

[7]. Модель на основі TST, де точки чорного кольору представляють спостережувані частоти атак, а червоні крапки – це відповідні прораховані значення із застосуванням моделювання. Автори зазначають, що з рис. 3 видно, що модель FARIMA + GARCH підходить для I-III періодів краще, ніж FARIMA (особливо для екстремальних швидкостей атаки), але не підходить до IV-V періодів (хоча FARIMA + GARCH підходить точніше, ніж FARIMA) [7].

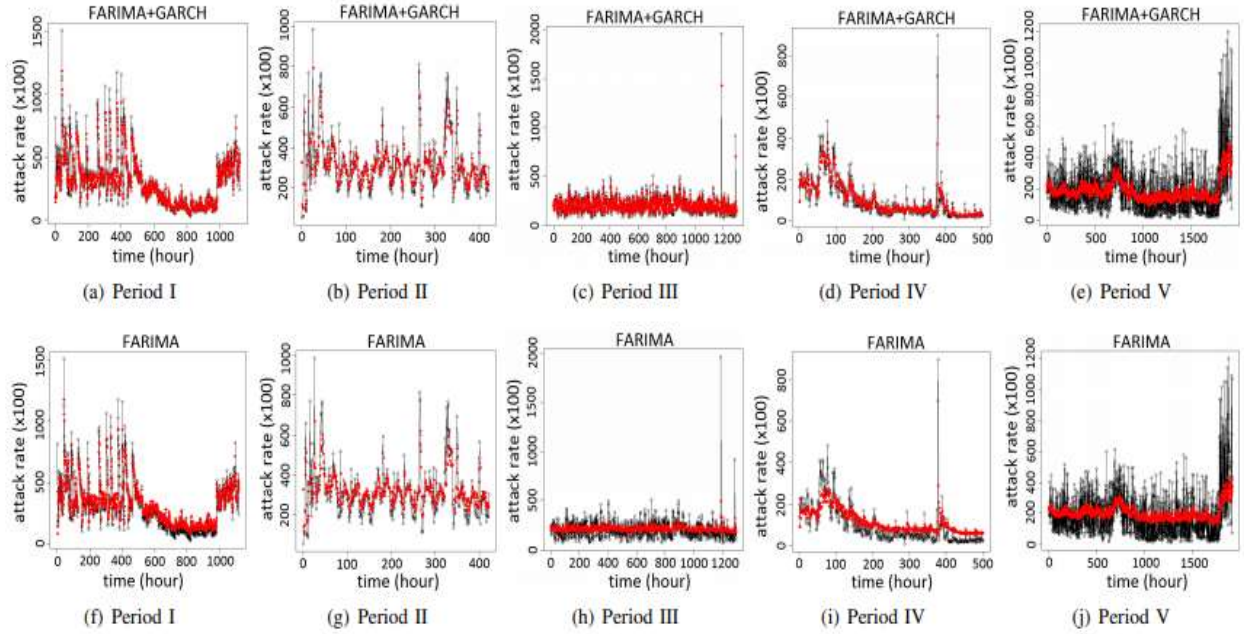


Рисунок 3 – Моделювання функції інтенсивності кібератак на підприємство на основі моделей TST з порівнянням прогнозів на основі FARIMA + GARCH та FARIMA [3]

На рис. 4 представлено порівняння прогнозів рівня віддачі від кібератак на основі EVT (тобто очікуваних величин екстремальної швидкості атаки), спостережуваних частот атаки протягом останніх 120 годин у кожному періоді та прогнозовані темпи атаки на основі TST.

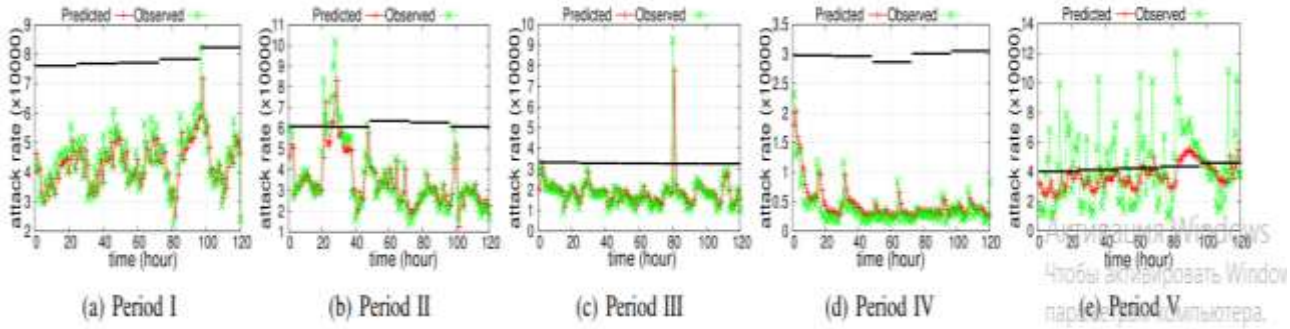


Рисунок 4 – Порівняння прогнозів рівня віддачі кібератак на основі EVT та TST [3]

Прогнози рівня на основі EVT виробляються спеціальним алгоритмом нанесені у вигляді горизонтальних ліній протягом відповідних інтервалів з 24 годин. Прогнози на основі TST виробляються алгоритмом 3. Для періодів I-III, побудовані прогнози повернення на основі EVT та TST, а також максимальні показники атак є точними. Для періоду IV, прогнози на основі EBT екстремальних частот нападу приблизно на порядок вище спостережуваних частот нападу, але прогнози на основі TST максимальних показників атаки є точними. Для періоду V ні EVT, ні TST не можуть дати точні прогнозі інтенсивності кібератак (рис. 3) [7].

У науковій літературі досліджуються кібератаки з відмовою в обслуговуванні (DoS) [8], вивчення хробаків та діяльності ботнетів [9], аналіз даних кількості кібератак, зібраних в чорному отворі [10] та в однобічному русі [11]. Дослідження [2, 12] присвячені класифікації дані на класи (сканування, однорангове сканування, програми, недоступні послуги, неправильні конфігурації, черв'яки тощо). У роботі [13] характеризується позиція кібербезпеки підприємства на основі даних зібраних в чорних дірах.

Таким чином, на сьогодні проблематика дослідження інтенсивності кібератак та їх передбачення є мало дослідженою у науковій літературі, що пов'язано із непередбаченістю кібератак та відсутністю у багатьох випадках реальних даних, а також доступних методів їх прогнозування.

Виклад основного матеріалу. Позначимо інтенсивність кібератак $I_K(t)$. Рівняння Бернуллі, що описує процес часового ряду інтенсивності кібератак має вигляд

$$dI_K(t)/dt - \zeta \cdot I_K(t) = -\zeta \frac{1}{I_K(t)_{Max}} \cdot {I_K}^2(t), \qquad I_K(0) = I_{K_0}, \tag{1}$$

де $I_K(t)_{Max}$ – максимально можливий рівень функції інтенсивності кібератак;

$I_K(0) = I_{K_0}$ – початковий рівень функції інтенсивності кібератак після проведення планового аудиту;

ζ – рівень корегування загроз кібератак завдяки звичайного аудиту;

Застосуємо до функції інтенсивності кібератак p-перетворення наступного вигляду:

$$\begin{gathered} I_K(t) \to i_K(t)^{p-1}, \\ . \\ p \in (0,1) \cup (1,\infty). \end{gathered} \tag{2}$$

З урахування p-перетворення рівняння (1) перетворюється таким чином:

$$(p-1) \cdot i_K(t)^{p-2} - \zeta \cdot i_K(t)^{p-1} = -\zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}} \cdot i_K(t)^{2p-2},$$

або

$$(p-1) \cdot i_K(t)^{-p} - \zeta \cdot i_K(t)^{1-p} = -\zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}}. \tag{3}$$

Домножимо ліву і праву частину на (–1). Тоді маємо:

$$-(p-1) \cdot i_K(t)^{-p} + \zeta \cdot i_K(t)^{1-p} = \zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}}.$$

Зробимо заміну:

$$\begin{gathered} i_K(t)^{1-p} = \Psi, \\ (1-p) \cdot i_K(t)^{-p} \cdot di_K(t)/dt = d\Psi/dt, \end{gathered}$$

або

$$-(p-1) \cdot i_K(t)^{-p} \cdot di_K(t)/dt = d\Psi/dt.$$

Тепер рівняння (3) зводиться до лінійного диференціального рівняння 1-го порядку:

$$d\Psi/dt + \zeta \cdot \Psi = \zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}}. \tag{4}$$

Загальний розв'язок цього рівняння має вигляд:

$$\Psi = \frac{1}{{i_K(t)^{p-1}}_{Max}} + ce^{-\zeta t}. \tag{5}$$

Враховуючи p-перетворення, початкові умови набувають вигляду:

$$\Psi(0) = i_K^{1-p}(0). \tag{6}$$

Тепер одержимо розв'язок диференціального рівняння (4) у вигляді:

$$i_K(t) = \frac{i_K(t)_{Max}}{\left(1 + \frac{i_K(t)^{p-1}_{Max} - i_K{}^{p-1}(0)}{i_K{}^{p-1}(0)} \cdot e^{-\zeta t}\right)^{\frac{1}{p-1}}}. \tag{7}$$

Функція (7) у безрозмірному вигляді:

$$\frac{i_K(t)}{i_K(t)_{Max}} = \frac{1}{\left(1 + \frac{1 - \frac{i_K{}^{p-1}(0)}{i_K(t)^{p-1}_{Max}}}{\frac{i_K{}^{p-1}(0)}{i_K(t)^{p-1}_{Max}}} \cdot e^{-\zeta \frac{t}{T}}\right)^{\frac{1}{p-1}}}, \tag{8}$$

Введемо позначення безрозмірних змінних:

$$i_K{}^*(t) = \frac{i_K(t)}{i_K(t)_{Max}}, \qquad t^* = \frac{t}{T}. \tag{9}$$

де T – період між плановими аудитами.

Остаточно отримаємо функцію інтенсивності кібератак із урахуванням степеневого p-перетворення у вигляді:

$$i_K{}^*(t) = \frac{1}{\left(1 + \frac{1 - i_K{}^*(0)}{i_K{}^*(0)} \cdot e^{-\zeta t^*}\right)^{\frac{1}{p-1}}}. \tag{10}$$

Знайшовши першу та другу похідні функції (8), знаходимо координати точки перегину:

$$\left(t^*, i_K{}^*(t)\right) = \left(\frac{1}{\zeta} \ln\left(\frac{1}{(p-1)} \cdot \frac{i_K{}^{p-1}(t)_{Max} - i_K{}^{p-1}(0)}{i_K{}^{p-1}(0)}\right);\ i_K(t)_{Max} \cdot p^{-\frac{1}{p-1}}\right). \tag{11}$$

Розглянемо статистичні дані кількості кібератак на підприємстві за умови того, що плановий аудит проводиться раз в квартал.

На рис. 5 представлено розподіл кількості кібератак за три часових періоди 2019 року за основними моделями кібератак.

Стосовно ураження мережевої інфраструктури (див. рис. 5), то відмітимо, що зловмисні користувачі використовують програми HackTool під час налаштування атак на локальні або віддалені комп'ютери, що актуально при залученні фріланс-ресурсу. Програми цього класу можуть активувати незареєстровані програмні продукти Microsoft. Такі програми можна використовувати разом із шкідливим чи небажаним програмним забезпеченням. Програми HackTool використовуються для створення нових користувачів зі списку дозволених відвідувачів системи та видалення інформації із системних журналів, щоб приховати присутність зловмисного користувача в системі. Ці програми також використовуються для аналізу та збору мережевих пакетів для здійснення конкретних шкідливих дій.

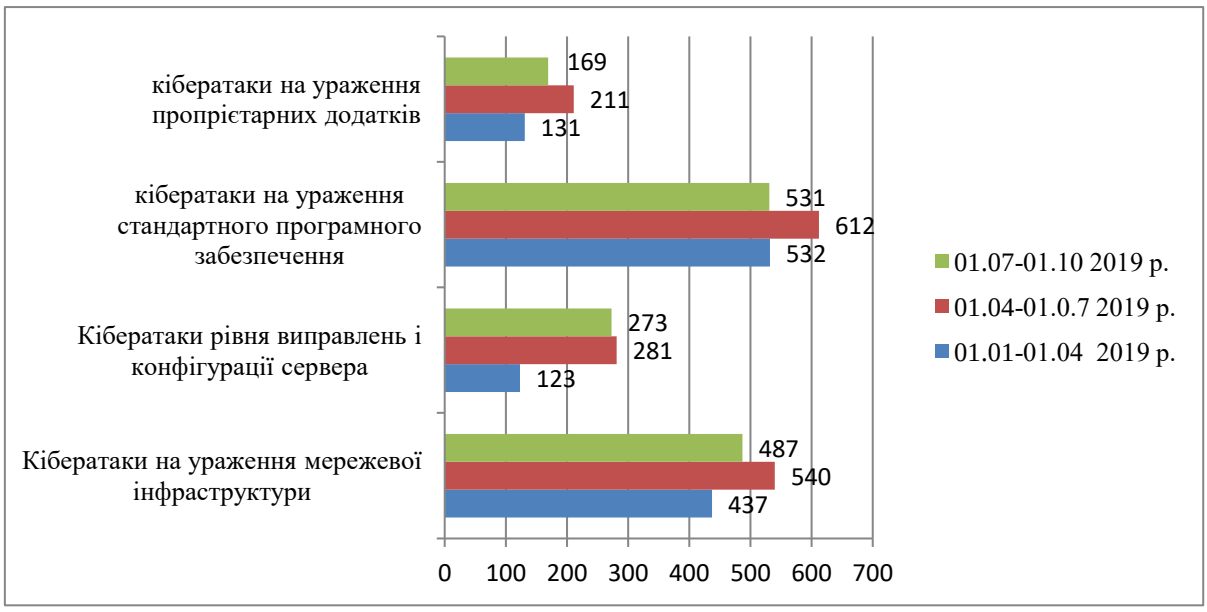


Рисунок 5 – Діаграма кількості кібератак за три часових періоди за основними моделями кібератак

Джерело: складено автором на основі даних підприємства

У табл. 1 представлено види кібератак на ураження мережевої інфраструктури та їх кількість на підприємстві по кварталам за період 2017 – 2019 рр.

Таблиця 1

Види кібератак на ураження мережевої інфраструктури та їх кількість на підприємстві за період 2017 – 2019 рр.

Джерело: складено на основі даних підприємств

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
U1	HackTool.Win32.KMSAuto.c	19	36	58	35	66	78	33	46	70	43	57	75
U2	HackTool.Win32.KMSAuto.ew	21	35	56	34	63	75	32	45	69	42	54	72
U3	DangerousObject.Multi.Generic	23	33	53	31	59	70	26	36	55	40	50	67
U4	Trojan.Script.Generic	19	31	50	26	49	58	24	33	51	38	40	55
U5	HackTool.MSIL.KMSAuto.by	18	28	46	25	47	56	21	28	44	35	38	53
U6	HackTool.Win64.KMSAuto.b	16	27	43	20	39	46	20	28	43	34	30	43
U7	HackTool.MSIL.KMSAuto.bx	15	27	42	18	34	42	20	27	42	34	25	39
U8	HackTool.Win32.KMSAuto.bu	15	24	40	18	31	40	18	26	40	31	22	37
U1	HackTool.MSIL.KMSAuto.dc	10	18	28	17	32	38	17	25	38	25	23	35
U10	HackTool.MSIL.KMSAuto.a	8	13	21	15	29	37	15	23	35	20	20	34

У табл. 2 представлено види кібератак на ураження рівня виправлень і конфігурації сервера та їх кількість на підприємстві по кварталам за період 2017 – 2019 рр.

Таблиця 2

Види кібератак (рівня виправлень і конфігурації сервера) та їх кількість на підприємстві за період 2017 – 2019 рр.

Джерело: складено автором на основі даних підприємств

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
N1	Intrusion.Win.MS17-010.o	18	19	21	35	41	47	30	33	35	32	38	42
N2	Bruteforce.Generic.Rdp.d	11	12	14	34	39	39	28	30	33	30	36	40
N3	Intrusion.Win.MS17-010.p	9	13	13	31	32	36	26	29	31	28	29	38
N4	Bruteforce.Generic.Rdp.a	10	10	13	24	31	35	24	26	29	26	28	36
N5	Bruteforce.Generic.Rdp.c	9	10	12	25	24	31	24	27	29	26	21	36
N6	Intrusion.Win.NETAPI.buffer-overflow.exploit	7	11	12	20	23	27	23	25	28	25	20	35
N7	Intrusion.Win.CVE-2017-0147.d.leak	8	9	11	19	22	27	21	23	26	23	19	33
N8	Intrusion.Generic.CVE-2018-1273.exploit	7	7	11	18	11	15	20	20	25	22	8	32
N1	Intrusion.Win.CVE-2019-0708.b.exploit	5	5	9	17	10	13	14	16	19	16	7	26
N10	Intrusion.Win.EternalRomance.s	8	5	7	13	7	11	13	11	18	15	4	25

У табл. 3 представлено види кібератак на ураження стандартного програмного забезпечення та їх кількість підприємстві по кварталам за період 2017 – 2019 рр.

Таблиця 3

Види кібератак та їх кількість (стандартне програмне забезпечення) на підприємстві за період 2017 – 2019 рр.

Джерело: складено автором на основі даних підприємства

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
H1	Trojan.Multi.BroSubsc.gen	45	55	68	53	67	84	27	51	61	25	29	65
H2	HackTool.MSIL.KMSAuto.a	42	52	65	52	66	83	28	52	62	26	30	62
H3	HackTool.MSIL.KMSAuto.cz	39	49	62	45	65	77	22	44	62	20	24	59
H4	Trojan.Script.Generic	35	45	58	44	51	75	24	44	51	22	26	55
H5	DangerousObject.Multi.Generic	31	41	56	33	47	64	22	37	50	20	24	53
H6	Trojan.Multi.Agent.gen	30	40	53	19	33	50	23	19	50	21	25	50
H7	Trojan.Multi.GenBadur.gen	29	39	52	16	31	48	21	11	50	19	23	49
H8	HackTool.Win32.KMSAuto.er	26	37	50	15	29	46	18	15	50	16	20	47
H9	HackTool.MSIL.KMSAuto.dc	15	22	38	13	19	44	14	10	49	12	16	35
H10	HackTool.Win32.KMSAuto.bu	7	9	30	3	7	41	14	4	46	12	16	27

У табл. 4 представлено кібератаки на ураження пропрієтарних додатків та їх кількість на підприємстві по кварталам за період 2017 – 2019 рр.

На рис. 6 представлено часові ряди кількості кібератак на систему підприємства за однакові часові періоди 2017 – 2019 років, що попадають у часовий проміжок від кінця аудиту до початку наступного.

Таблиця 4

Види кібератак (пропрієтарні додатки) та їх кількість
на підприємстві за період 2017 – 2019 рр.

Джерело: складено автором на основі даних підприємства

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
E1	Exploit.VBS.Agent.ad	27	51	29	30	24	33	27	26	25	22	20	26
E2	Exploit.Win32.Agent.gen	12	52	14	31	25	31	28	27	23	7	21	11
E3	Exploit.MSOffice.CVE-2017-11882.gen	11	49	13	28	22	29	22	24	21	3	15	10
E4	Exploit.AndroidOS.Lotoor.be	11	45	13	24	18	27	24	20	19	6	13	10
E5	Exploit.AndroidOS.Lotoor.bg	10	41	12	20	14	25	22	16	18	9	15	9
E6	Exploit.WinLNK.CVE-2017-8464.ecr	10	40	12	19	13	21	23	15	16	5	16	9
E7	Exploit.Win32.ShellCode.jhs	9	39	11	18	12	19	21	14	16	4	9	8
E8	Exploit.AndroidOS.Lotoor.bm	9	37	11	16	10	11	18	12	15	7	11	8
E1	Exploit.AndroidOS.Lotoor.cd	7	22	9	3	3	9	14	5	11	2	7	6
E10	Exploit.Win32.ShadowBrokers.ae	5	9	7	5	2	6	14	4	5	5	7	4

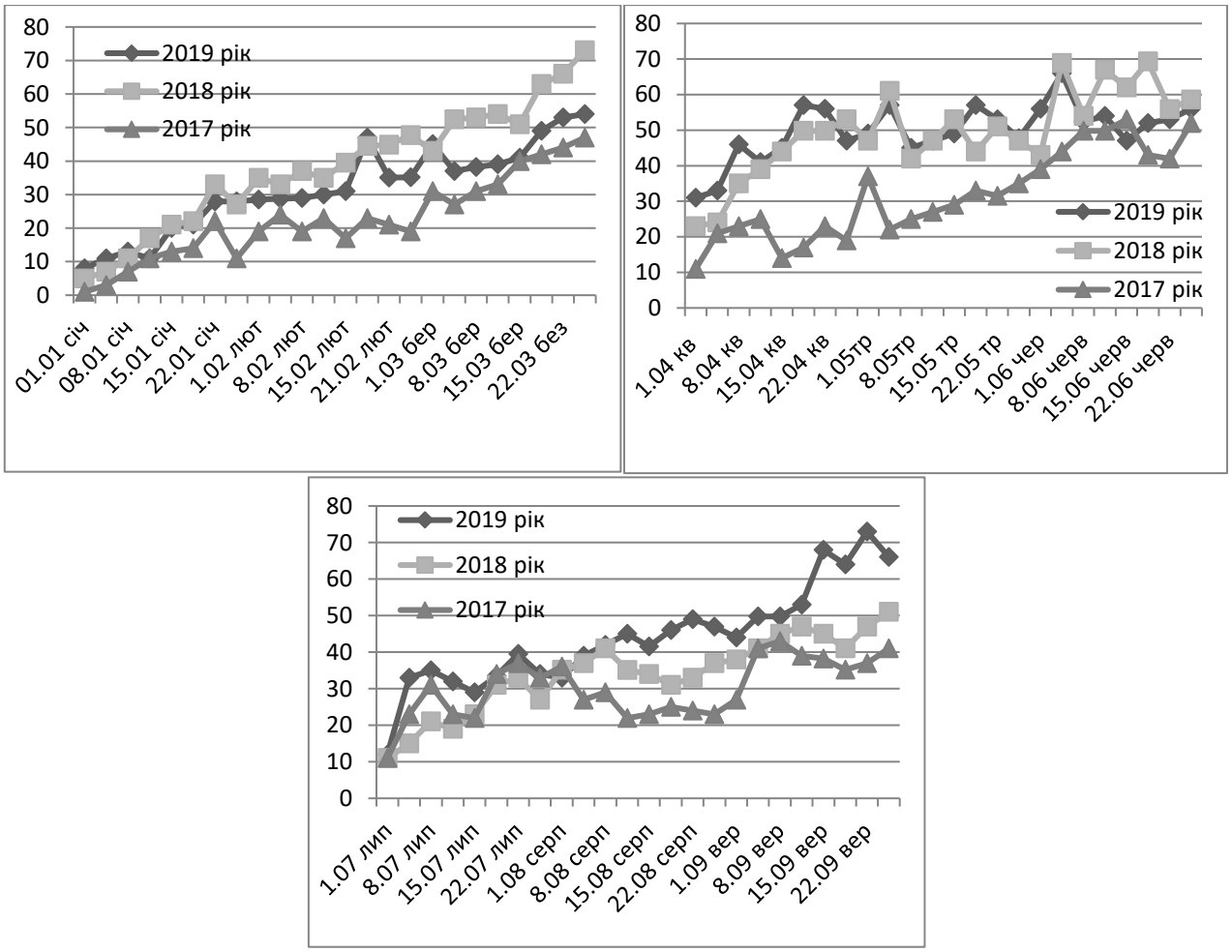
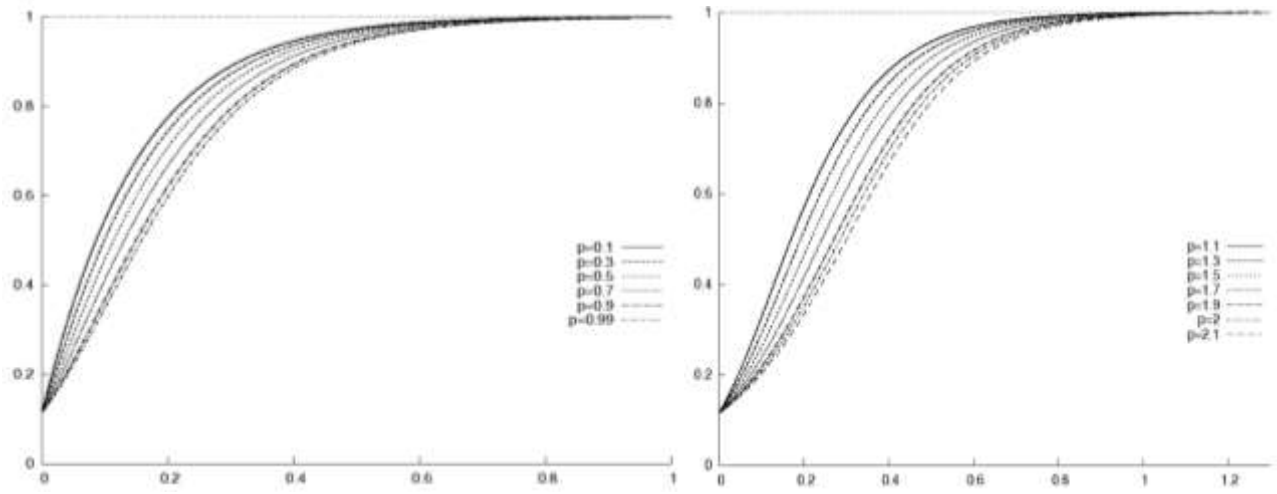


Рисунок 6 – Часові ряди кібератак на систему підприємства за часові періоди:
(1.01-31.03); (1.04-31.06); (1.04-31.06); (1.07-30.09) 2017 – 2019 років,
що починаються після проведення планових аудитів

Джерело: авторські розрахунки

На рис. 7 представлена геометрична візуалізація зміни крутизни логістичної кривої інтенсивності кібератак при параметрі $p \in (0,1)$ та $p \in (1,\ 2.1)$ з кроком 0,2 за період часу T.



а) б)

Рисунок 7 – Зміна крутизни логістичної кривої інтенсивності кібератак з кроком 0,2 за період часу T при параметрі: а) $p \in (0,1)$; б) $p \in (1,\ 2.1)$

Джерело: авторські розрахунки

Отже, необхідно апроксимувати загальну кількість статистичних даних за 4 періодами за 2017 – 2019 років з підбором відповідних параметрів *p* з *p*-перетворення і знайти прогнозний довірчий інтервал функції інтенсивності кібератак, що дасть можливість застосувати теорію еластичності функції інтенсивності кібератак, що, в свою чергу, приведе до визначення часового інтервалу, в якому ефективно проводити спеціальний аудит на підприємстві.

Висновки. Математичне моделювання часових рядів інтенсивності кібератак на підприємство розглядається з точки зору аналітичної інтерпретації за допомогою нелінійного диференціального рівняння 1-го порядку рівняння Бернуллі, що описує процес часового ряду інтенсивності кібератак. Для проведення аналізу функції інтенсивності кібератак було застосовано степеневе *p*-перетворення аналітичною функцією. Це дало можливаість введення малого параметра у функцію інтенсивності кібератак, що виражає чутливість логістичної кривої до зміни статистики і аналітично характеризує зміну крутизни логістичної кривої інтенсивності кібератак. Розглянуто статистичні дані кількості кібератак на підприємстві за умови того, що плановий аудит проводиться раз в квартал. Представлено види кібератак на ураження мережевої інфраструктури, пропрієтарних додатків, рівня виправлень і конфігурацій сервера, стандартного програмного забезпечення та їх кількість на підприємстві за певні часові періоди з їх геометричною візуалізацією. Дослідження є підгрунтям застосування теорії еластичності функції інтенсивності кібератак, що приведе до визначення часового інтервалу, на якому ефективно проводити спеціальний аудит на підприємстві.

ЛІТЕРАТУРА:

1. IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting. ZZS03196-USEN-06. URL: https://www.ibm.com/downloads/cas/WZKLWGPB

2. Шуклін Г.В., Барабаш О.В. Метод побудови стабілізаційної функції керування кібербезпекою на основі математичної моделі коливань під дією сил із запізненням. *Телекомунікаційні та інформаційні технології*. Київ. 2018. № 2 (59). С. 110–116.

3. Xu, Tingyang, Jiangwen Sun and Jinbo Bi (2015) ”Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction”. ACM, KDD 2015.

4. A. Joulin, E. Grave, P. Bojanowski and T. Mikolov (2017) “Bag of tricks for efficient text classification”. In Proceedings of the 15th Conference of the European Chapter of the Association for

Computational Linguistics: Volume 2, Short Papers. Association for Computational Linguistics, April 2017, pp. 427–431.

5. R. A. Bridges, C. L. Jones, M. D. Iannacone, K. M. Testa and J. R. Goodall (2014) "Automatic labeling for entity extraction in cyber security". In ASE Third International Conference on Cyber Security, Academy of Science and Engineering (ASE), 2014.

6. S. K. Lim, A. O. Muis, W. Lu and C. H. Ong (2017) "Malwaretextdb: A database for annotated malware articles". Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Vancouver, Canada: Association for Computational Linguistics, July 2017, pp. 1557–1567. [Online]. Available: http://aclweb.org/anthology/P17-1143.

7. Zhenxin Zhan, Maochao Xu and Shouhuai Xu. (2016) "Predicting Cyber Attack Rates with Extreme Values". arXiv:1603.07432v1 [cs.CR] 24 Mar 2016.

8. B. J. Dorr, M. Petrovic, J. F. Allen, C. M. Teng and A. Dalton (2014) "Discovering and characterizing emerging events in big data". AAAI Fall Symposium Series, 2014.

9. Sauerwein, C. Sillaber, M. M. Huber, A. Mussmann and R. Breu (2018) "The tweet advantage: An empirical analysis of 0-day vulnerability information shared on twitter". IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2018, pp. 201–215.

10. Babko-Malaya O., Cathey R., Hinton S., Maimon D. and Gladkova T. (2017) "Detection of hacking behaviors and communication patterns on social media". In: Proceedings of the 2017 IEEE International Conference on Big Data, pp. 4636 – 4641.

11. Accenture Security (2017). Cost of cyber crime study. https://www.accenture. com/us-en/insight-cost-of-cybercrime-2017. Accessed 5 Jan 2018.

12. Bilge L., Han Y. and Dell'Amico M (2017). "Riskteller: Predicting the risk of cyber incidents". In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, New York. pp 1299 – 1311. https://doi.org/10.1145/3133956.3134022.

13. Okutan A., Yang S.J. and McConky K. (2018). "Forecasting cyber attacks with imbalanced data sets and different time granularities". CoRR abs/1803.09560. http://arxiv.org/abs/1803.09560. 1803.09560.

REFERENCES:

1. IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting. ZZS03196-USEN-06. URL: https://www.ibm.com/downloads/cas/WZKLWGPB

2. Shuklin, H.V. and Barabash, O.V. (2018) "Metod pobudovy stabilizatsiinoi funktsii keruvannia kiberbezpekoiu na osnovi matematychnoi modeli kolyvan pid diieiu syl iz zapiznenniam" [A method of constructing a stabilization function for cybersecurity management based on a mathematical model of oscillations under the influence of delayed forces], Telecommunication and information technologies, Kyiv, No. 2 (59), pp. 110–116.

3. Xu, Tingyang, Jiangwen Sun and Jinbo Bi (2015) "Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction". ACM, KDD 2015.

4. A. Joulin, E. Grave, P. Bojanowski and T. Mikolov (2017) "Bag of tricks for efficient text classification". In Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers. Association for Computational Linguistics, April 2017, pp. 427–431.

5. R. A. Bridges, C. L. Jones, M. D. Iannacone, K. M. Testa and J. R. Goodall (2014) "Automatic labeling for entity extraction in cyber security". In ASE Third International Conference on Cyber Security, Academy of Science and Engineering (ASE), 2014.

6. S. K. Lim, A. O. Muis, W. Lu and C. H. Ong (2017) "Malwaretextdb: A database for annotated malware articles". Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Vancouver, Canada: Association for Computational Linguistics, July 2017, pp. 1557–1567. [Online]. Available: http://aclweb.org/anthology/P17-1143.

7. Zhenxin Zhan, Maochao Xu and Shouhuai Xu. (2016) "Predicting Cyber Attack Rates with Extreme Values". arXiv:1603.07432v1 [cs.CR] 24 Mar 2016.

8. B. J. Dorr, M. Petrovic, J. F. Allen, C. M. Teng and A. Dalton (2014) "Discovering and characterizing emerging events in big data". AAAI Fall Symposium Series, 2014.

9. Sauerwein, C. Sillaber, M. M. Huber, A. Mussmann and R. Breu (2018) "The tweet advantage: An empirical analysis of 0-day vulnerability information shared on twitter". IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2018, pp. 201–215.

10. Babko-Malaya O., Cathey R., Hinton S., Maimon D. and Gladkova T. (2017) “Detection of hacking behaviors and communication patterns on social media”. In: Proceedings of the 2017 IEEE International Conference on Big Data, pp. 4636 – 4641.

11. Accenture Security (2017). Cost of cyber crime study. https://www.accenture. com/us-en/insight-cost-of-cybercrime-2017. Accessed 5 Jan 2018.

12. Bilge L., Han Y. and Dell’Amico M (2017). “Riskteller: Predicting the risk of cyber incidents”. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, New York. pp 1299 – 1311. https://doi.org/10.1145/3133956.3134022.

13. Okutan A., Yang S.J. and McConky K. (2018). “Forecasting cyber attacks with imbalanced data sets and different time granularities”. CoRR abs/1803.09560. http://arxiv.org/abs/1803.09560. 1803.09560.

д.т.н., проф. Барабаш О.В., Галахов Е.М.

ИССЛЕДОВАНИЕ ФУНКЦИИ ИНТЕНСИВНОСТИ КИБЕРАТАК ПРИ ПОМОЩИ СТЕПЕННОГО *P*-ПРЕОБРАЗОВАНИЯ АНАЛИТИЧЕСКОЙ ФУНКЦИИ

Обеспечение заданного уровня кибербезопасности требует определения субъектов угрозы, их целей, намерения нападений на инфраструктуру и слабые места информационной безопасности предприятия. Для достижения этих целей, на предприятиях нужно разрабатывать новые решения информационной безопасности, распространяющиеся на области, которые защищены традиционной безопасностью. Представлены соответственно уровни эволюции и адаптированности вирусов, а также политики защиты кибербезопасности. Показано, что ошибки прогнозирования функций интенсивности кибератак на предприятие частично обусловлены подбором модели при исследовании показателей кибератак. Представлены известные методологии анализа интенсивности кибератак на предприятие. Доказано, что проблематика исследования интенсивности кибератак и их предсказания мало исследованы в научной литературе, что связано с непредсказуемостью кибератак и отсутствием во многих случаях реальных данных, а также доступных методов их прогнозирования.

Представлены математическое моделирование временных рядов интенсивности кибератак на предприятие для предоставления комплексных решений и прогнозов усиления устойчивости предприятия против текущих целевых киберугроз. Рассматривается нелинейное дифференциальное уравнение первого порядка – уравнение Бернулли, которое описывает процесс временного ряда интенсивности кибератак. Анализ функции интенсивности кибератак проводится аналитически благодаря степенному p-преобразованию аналитической функцией. Рассмотрены статистические данные количества кибератак на предприятии при условии того, что плановый аудит проводится раз в квартал. Представлены виды кибератак на поражение сетевой инфраструктуры, проприетарных приложений, уровня исправлений и конфигураций сервера, стандартного программного обеспечения и их количество на предприятии за определенные временные периоды. Представлена геометрическая визуализация изменения крутизны логистической кривой интенсивности кибератак при различных значениях параметра с равномерным шагом за период между плановыми аудитами при применении p-преобразования.

Ключевые слова: кибербезопасность, интенсивность кибератак, уравнение Бернулли, поражения, логистическая кривая.

Prof. Barabash O.V., Halakhov Y.

RESEARCH OF THE FUNCTION OF INTENSITY OF CYBER ATTACKS USING THE DEGREE OF P-TRANSFORMATION OF ANALYTICAL FUNCTION

Strengthening cybersecurity requires identifying the subjects of the threat, their goals, intentions of attacks on the infrastructure and weaknesses of the information security of the enterprise. To achieve these goals, enterprises need new information security solutions that extend to areas that are protected by traditional security. The levels of evolution and adaptability of viruses, as well as cybersecurity protection policies, respectively, are presented. It is shown that errors in predicting the functions of the intensity of cyberattacks at an enterprise are partially due to the selection of a model in the study of indicators of cyberattacks. Known methodologies for analyzing the intensity of cyberattacks at an enterprise are presented. It is proved that the problems of studying the intensity of cyberattacks and their predictions have

been little studied in the scientific literature, which is associated with the unpredictability of cyberattacks and the absence in many cases of real data, as well as available methods for predicting them.

Mathematical modeling of time series of the intensity of cyberattacks per enterprise is presented to provide comprehensive solutions and predictions of strengthening the enterprise's resistance against current targeted cyber threats. We consider a first-order nonlinear differential equation, the Bernoulli equation, which describes the process of the time series of the intensity of cyberattacks. The analysis of the intensity function of cyberattacks is carried out analytically due to the power-law p-transformation by the analytical function. Statistical data on the number of cyberattacks at the enterprise are considered, provided that a scheduled audit is carried out once a quarter. The types of cyberattacks to defeat network infrastructure, proprietary applications, the level of patches and server configurations, standard software, and their number at the enterprise for certain time periods are presented. A geometric visualization of the change in the steepness of the logistic curve of the intensity of cyberattacks is presented at various parameter values with a uniform step for the period between scheduled audits when applying p-conversion.

Keywords: cyber security, cyberattack intensity, Bernoulli equation, defeat, logistic curve.

УДК 004.85

к.т.н., доц. **Бойчук В.О.** (ХмНУ)
к.е.н., доц. **Бойчук А.А.** (ТНЕУ)
Бойчук М.В. (ХмНУ)
Бурдюг О.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-07

МЕТОД ФОРМУВАННЯ ПОСЛІДОВНОСТІ ДІЙ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ

У статті запропоновано підхід, де реалізація формування послідовностей дій інтелектуальних агентів виконується по аналогії з діяльністю біологічних організмів з використанням механізму емоцій для динамічного налаштування організму на виконання дій. Таким чином імітуються функції лімбічної системи в організації рухів на основі мотиваційної поведінки. При плануванні в першу чергу визначається загальний стан агенту. Використовуючи отриманий стан формується послідовність дій. Такий підхід дасть можливість динамічно переналаштовувати послідовність і реагувати на небезпечну ситуацію або на зміну внутрішнього стану агенту.

Інтелектуальний агент отримує з сенсорів і рецепторів ознаки початкової умови по ній визначається ціль та формується послідовність дій. Елементами послідовності дій є елементарні дії. Елементарна дія характеризується набором вхідних параметрів для функціонування. Ознаки передумови відповідають першій дії в послідовності, остання дія в послідовності прив'язана до ознаки цілі.

Послідовність дій агенту представляється орграфом, де вершини визначають елементарні дії, а ребра визначають ступінь сили зв'язку між ними. Початкові умови відповідають першій дії в послідовності, з неї розпочинається реалізація послідовності дій. Ознаки цілі відповідають останній вершині в послідовності дій

Ваги зв'язків змінюються при встановлені змінних загального стану, що дає змогу виконати послідовність дій в реальному масштабі часу з динамічним переналаштуванням і вибрати серед характерних для конкретного стану послідовностей дій. Метод формує послідовність дій, яка ініціюється емоційними станами, і переводить її в послідовність автоматичних дій на основі досягнення цілі і яка в майбутньому буде виконуватись в нормальному стані. Для перевірки функціонування методу реалізований симулятор агенту-роботу в середовищі програми V-REP. Отримані результати можуть бути використані для інтелектуального планування на основі підкріплення при керуванні агентами, роботами на виробничих підприємствах, військовими агентами, потоками міського руху, логістичними системами, соціальними явищами.

Ключові слова: інтелектуальний агент, планування, модель, Q-навчання, емоційні стани, навчання з підкріпленням.

Вступ. Планування - це процес генерації уявлень про майбутню поведінку до того, як отримані таким чином плани будуть використані для реалізації цієї поведінки. Результатом планування зазвичай є деяка множина дій, а також накладені на них часові та інші обмеження і передбачається, що ці дії будуть виконуватися будь-яким агентом або агентами.

Більшість підходів, що застосовуються в штучному інтелекті при плануванні, не прагнуть будувати функціональні моделі людського мозку або його відділів. Рішення, пропоновані теоріями штучного інтелекту, будують моделі, поведінка яких схожа з поведінкою людини. Але внутрішній склад цих моделей, як правило, не є моделлю нервової тканини або процесів, що протікають в нервовій тканині живої істоти. Тобто штучний інтелект хоч і займається відтворенням окремих функцій творчої діяльності людини, але його методи кардинально відрізняються від природного, біологічного протікання інтелектуальних процесів.

Як правило інтелектуальне планування засноване на апараті математичної логіки, а міркування, необхідні для формування плану, зводяться до логічного висновку. Таким чином, логічний висновок, в даному випадку, і буде моделлю міркувань. Традиційне планування не може бути безпосередньо застосовано до задач реального світу, оскільки проблемний простір пошуку занадто великий. А між тим біологічні істоти за рахунок навчання з підкріпленням можуть планувати свої дії з достатньою для вживання ефективністю. Запозичення таких ідей планування повинно підвищити ефективність функціонування інтелектуальних агентів.

Аналіз останніх досліджень і публікацій. Якщо розглянути планування в природі, то вищі біологічні істоти не навчаються з нуля, але використовують невеликий набір простих моделей поведінки. Ці поведінки низького рівня можуть порівняно легко спроектовані або засвоєні, але задача координації цих поведінок досить складна. Для перемикання і запам’ятовування(підкріплення) поведінок використовується механізм емоції.

Розглянемо приклади реалізації навчання на основі емоцій з підкріпленням при плануванні дій інтелектуальних агентів.

Архітектура EB [1] заснована на емоціях, в якій традиційна адаптивна система навчання доповнюється системою емоцій, яка відповідальна за навчання та поведінку. Агент має деякі вроджені емоції, що визначають його цілі, і він потім засвоює емоційні асоціації середовища-стану, які визначають його рішення. Агент використовує алгоритм Q-навчання для навчання вибору поведінки під час взаємодії зі своїм оточенням.

Архітектура EB II [2] - складається з двох основних систем: цільової системи (GS) та адаптивної системи (AS). Цільова системи оцінює ефективність роботи адаптивної системи з точки зору гомеостатичних змінних і визначає, коли поведінку слід перервати. Обчислюється так зване значення «благополуччя», яке використовується як підкріплення адаптивною системою та визначає кроки запуску. Адаптивна система дізнається, яку поведінку вибрати на кроках запуску, використовуючи методи навчання з підкріпленням, спираючись на нейронні мережі для зберігання значень корисності.

Сукупність перцептивних значень та внутрішніх значень використовувались при обчисленні одного мультимірного емоційного стану. Цей стан, у свою чергу, використовувався для визначення навчання на кожному часовому кроці та значні відмінності у його значенні вважалися релевантними подіями, що використовуються для запуску механізм вибору поведінки.

Цілі чітко визначені і пов'язані з гомеостатичними змінними. Ці гомеостатичні змінні асоціюються з трьома різними станами: цільовим (Target), відновлення(Recovery) та небезпечним (Dangerous). Стан кожної змінної залежить від її безперервного значення, яке групується на чотирьох якісних категоріях: оптимальний (Optimal), прийнятний (Acceptable), дефіцитний (Deficient) і небезпечний(Danger). Змінна залишається в цільовому стані до тих пір, поки є її значення оптимальні або прийнятні, але вона повертається до свого цільового стану лише після того, як його значення знову стануть оптимальними.

Архітектура ALEC (Asynchronous Learning by Emotion and Cognition)[3], яка має на меті покращити ефективність навчання шляхом розширення архітектури ЕВ когнітивною системою, що доповнює свої поточні можливості адаптації на основі емоцій правилами, які створюються з взаємодії агент-середовище. Різні можливості навчання двох системи та їх взаємодія можуть створити більш потужну адаптивну систему.

В іншій системі планування дій агентів [4] формується набір поведінкових правил, представлений в MYCIN подібній формі, тобто в формі продукцій з коефіцієнтами впевненості. Вплив емоцій на вчинення дії реалізується як позитивний зворотний зв'язок між вихідним сигналом (поточна дія) і поведінковими правилами.

Основна система управління робота оперує тільки термінами поведінкових дій. Ця система управління не використовує таких дій, як "Повернути ліворуч або праворуч"," Рухатися вперед або назад " і т.п. Всі ці дії перенесені на нижній рівень управління. Основна система управління застосовує складні поведінкові процедури: пошуку їжі, процедури сну (відпочинку) і т.д.

Висновок проходить через блок "Збудження/Гальмування" для активації відповідних про процесів збудження і гальмування. Параметр збудження реалізований через аналог штучного нейрона. Цей елемент бере вхідні сигнали (від давачів і блоку "Потреби"), підсумовує їх і передає на вихід. На відміну від стандартного нейрона тут не використовуються вагові коефіцієнти (зважені входи), а застосовується вага для всіх входів. Значення цієї ваги є параметром збудження.

При використанні конекціоністского підходу в алгоритмі Q-Learning табличне представлення Q-функції замінюється нейронною мережею [5]. На входи мережі подаються стани, а вихідними даними є оцінки Q-значень. Таким чином, ніяких серйозних змін в класичний Q-Learning не вноситься, просто змінюється засіб зберігання оцінок Q-значень. Використовується методика роботи з нейронною мережею, запропонована Ліном, яка полягає в застосуванні окремої нейронної мережі для кожної дії .

На кожній ітерації роботи алгоритму поточний стан системи подається на входи кожної нейронної мережі, однак оновлення ваг здійснюється тільки для тієї нейронної мережі, дія якої була вибрана. Прокручування списку стан-дія в зворотному порядку дозволяє виробляти навчання на більш правильних оцінках.

Прокручування списку стан – дія в зворотному порядку дозволяє розробляти процес навчання на більш правильних оцінках. Однак послідовність кроків, яку виконує система, може виявитися неоптимальною і, отже, оцінки на яких буде проводитися навчання, також виявляються неоптимальними.

Якщо розглянути недоліки цих методів, то можна сказати, що хоча вони й використовують навчання підкріпленням, однак не призначені для динамічного, гнучкого планування і навчання послідовності дій.

Постановка задачі. Для розв’язку задачі планування діяльності агенту необхідно здійснити послідовність дій при яких середовище перейде з початкового стану у потрібний цільовий стан.

У природному середовищі організми виконують ідентифікацію та класифікацію початкових умов і цілі керування використовуючи нейронні мережі на основі параметрів зовнішнього середовища і внутрішнього стану організму. Послідовність дій аналогічно реалізується з використанням нейронних мереж головного, спинного мозку і т.д.

Відповідно вищесказаному реалізацію планування дій можна виконувати по аналогії з діяльністю біологічних організмів з використанням механізму емоцій для динамічного налаштування організму на виконання дій.

Основна частина. Регулювання емоцій здійснюється лімбічною системою, яка складається з старих відділів переднього мозку.

Таким чином ми будемо імітувати функції лімбічної системи в організації рухів на основі мотиваційної поведінки.

Назвемо аналоги емоцій загальними станам агенту. Вони визначаються множиною змінних $y_1,\ldots,y_k$. від 0 до 1, де значення кожної змінної відображує інтенсивність стану.

При плануванні в першу чергу визначається загальний стан агента. Використовуючи отриманий стан формується послідовність дій. Такий підхід дасть можливість динамічно переналаштовувати послідовність і реагувати на небезпечну ситуацію або на зміну внутрішнього стану агента.

У випадку, якщо інтенсивність деякої змінної загального стану вище деякого порогу, агент може виконувати тільки стандартні стереотипні дії, які характерні для цього стану. Якщо ж інтенсивність змінної загального стану менше цього порога, то може бути вибрана інша послідовність дій. У випадку отримання інших параметрів загального стану системи дії агента можуть динамічно змінюватись.

Дані в агент надходять з зовнішніх сенсорів і з внутрішніх рецепторів. Для планування дій і наступної обробки ці дані різних типів переводяться в символьний та кількісний вигляд. Дану функцію реалізують компоненти обробки сигналів з сенсорів і рецепторів. Фізично даними компонентами можуть бути і нейронні мережі різних типів і компоненти з функціями виконання обчислень і перетворень над кількісними даними.

Дані компоненти отримують набор кількісних значень $x_1,\ldots,x_n$ по яких можна обчислити стан агенту і використати при формуванні послідовності дій.

Загальна структура агента по пропонованому підходу зображена на рис. 1.

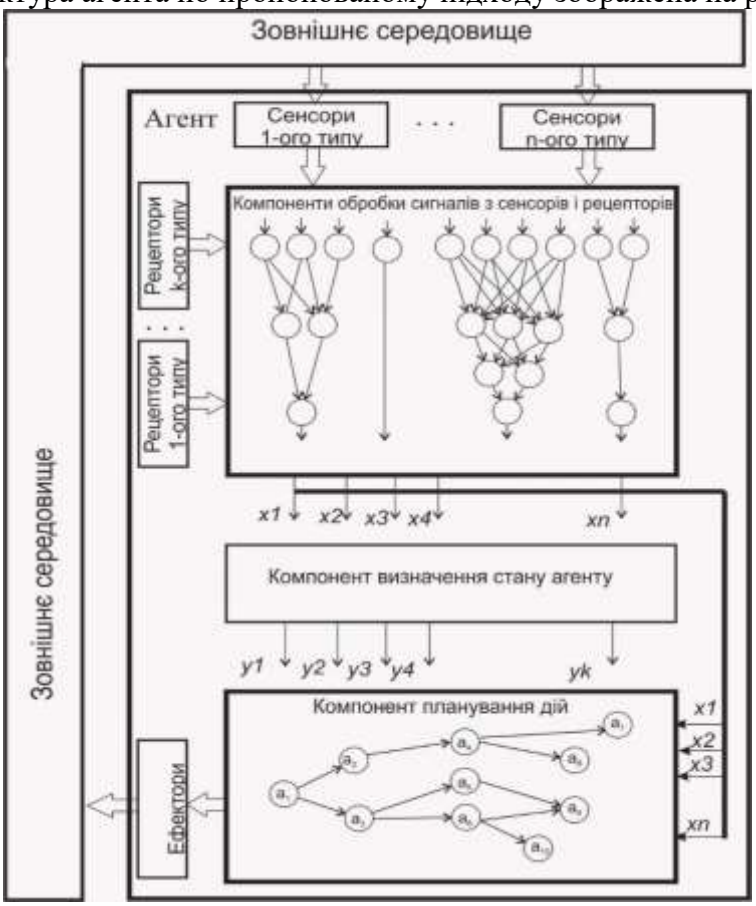


Рисунок 1 – Загальна структура агенту

Запропонуємо основні положення моделі представлення послідовності дій на базі представленого вище підходу

Інтелектуальний агент отримує з сенсорів і рецепторів ознаки початкової умови, по ній визначається ціль та формується послідовність дій. Елементами послідовності дій є елементарні дії $a_1,a_2,a_3,\ldots,a_n$ для використання агентом. Елементарна дія характеризується набором вхідних параметрів для функціонування $x_{11},x_{12},..,x_{1m}$.

Ознаки передумови q_i відповідають першій дії в послідовності, остання дія в послідовності прив'язана до ознаки цілі g_i.

Відповідно вищесказаному необхідно скомпонувати з елементарних дій їх стабільні послідовності, які б відповідали початковим умовам і приводили до деякої цілі.

Візьмемо в якості прикладу рухи деякого агента-робота, який переміщається по площині. Елементарними діями робота є поворот, рух вперед, назад. Параметрами дій можуть бути визначені швидкість руху, кут повороту та ін. Якщо в напрямку робота швидко переміщається великий об'єкт, то робот-агент має класифікувати ознаки великого об'єкту і швидкого руху в напрямку агента. Робот має перейти в загальний стан страху. На основі цього стану він повинен спочатку зупинитися, а потім розвернутися і максимально швидко рухатись від джерела небезпеки. Такі початкові умови мають генерувати негайну послідовність дій, яка з людської точки зору викликається такою емоцією, як страх. Ціль цієї послідовності дій є відсутність великого об'єкту в полі зору.

За аналогією з біологічними системами з множин впорядкованих елементарних дій складаються стандартні послідовності дій для рефлекторних реакцій на визначені початкові умови.

Модель представлення послідовності дій для навчання з підкріпленням:

$$L=(Q,G,X,W,A),$$

де $q_i \in Q$- ознаки початкового стану, $g_i \in G$ – ознаки цілі дій, $a_i \in A$ – елементарна дія, $x_{ij} \in X$ – вхідні параметри елементарних дій, $w_{ij} \in W$ – вага переходу від одної елементарної дії до іншої.

Представимо послідовність дій агенту направленим графом, де вершини визначають елементарні дії, а ребра визначають ступінь сили зв'язку між ними. Початкові умови q відповідають першій дії в послідовності, з неї розпочинається реалізація послідовності дій. Ознаки цілі g відповідають останній вершині в послідовності дій.

На рис. 2.3 показаний приклад графу послідовності дій.

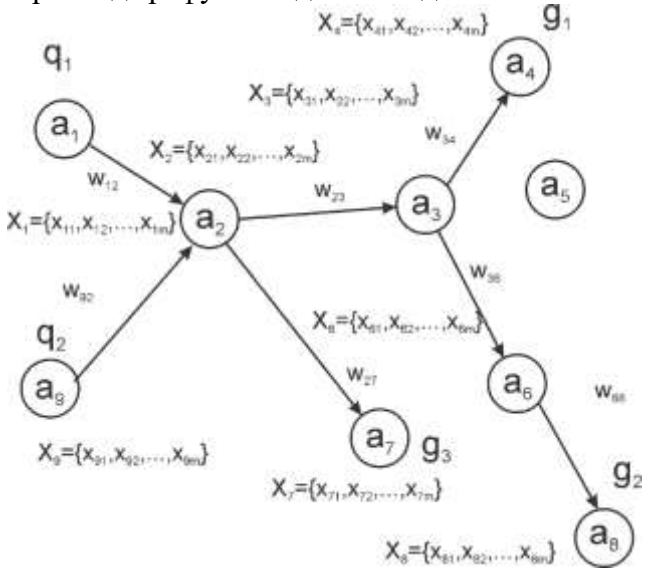


Рисунок 2 – Граф послідовності дій

З вершини в загальному випадку може бути декілька варіантів переходів до інших вершин, ваги всіх ребер, які виходять з однієї вершини в сумі повинні дорівнювати одиниці.

У випадку, коли вага ребра більше деякого порогового значення w_{thres_max}, то вибирається наступна елементарна дія, у яку входить це ребро.

У випадку, коли вага усіх ребер менше цього порогу w_{thres_max}, то агент аналізує поточний стан і реалізує перехід згідно ребер, які більше деякого порога w_{thres_min}.

Якщо існує такий шлях від ідентифікації ознак початкових умов до ознак цілі, в якому всі послідовні ребра мають вагу більше $w_{thres\_max,}$ то послідовність дій по цьому шляху виконується автоматично.

Агент початково налаштований на стандартні дії після ідентифікації початкових умов і отримання загального стану.

Ваги зв'язків змінюються при встановлені змінних загального стану, що дає змогу виконати послідовність дій в реальному масштабі часу з динамічним переналаштуванням і вибрати серед характерних для конкретного стану послідовностей дій.

Функція залежності ваги зв'язку від змінних загального стану має наступний вигляд:

$$w_{ij}=f(y_1,\ldots,y_n),$$

де $y_1,\ldots,y_n$ - значення змінних загального стану 1..n; $k_1,\ldots,k_n$ – коефіцієнти для позначення значення $y_1,\ldots,y_n$ для відповідного ребра, $0< k_i < 1$.

Для прикладу:

$$w_{ij}=k_1y_1+k_2y_2+\ldots+k_ny_n= \sum_{i=1}^{n} k_i \cdot y_i,$$

лінійний варіант функції залежності ваги зв'язку від змінних загального стану.

Відповідно кожній дузі ставиться у відповідність набір параметрів змінних загального стану $y_1,\ldots,y_n$ зі значення інтенсивностей станів(емоцій) 1..n; $k_1,\ldots,k_n$ – коефіцієнти для позначення важливості $y_1,\ldots,y_n$ для даного ребра

Модель розроблена для імітації виконання дій в біологічних організмах і коефіцієнти k_i у загальному можуть відповідати різним нейромедіаторам в синапсах між нейронами головного мозку і можуть змінюватись при навчанні. Успішне пройдення шляху від початкових умов до цілі по шляху впливає на ваги ребер цього шляху. Тобто змінюються коефіцієнти k вздовж шляху від початкової умови до цілі при успішному її досягненні.

Відповідно, метод формування послідовності дій виходить з уявлень про формування дій в біологічних організмів, а саме:

1. Існує множина станів агенту (емоційних) станів $y_1,\ldots.y_n$. Кожен стан може мати значення від 0 (повна відсутність) до 1 (найбільш виражений, який пригнічує всі інші емоційні стани).
2. Змінні, які характеризують емоційні стани, мають початкові значення, які характерні для агента.
3. Емоційні стани встановлюються на деякий наперед визначений час, по спливанні якого вони вертаються до початкового значення.
4. Існує початковий нормальний стан з деяким значенням в якому агент перебуває по замовчуванню.
5. Задається множина стандартних дій, які може виконувати агент $a_1,\ldots.a_n$.
6. Виконання кожної дії обумовлюється набором параметрів на вході дії $x_1,\ldots.x_n$.
7. Існує початкова множина значень сенсорних і рецепторних входів, які встановлюють визначені емоційні стани. Множина може збільшуватись при навчанні.
8. Для кожного стану агенту вище деякого порога існують прості стереотипні дії, які агент обов'язково виконує.
9. Ймовірність вибору дій для виконання може змінюватись в залежності від встановлених станів.
10. Стани успіху і невдачі встановлюються при співпадінні/неспівпадінні поточних значень сенсорних і рецепторних входів з ознаками цілі і використовуються для підкріплення послідовності дій.

Тобто, мета методу сформувати послідовність дій, яка ініціюється емоційними станом, і перевести в послідовність автоматичних дій на основі досягнення цілі і яка в майбутньому буде виконуватись в нормальному стані .

На рис. 3 показаний можливий граф дій робота-агенту, який рухається по площині, що обмежена стінами. Робот повинен навчитися уникати перешкоду (стіну) і повертати при цьому у відповідну сторону.

Робот має три ультразвукові сенсори, перший який визначає відстань до перешкоди по напрямку рухи і два інших, які визначають перешкоду праворуч або ліворуч під кутом 75 градусів. x_1 - параметр, який задає відстань до перешкоди по напрямку руху, x_2 – параметр на основі показників двох сенсорів, який приймає значення 0 або 1 в залежності де знаходиться перешкода, праворуч або ліворуч.

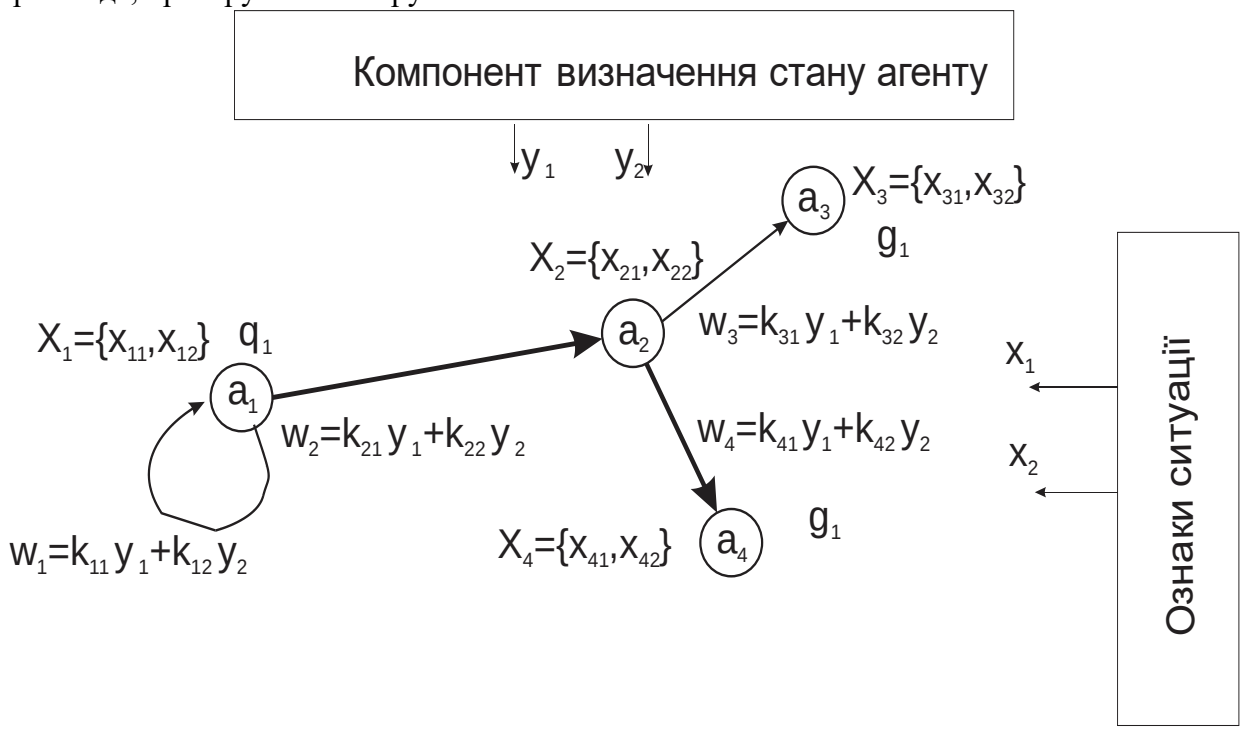


Рисунок 3 – Приклад графу моделі при виконання завдання уникання перешкоди

y_1– показник рівня нормального стану, впливає на рівень функціонування агенту при відсутності ідентифікованих емоційних станів

y_2 – показник рівня стану страху, росте при наближені агенту до перешкоди

q_1 – початкові умови, відстань до перешкоди менше порога

g_1– ціль дій, відсутність перешкоди по ходу руху агенту

k_1 – коефіцієнт рівня впливу нормального стану на дугу переходу

k_2 – коефіцієнт рівня впливу стану страху на дугу переходу

a_1- рух робота по прямій

a_2 – зупинка агенту

a_3 – поворот ліворуч 90°

a_4 – поворот праворуч 90°

x_1– відстань до перешкоди

x_2 – напрямок знаходження перешкоди

Δk – крок коректування коефіцієнтів k при навчанні

При наближені до агента до перешкоди на близьку відстань менше деякого порогу зростає рівень страху y_2. Це є і початковими умовами для планування дій, цілю яких є відсутність перешкоди по ходу руху агенту.

Спочатку вибирається стандартна дія при високому рівні страху - зупинка, потім інші дії з набору дій після виконання дій будується послідовність дій і перевіряється досягнення цілі. При досягнені цілі проводиться коректування коефіцієнтів по ланцюжку $k_1+\Delta k$, $k_2-\Delta k$, Δk –

коефіцієнт швидкості навчання. Тобто при частому успішному проходженні послідовності дій уникнення перешкоди буде викликатися не страхом, а нормальним станом. І виконуватись або в автоматичному режимі або з вибором в яку сторону доцільно повертати, щоб уникнути перешкоду, на основі аналізу x_1,x_2.

Для перевірки функціонування методу згідно задачі на рис. 3 на мові Lua написаний симулятор агенту в середовищі програми V-REP для моделі робота dr20. Програма V-REP забезпечує точну симуляцію робота і дає розробнику простий фреймворк, щоб практикуватися в створенні ПЗ для роботів.

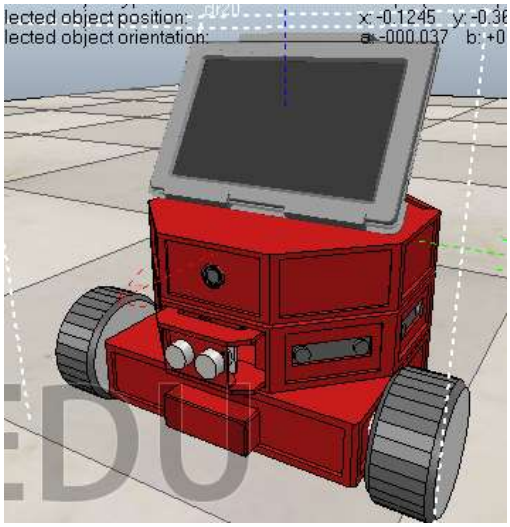


Рисунок 4 – Модель робота dr20 в середовищі V-REP

Початкове значення нормального стану вибрано рівним 0,6. Значення змінної страху для початку вибирається рівним 0. При досягненні успіху значення нормального стану зростає до 1, при невдачі зменшується до 0,2, його мінімального значення. Значення змінної стану страху збільшується до одиниці при зустрічі перешкоди. Стан страху падає з одиниці до нуля за виконання двох дій циклу моделювання.

Моделювання виконувалось на комп'ютері с процесором Intel Atom 570 с 2 Гігабайтами оперативної пам'яті з використанням операційної системи Linux Mint. Час навчання коливався від 5 до 10 хвилин з мінімумом при значенні Δk 0,07.

Висновки. В статті запропоновано підхід, де реалізація формування послідовностей дій інтелектуальних агентів виконується по аналогії з діяльністю біологічних організмів з використанням механізму емоцій для динамічного налаштування організму на виконання дій. Таким чином імітуються функції лімбічної системи в організації рухів на основі мотиваційної поведінки.

Послідовність дій агенту представляється орграфом, де вершини визначають елементарні дії, а ребра визначають ступінь сили зв'язку між ними. Початкові умови відповідають першій дії в послідовності, з неї розпочинається реалізація послідовності дій. Ознаки цілі відповідають останній вершині в послідовності дій

Метод формує послідовність дій, яка ініціюється емоційними станами, і переводить її в послідовність автоматичних дій на основі досягнення цілі і яка в майбутньому буде виконуватись в нормальному стані.

Для перевірки функціонування методу реалізований симулятор агенту-роботу в середовищі програми V-REP. Отримані результати можуть бути використані для інтелектуального планування на основі підкріплення можуть бути використані при керуванні агентами, роботами на виробничих підприємствах, військовими агентами, потоками міського руху, логістичними системами, соціальними явищами.

ЛІТЕРАТУРА:

1 Sandra Clara Gadanho. Reinforcement Learning in Autonomous Robots: An Empirical Investigation of the Role of Emotions. PhD thesis, University of Edinburgh, 1999.

2. Sandra Clara Gadanho and John Hallam. Emotion-triggered learning in autonomous robot control.Cybernetics and Systems — Special Issue: Grounding emotions in adaptive systems, 32(5):531–559, July 2001.

3. Sun R., Peterson T. Learning in Reactive Sequential Decision Tasks: the CLARION Model / Proc. 1996 IEEE ICNN, Washington, DC, USA. Plenary, Panel and Special Sessions Volume. – pp.70–75.

4. Карпов В. Э. Эмоции и темперамент роботов поведенческие аспекты / В. Э. Карпов // Известия ран. Теория и системы управления. – М.:, 2014, № 5, с. 166–185.

5. Кузьмин В. Использование нейронных сетей в алгоритме Q-learning / В. Кузьмин // Transport and Telecommunication. – Рига: Vol.4, N 1. С 75-86, 2003.

REFERENCES:

1 Sandra Clara Gadanho. Reinforcement Learning in Autonomous Robots: An Empirical Investigation of the Role of Emotions. PhD thesis, University of Edinburgh, 1999.

2. Sandra Clara Gadanho and John Hallam. Emotion-triggered learning in autonomous robot control.Cybernetics and Systems – Special Issue: Grounding emotions in adaptive systems, 32(5):531–559, July 2001a.

3. Sun R., Peterson T. Learning in Reactive Sequential Decision Tasks: the CLARION Model / Proc. 1996 IEEE ICNN, Washington, DC, USA. Plenary, Panel and Special Sessions Volume. – pp.70–75.

4. Karpov V. E. Emotsyy y temperament robotov povedencheskye aspekty / V. E. Karpov // Yzvestyia ran. Teoryia y systemы upravlenyia. – M.:, 2014, № 5, s. 166-185.

5. Kuzmyn V. Yspolzovanye neironnykh setei v alhorytme Q-learning / V. Kuzmyn // Transport and Telecommunication. – Ryha: Vol.4, N 1, pp. 75-86, 2003.

к.т.н., доц. Бойчук В.А., к.е.н., доц. Бойчук А.А., Бойчук М.В., Бурдюг О.В.

МЕТОД ФОРМИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ

В статье предложен подход, где реализация формирования последовательностей действий интеллектуальных агентов выполняется по аналогии с деятельностью биологических организмов с использованием механизма эмоций для динамической настройки организма на выполнение действий. Таким образом имитируются функции лимбической системы в организации движений на основе мотивационного поведения. При планировании в первую очередь определяется общее состояние агенту. Используя полученное состояние формируется последовательность действий. Такой подход даст возможность динамично перенастраивать последовательность и реагировать на опасную ситуацию или на изменение внутреннего состояния агента.

Интеллектуальный агент получает с сенсоров и рецепторов признаки начального условия по ней определяется цель и формируется последовательность действий. Элементами последовательности действий является элементарные действия. Элементарное действие характеризуется набором входных параметров для функционирования. Признаки предпосылки соответствуют первом действии в последовательности, последнее действие в последовательности привязана к признаку цели.

Последовательность действий агенту представляется орграф, где вершины определяют элементарные действия, а ребра определяют степень силы связи между ними. Начальные условия соответствуют первом действии в последовательности, с нее начинается реализация последовательности действий. Признаки цели соответствуют последней вершине в последовательности действий. Весы связей меняются при установке переменных общего состояния, что позволяет выполнить последовательность действий в реальном масштабе времени с динамическим перенастройкой и выбрать среди характерных для конкретного состояния последовательностей действий.

Метод формирует последовательность действий, которая инициируется эмоциональными состояниями и переводит ее в последовательность автоматических действий на основе достижения цели и которая в будущем будет выполняться в нормальном состоянии. Для

проверки функционирования метода реализован симулятор агенту-работу в среде программы V-REP. Полученные результаты могут быть для интеллектуального планирования на основе подкрепления могут быть использованы при управлении агентами, работами на производственных предприятиях, военными агентами, потоками городского движения, логистическими системами, социальными явлениями.

Ключевые слова: интеллектуальный агент, планирование, модель, Q-обучения, эмоциональные состояния, обучение с подкреплением.

Ph.D. Boychuk V.O., Ph.D. Boychuk A.A., Boychuk M.V. Burdyug O.V.

THE ACTION SEQUENCE FORMING METHOD FOR INTELLECTUAL AGENTS

The article proposes an approach where the implementation of the formation of sequences of actions of intelligent agents is carried out by analogy with the activities of biological organisms using the mechanism of emotions to dynamically tune the body to perform actions. Thus, the functions of the limbic system are simulated in the organization of movements based on motivational behavior. When planning, first of all, the general condition of the agent is determined. Using the resulting state, a sequence of actions is formed. This approach will make it possible to dynamically reconfigure the sequence and respond to a dangerous situation or to a change in the internal state of the agent.

An intelligent agent receives from the sensors and receptors signs of an initial condition, the goal is determined by it, and a sequence of actions is formed. Elements of a sequence of actions are elementary actions. An elementary action is characterized by a set of input parameters for functioning. Signs of the premise correspond to the first action in the sequence, the last action in the sequence is tied to the sign of the goal.

The sequence of actions of the agent is represented by a digraph, where the vertices determine the elementary actions, and the edges determine the degree of bond strength between them. The initial conditions correspond to the first action in the sequence, the implementation of the sequence of actions begins with it. Signs of the goal correspond to the last peak in the sequence of actions

Link weights change when general state variables are set, which allows you to perform a sequence of actions in real time with dynamic reconfiguration and select sequences of actions that are characteristic of a particular state. The method forms a sequence of actions that is initiated by emotional states and translates it into a sequence of automatic actions based on the achievement of the goal and which in the future will be performed in a normal state.

To test the functioning of the method, a agent-work simulator is implemented in the V-REP program environment. The results obtained can be used for intelligent planning based on reinforcements and can be used in the management of agents, work in manufacturing enterprises, military agents, urban traffic flows, logistics systems, and social phenomena.

Keywords: intellectual agent, planning, model, Q-learning, emotional states, reinforced learning.

УДК 004.413.4

д.т.н., проф. **Даник Ю.Г.** (НУОУ)
Вдовенко С.Г. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-08

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ ДЕРЖАВИ

Зростання ролі і значення вирішення завдань кібербезпеки та кібероборони обумовлено інноваційним розвитком інформаційних, електронних та кібер- технологій, які стали рушієм ряду тенденцій у воєнній справі. Внаслідок формування та визнання штучного п'ятого простору – кіберпростору, окремою сферою боротьби між державами, включаючи збройне протиборство, питання кібербезпеки та кібероборони стали актуальними в забезпеченні національної безпеки і оборони розвинених держав, котрі особливу увагу приділяють формуванню та розвитку систем кібербезпеки та кібероборони, як головного фактору у досягненні воєнно-стратегічної переваги в забезпеченні національної безпеки і оборони в сучасних та перспективних умовах.

У статті здійснено аналіз загальних принципів побудови систем кібербезпеки і кібероборони провідних країн світу в контексті можливості та доцільності впровадження їх досвіду в Україні; аналіз передумов, існуючого стану та проблемних питань формування систем кібербезпеки та кібероборони в Україні. Зокрема, такими є: відсутність основних теоретичних та прикладних положень формування системи кібероборони; відсутність національного органу військового управління у сфері кібероборони; розпорошеність зусиль різних військово-організаційних структур щодо вирішення завдань кібербезпеки та відсутність сформульованих задач кібероборони.

Запропоновано найбільш раціональний варіант створення систем і структур кібербезпеки та кібероборони України з підсистемами освіти та науки, якій відповідно до сучасних тенденцій розвитку, з урахуванням військово-політичної обстановки, національних інтересів та законодавства, забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "смарт-оборони".

Ключові слова: кібербезпека, кібероборона, кіберпростір, система кібербезпеки, система кібероборони, кіберосвіта, кібератака, кібервплив, кіберзагроза, кібердія, кіберзахист, кібероперація, кіберрозвідка, кіберудар, суб'єкти кібербезпеки, суб'єкти кібероборони, об'єкти критичної інфраструктури.

Вступ та постановка проблеми. Стрімкий розвиток та масове впровадження досягнень електроніки, сучасних інформаційних та кібер- технологій призвело до формування нового спектру ризиків і загроз у сфері національної безпеки і оборони держави, які реалізуються у кіберпросторі та (або) через кіберпростір. Відбувається експоненціальне зростання інформатизації та автоматизації всіх сфер людської діяльності, кількості інформації що зберігається, обробляється і передається, швидкості її передачі і обробки, ускладнення систем управління взаємодії між ними та зв'язків між процесами управління. Кіберзагрози охоплюють всі базові сфери суспільної діяльності (політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, технологічну тощо), деструктивно впливаючи на національну безпеку в цілому.

В сучасному світі питання кібербезпеки та кібероборони стали наріжними і найбільш проблемними та актуальними в забезпеченні національної безпеки і оборони практично всіх розвинених держав. На саміті НАТО в Варшаві (7-9.07.2016) на Кібер конференції з інформаційного забезпечення НАТО (NIAS) (6.12.2016), на конференції "Кібернетична оборона" (Париж, 15.05.2018), на засіданні Північноатлантичної ради (Брюссель 11-12.07.2018) та на саміті у Лондоні у листопаді 2019 року присвяченому 70-річчю створення альянсу НАТО було зосереджено увагу на важливості своєчасного виявлення, запобігання, нейтралізації і ліквідації загроз в кіберпросторі [1,2,3].

Зазначені проблеми в Україні і світі розглядаються перш за все на рівні термінологічного визначення [4-8], аналізу окремих питань кібербезпеки, здебільшого з точки зору

кіберзлочинності та кібертероризму і в деякій мірі на рівні аналізу особливостей впровадження систем кібербезпеки [9-20]. Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної та кібербезпеки, окремі засади протидії кіберзлочинності та боротьби з кібертероризмом, а також загальної теорії кібербезпеки досліджували О.Баранов, В.Бурячок, Ю.Грицюк, Р.Грищук, Ю.Даник, Д.Дубов, Р.Лук'янчук, С.Мельник, В.Шеломенцев, М.Яцишин та інші. Але, проблема створення системи кібероборони та особливостей її трансформації в умовах стрімкого розвитку науки, техніки та технологій системно і цілісно до цього часу не розглядалися, узагальнений аналіз особливостей формування та трансформації систем кібербезпеки і кібероборони під впливом різноманітних чинників та залежності їх ефективності від складу, організації, структурної побудови і систем управління ними у безпосередньому взаємозв'язку із нормативно-правовим, організаційним, науковим та кадровим забезпеченням у контексті визначення їх мети, завдань, функцій і шляхів досягнення необхідних спроможностей не проводився. Проблеми кібероборони, з точки зору воєнно-політичного та воєнно-стратегічного аналізу розглядаються здебільш іноземними фахівцями, публікуються в офіційних виданнях самітів НАТО, але не мають юридичної сили альянсу та є лише поглядами фахівців [21- 23].

Мета цієї роботи полягає в проведенні аналізу і узагальненні відомих результатів та дослідженні загальної методології та практики формування і розвитку систем кібербезпеки і кібероборони провідних країн світу та, виходячи з цього, розробці найбільш раціонального варіанту вирішення цієї задачі в Україні.

Викладення основних основного матеріалу дослідження. Питання та передумови виникнення напрямів кібербезпеки та кібероборони в тому чи іншому контексті пов'язані із появою та розвитком радіотехніки і радіоелектроніки, електронної техніки і технічних засобів шифрування та криптоаналізу, обчислювальної техніки і інформатики, науки кібернетики та впровадженням систем управління в усіх галузях і сферах людської діяльності, теорії зв'язку та інформації і стрімким розвитком інформаційних, кібернетичних та інформаційно-комунікаційних систем.

На цей час загальновизнано, що в результаті високотехнологічної та інформаційної діяльності людства додатково до природних: суходільного, морського повітряного та космічного, фактично сформувався штучний п'ятий простір – кіберпростір, який перетворився на окрему сферу боротьби між державами, включаючи збройне протиборство [1,24]. Перше офіційне визначення кіберпростору було дано військовими експертами США в настанові КНШ 2006 року "Інформаційні операції": "Кіберпростір – сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення і обміну інформацією, і пов'язана з ними інформаційна інфраструктура ЗС США". За поглядами провідних фахівців з кібербезпеки, кіберпростір визначається скоріше соціальними взаємодіями, а не його технічною реалізацією [11]. На їхню думку, обчислювальне середовище в кіберпросторі є доповненням каналу зв'язку між реальними людьми. Уряди провідних країн світу відносять взаємопов'язані інформаційні технології і взаємозалежну мережу інфраструктур інформаційних технологій кіберпростору до національної критичної інфраструктури.

Трансформація поглядів на питання кібербезпеки і кібероборони та, відповідно, розвиток їх структур в провідних країнах світу відбувається під впливом розвитку технологій, змін у безпековому середовищі, формах, способах та технологіях ведення війн і нових досягнень в цьому які очікуються.

На цей час в світі існує біля 40 ключових макротехнологій, які за думкою провідних експертів визначають рівень економіки та обороноздатності країн в сучасних умовах.

До високих технологій та технологій подвійного призначення (high technology, hi-tech - англ.) частіше за все відносять такі технології: штучний інтелект, космічні, робототехнічні, інформаційні та кібер- технології; нано-, квантові, нейронні, біотехнології, генну інженерію, інноваційні електромеханіку, електроніку, матеріалознавство, створення

нових напівпровідникових матеріалів, генерування, акумулювання та передача енергії, “чисті” (cleantech) та енергозберігаючі технології, телекомунікаційні, інфокомунікаційні технології та технології управління і автоматизації.

В цих сферах прогнозуються проривні досягнення перш за все у штучному інтелекті, хмарних технологіях, інтернеті речей, продуктивності та природі обчислювальних засобів, можливостях зберігання обробки та передачі великих масивів даних та інформації (Big Data), засобах і технологіях їх реалізації на кардинально нових принципах. Можливості і вразливості практично всіх сучасних інфокомунікаційних та кібернетичних систем все більше залежать, крім того, від зростання взаємозв’язків різноманітних інформаційних систем та систем управління між собою в багатопараметричному та багатовимірному кіберпросторі та їх інформаційно-кібернетичного взаємопроникнення, взаємодії і взаємозалежності тощо.

Проблемні питання і особливості створення та розвитку систем кібероборони.

Державне та військове керівництво армій розвинених країн світу у відповідності до нових підходів щодо будівництва збройних сил особливу увагу приділяє формуванню та розвитку систем кібербезпеки та кібероборони, як головного фактору у досягненні воєнно-стратегічної переваги в забезпеченні національної безпеки і оборони в сучасних та перспективних умовах. Об’єктивність такого підходу обумовлена тим, що світ наразі перебуває на порозі нового стрибка технологій. У сфері оборони відбувається глобальний перехід на інтегровані системи управління військами та зброєю від стратегічного до тактичного рівня, та інноваційних систем озброєння, які до 80% побудовані з високотехнологічних складових.

Зростання ролі і значення вирішення завдань кібербезпеки та кібероборони також обумовлено інноваційним розвитком інформаційних, електронних та кібер- технологій, які стали рушієм ряду тенденцій у воєнній справі, зокрема таких, як:

1. глобальна інформатизація та початок роботизації військових формувань і створення високо інтегрованих систем управління, які, в свою чергу, стають об'єктами кібервпливу і вимагають розвитку форм і способів ведення кібер- протиборства;

2. зростання інтенсивності конфліктів в інформаційному та кіберпросторі, за участі спеціально створених для цього спеціалізованих структур та формувань. Ведення терористичних дій через інформаційний та кібер- простори та безпосередньо в них;

3. домінування більш розвинутих країн у веденні деструктивних дій саме через інформаційний та кібер- простори з одного боку, та з іншого - зростання уразливості держав при зростанні рівня їх високотехнологічного розвитку;

4. використання світових інформаційних мереж та електронних засобів масової інформації для маніпулювання свідомістю та досягнення когнітивних трансформацій як окремих спільнот і населення окремих країн так і світової громади;

5. виділення інформаційного та інформаційно-аналітичного забезпечення в самостійний вид забезпечення військ (сил) і формування відповідних структур для його здійснення;

6. постійне зростання кількості та можливостей комп’ютерних та електронних засобів, що задіяні в зберіганні, обміні і обробці інформації і під час прийняття управлінських рішень у тому числі на всіх етапах планування операцій та у ході бойових дій. Зростання ролі імітаційного моделювання при плануванні операцій і в процесі ведення бойових дій. Подальша інтеграція засобів штучного інтелекту в системи воєнного призначення;

7. інтеграція на основі продуктів високих технологій систем розвідки, управління та ураження від підрозділу (одиниці бойової техніки) до командування всіх ланок управління. Мініатюризація комп’ютерних та електронних засобів, їх використання практично у всі зразках озброєння та бойової техніки (від високоточної зброї до особистої зброї та спорядження).

Аналіз теорії, практики й досвіду побудови систем і забезпечення кібербезпеки та кібероборони провідних держав світу свідчить, що основною тенденцією при їх формуванні стало поєднання в єдиній структурі, яка відповідає за кібероборону, відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері, різних

напрямів діяльності (та відповідно, підрозділів, які її здійснюють) поєднаних їх відношенням до кіберпростору. Визначним чином на ці процеси вплинуло безпосередньо особливості формування та постійні розвиток і трансформація кіберпростору.

У провідних країнах світу при формуванні систем кібербезпеки та кібероборони основною тенденцією стало створення нового виду Збройних Сил – Кіберсил (Кібервійськ) з відповідними кіберкомандуваннями, шляхом об'єднання в єдиній структурі, що відповідає за кібероборону, органів військового управління, сил і засобів, які мають відношення до кіберпростору, з реформуванням, перерозподілом функцій, та перепідпорядкуванням військових частин, зі зміною, за необхідності, напрямків їх діяльності, корегування наукової та освітньої діяльності наукових центрів та закладів освіти, включно утворення нових структурних підрозділів, закладів освіти, військових частин та підрозділів різних напрямів діяльності для виконання спільних заходів кіберрозвідки, кіберзахисту, активних дій в кіберпросторі, відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері (таблиця 1).

Аналіз викладеного (таблиця 1) свідчить, що до складу Кіберсил (кібервійськ), як правило входять підрозділи радіоелектронної розвідки (РЕР), радіоелектронної боротьби (РЕБ), інформаційно-психологічних операцій (ІПсО), зв'язку та інформаційних систем, захисту інформації в ІТС, криптографічного забезпечення та криптологічної підтримки, геоінформаційного забезпечення тощо. Створені в провідних країнах світу системи кібероборони включають та об'єднують структури, які: відповідають за дії в комп'ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, організацію та застосування технічних видів розвідки, забезпечують зв'язок та криптографічний захист інформації, проваджують діяльність у сфері технічних розвідок та здійснюють криптоаналіз, приймають участь у заходах введення в оману, здійснюють наукові дослідження в цих сферах та підготовку кадрів.

Наукове, науково-технічне, освітньо-тренувальне супроводження утворення Кіберсил здійснюється, як правило, багатофункціональними профільними військовими закладами. Держзамовлення на підготовку фахівців, включно науково-педагогічних працівників – збільшується. При відсутності профільних ВНЗ – вони утворюються. В провідних країнах світу (Великобританія, ФРН, Польща) ефективність вирішення зазначених проблем досягається шляхом формування та забезпечення функціонування інтегрованих навчально-наукових, дослідно-випробувальних університетів, які здійснюють на єдиній базі освітню і наукову діяльність за високотехнологічними напрямами. Наприклад, така інтеграція військової освіти і науки за високотехнологічними напрямами успішно реалізована у Військовому університеті технологій (Польща), де на одній базі зосереджені всі високотехнологічні напрями, спеціальності і спеціалізації підготовки військових фахівців (факультети: національної безпеки, електроніки та телекомунікацій, енергетики, технічної фізики, геодезії і картографії, інформатики, інженерії безпеки, інженерії матеріалів, криптології і кібербезпеки, авіації і космонавтики, механіки і машинобудування, мехатроніки, управління тощо) та наукових досліджень.

Законами України та іншими нормативно-правовими актами не визначено перелік вичерпних заходів щодо підготовки до відбиття та відбиття воєнної агресії у кіберпросторі. На думку авторів, завдання кібербезпеки та кібероборони в цілому можуть розглядатися в межах трьох три основних підсистем: кіберрозвідки, кіберзахисту, кібервпливу (активних дій). Питання забезпечення кібербезпеки можуть умовно розглядатися за:

напрямками – захист громадянина і суспільства, захист держави;

об'єктами кібервпливу – соціальні, технічні, соціотехнічні системи (рис. 1);

рівнями – державний (стратегічний), регіональний (оперативний), місцевий (тактичний);

завданнями – запобігання, стримування, протидії;

сферами – економіка (виробничий та невиробничий сектори, критична інфраструктура держави), сфери зовнішньої та внутрішньої політики, державного управління, освіта, наука, безпека і оборона (рис.2);

Зведені дані щодо кіберсил окремих держав світу. Таблиця 1

Показники (індикатори)	США	ФРН	Велика Британія	Франція	Польща	Угорщина	Ізраїль	РФ	Україна
Наявність національної Стратегії (доктрини) КО (КЗ). Рік видання діючої.	2018	2016	2018	2018	2018	2018	2015	2015	2016
Складові частини (функціональні елементи) Кіберсил	РЕР, РЕБ ІПсО зв'язок та ІС, крипто,	РЕР, РЕБ ІПсО зв'язок та ІС, крипто, гео-інформ забезп	РЕР РЕБ ІПсО зв'язок та ІС крипто	РЕР РЕБ ІПсО зв'язок та ІС, крипто	РЕБ, зв'язок та ІС, крипто	РЕБ, зв'язок та ІС, крипто	РЕР, РЕБ ІПсО зв'язок та ІС, крипто	ІПсО	-
Наявність сил КО, як окремого виду ЗС	+	+	+	+	+	+	+	+	-
Чисельність, тис/ % від чисельності ЗС	50/ 2,5%	13,5/ 6%	2/ 1,5%	4/ 1,5%	1/ 1%	1/ 0,4%	> 3/ 5,5%	1/ 0,1%	-
Наявність органу управління КО (кіберкомандування)	+	+	+	+	+	+	+	+	-
Роки формування,	2009-2019	2017-2021	2017-2021	2015-2019	2018-2021	2019-2022	2018-2021	2016 - …	-
Рік набуття спроможностей	2018	2021	2021	2018	2021	2020	2021	2015	?
Спосіб формування: на базі існуючих + нова структура -	+	+	+	+	+	+	+	-	-
Наявність системи наукової підтримки, освіти та підготовки системи КО (цив.*)	7	1	15*	2	2	1	3*	3	4 (неузгодж)

складовими частинами – кіберзахист (боротьба з кіберзлочинністю, кібершпигунством, кібертероризмом), кібероборона (дії в ІТ-мережах та програмно-комп'ютерні, дії в електромагнітному спектрі випромінювання, дії в соціокіберпросторі, кіберпросторі та через кіберпростір: інформаційні, психологічні, когнітивні) (рис. 3);

формами і способами кіберзахисту та активних кібердій (рис. 4);

суб'єктами, що здійснюють кіберзахист та кібероборону.

Процеси побудови, розвитку, та набуття спроможностей щодо бойового застосування систем кібероборони провідних країн світу супроводжувалися виявленням та вирішенням ряду проблем, основними з яких були:

протиріччя у відповідності теорії та практики забезпечення кібербезпеки та кібероборони в умовах формування та інтенсивного розвитку засад, форм, способів, засобів і технологій інформаційних та кібердій;

відсутність або недосконаліть дефініційно-термінологічного апарату, концепцій та стратегій створення і застосування кіберсил;

недостатня кількість або відсутність підготовлених кадрів, систем їх підготовки, науково-технічного супроводження;

відсутність або нераціональне вирішення питань державно-приватного партнерства;

відсутність необхідних та/або невідповідність практичній необхідності законів та нормативно-правових актів;

невідповідність визначеним завданням організаційно-штатних структур органів військового управління, підрозділів, які з інших видів збройних сил включалися до складу кіберкомандувань; невідповідність практичній потребі наявної штатної техніки та обладнання підрозділів кіберсил.

Рисунок 1 – Об'єкти кібервпливу

Разом з тим, формування систем кібербезпеки та кібероборони провідних країн світу відбуваються спираючись на загальні принципи, позитивні риси яких можуть та повинні бути використані при побудові системи кібероборони України, основні з них:

інтегрованість системи кібероборони в багаторівневу систему кібербезпеки держави (коаліції);

безперервність функціонування системи кібероборони;

відповідність рівня всебічного забезпечення кіберсил потребам оборони;

оптимальність (раціональність) побудови сил кібероборони;

керованість з єдиного координуючого органу з питань забезпечення кібербезпеки;

науково обґрунтовані законодавче, нормативно-правове, дефініційно-термінологічне супроводження;

державно-приватне та міжнародне партнерство;

узгодженість та взаємодія різних відомств у сфері забезпечення кібероборони держави;

інтегрованість закладів освіти до високотехнологічних навчально-наукових, дослідно-випробувальних комплексів, уніфікованість вимог щодо підготовки військового й цивільного персоналу кібербезпеки;

однозначність критеріїв (індикаторів) загроз у сфері кібероборони держави, рівня готовності систем КБ та КО, тощо.

Аналіз стану кібероборони в Україні. Оборона України, захист її суверенітету, територіальної цілісності і недоторканності, охорона повітряного та підводного простору держави покладаються на ЗС України [25-27]. З ухваленням у жовтні 2017 року Закону [28] на Міністерство оборони та Генеральний штаб Збройних Сил України покладено нове завдання щодо впровадження заходів із забезпечення кібероборони.

Законодавством також визначається обов'язковість здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі, кібероборони для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії, забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану, у тому числі – шляхом проведення спеціальних операцій (розвідувальних, інформаційних, психологічних, інформаційно-психологічних тощо) у кіберпросторі при підготовці до захисту та захисту України в разі збройної агресії. Розвідувальним органам України визначені завдання із здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки. Значна увага приділяється військовій співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз [26-29].

Разом з тим, Законами України, або іншими нормативно-правовими актами не визначені:

кіберпростір, як середовище ведення оборонних дій для забезпечення захисту суверенітету держави;

перелік кіберзагроз державі в оборонній сфері;

перелік вичерпних заходів із підготовки до відбиття та відбиття воєнної агресії у кіберпросторі;

механізм координації діяльності суб'єктів кіберзахисту України при реалізації завдань щодо оборони України в кіберпросторі.

Пропозиції та рекомендації. Кібероборона – окрема, особлива, специфічна складова кібербезпеки держави, що має різнопланові повсякденні, поточні та бойові (спеціальні) завдання і функції. Тому, необхідно створювати єдину систему кібероборони під єдиним командуванням, всі складові якої діють узгоджено за єдиним замислом і планом. Відсутність зв'язків між розрізненими елементами знижує ефективність їх застосування. Натомість їх наявність – додає нові спроможності щодо ураження противника, ступінь якого може бути багатократно збільшена за рахунок ланцюгових ефектів кібердій [30].

Виходячи з викладеного, пропонується базис системи кібердій в інтересах кібероборони держави будувати на трьох основних поєднаних у єдине ціле складових підсистемах: кіберрозвідки, кіберзахисту, кібервпливу (рис. 3).

Для забезпечення створення та функціонування цілісної системи кіберорборони (СКО) з урахуванням національних вимог [24-29, 31] та рекомендацій експертів НАТО та країн-партнерів щодо уніфікації бойових командувань і процедур [1,23,31-33] необхідно здійснити низку взаємопов'язаних політичних, правових, організаційних, науково-технічних, безпосередньо військових та інших заходів.

Законами України та Стратегією воєнної безпеки України мають бути визначені нові функції і завдання МО України та ЗС України в СКО та відповідному кіберкомандуванню, зокрема такі як:

Рисунок 2 – Сфери економіки що підлягають кібероборони

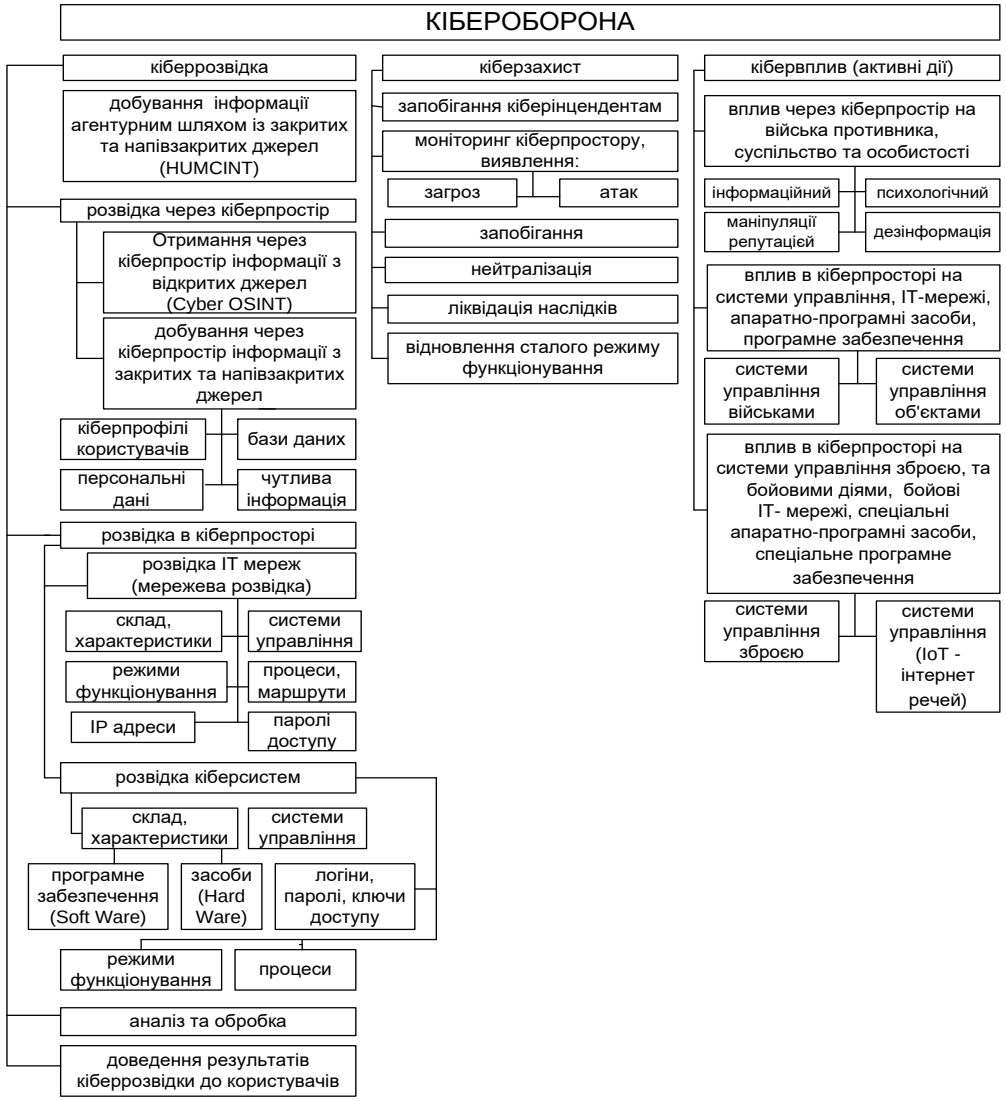


Рисунок 3 – Складові частини та завдання кібероборони

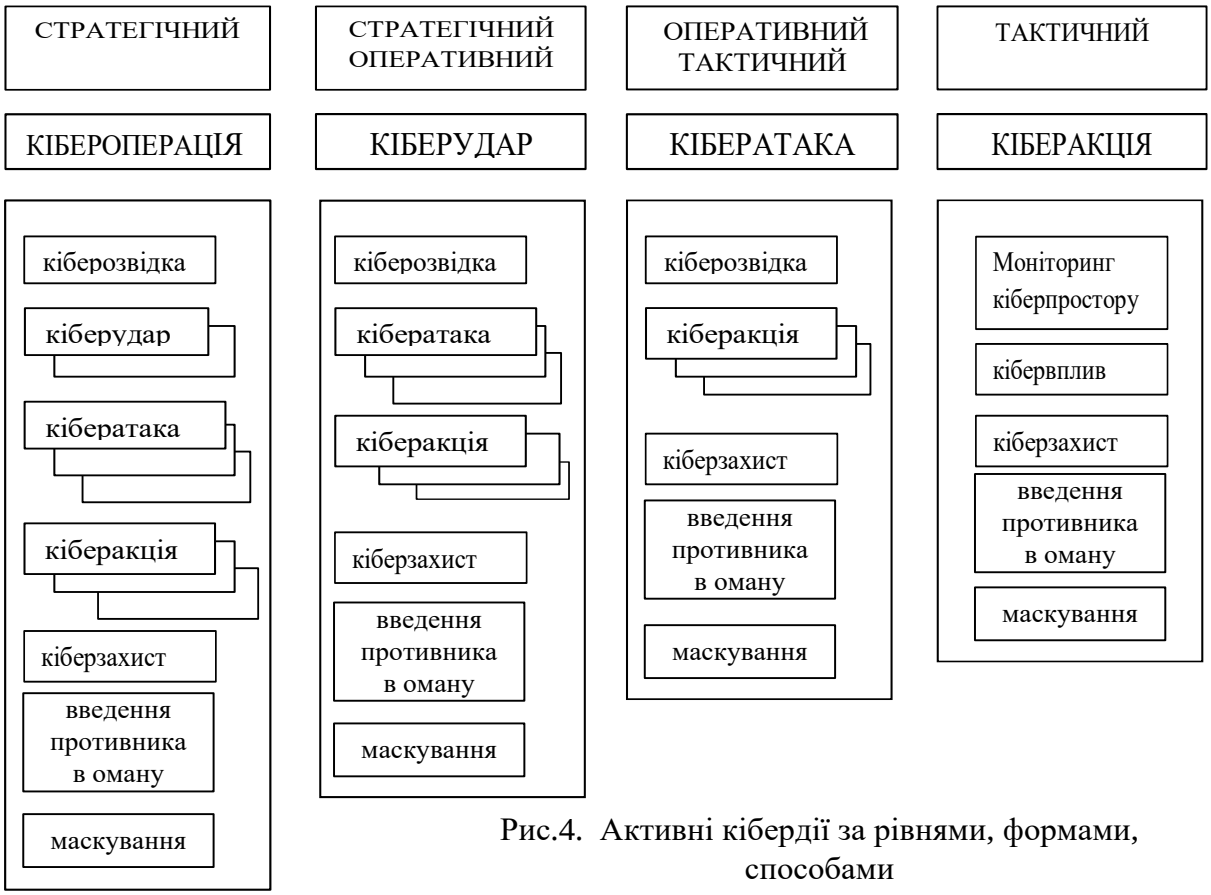


Рис.4. Активні кібердії за рівнями, формами, способами

розробка та реалізація засад державної політики у сфері кібероборони, визначення завдань, функцій та критеріїв військово-політичної, військової, військово-технічної, науково-технічної та розвідувальної діяльності суб'єктів кібероборони з питань планування кібероборони та дій у кіберпросторі і через кіберпростір на стратегічному рівні відповідно до Плану оборони держави;

участь в підготовці об'єктів критичної інформаційної інфраструктури держави щодо протидії кіберзагрозам та сталому їх функціонуванню в особливий період та в умовах воєнного стану;

розробка засад застосування ЗС України, інших військових та спеціальних формувань для виконання завдань кібероборони, включно питання асиметричних кібердій спрямованих на примушення противника до відмови або припинення воєнних (бойових) дій, кібердій під час підготовки і проведення спільних оборонних, наступальних, контр-наступальних операцій сил оборони, спеціальних операцій, коаліційних операцій, територіальної оборони, дій руху опору, ліквідації наслідків надзвичайних ситуацій, спричинених застосуванням зброї, та при захисті населення і територій від наслідків ведення воєнних дій;

формування стандартів підготовки та держзамовлення на підготовку фахівців з кібербезпеки та кіберобоони, розробка програм та планів оперативної і спеціальної підготовки, бойових статутів, стандартів і настанов ЗС України з питань кібероборони;

планування, організація та здійснення заходів з нейтралізації та активної протидії кіберзагрозам національним інтересам України у сфері оборони;

планування, координації дій, організації взаємодії та проведення заходів щодо підготовки держави до кібероборони зі структурними підрозділами інших центральних органів виконавчої влади та з міжнародними партнерами, узгоджене управління суб'єктами кібероборони.

втілення найсучасніших інформаційних технологій у сфері оборони, забезпечення розвитку і безпеки власної інформаційної та управлінської інфраструктури та ресурсів, захист їх від кіберзагроз.

Зазначене вимагає формування такої системи кібербезпеки та кібероборони, яка забезпечить скоординоване управління всіма її складовими. Така система потребує наявності відповідного єдиного органу управління, подібного за структурою, завданнями і функціями до аналогічних органів управління в цій сфері країн-членів НАТО, призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони України та Збройних Сил України в інформаційному та кіберпросторі; організації та координації заходів щодо кібербезпеки та захисту критичної інформаційної інфраструктури держави; управління силами кібербезпеки та кібероборони під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану.

Цей орган управління відповідальний за організацію та здійснення заходів щодо забезпечення інформаційної та кібербезпеки в сфері оборони і кібероборони, має складатися зі структурних підрозділів, які умовно можна визначити виходячи з функціональних завдань, а саме: моніторингу кіберпростору, захисту кіберпростору, активних дій у кіберпросторі, та вирішувати такі основні задачі:

участь у формуванні та реалізації державної політики з питань інформаційної, кібер-безпеки та кібероборони;

формування та реалізація політики Міністерства оборони України та Збройних Сил України щодо дій у кіберпросторі;

участь у виконанні заходів зі створення та розвитку інформаційних систем та ресурсів у Збройних Силах України;

координації дій суб'єктів інформаційної, кібер- безпеки та кібероборони Міністерства оборони та Збройних Сил України;

участь у формуванні стандартів підготовки та держзамовлення на підготовку фахівців з інформаційної, кібер- безпеки та кібероборони;

організації взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади, в рамках державно-приватного партнерства та міжнародними партнерами з питань кібербезпеки і кібероборони;

підтримання взаємодії з системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом. Контроль та координація їх дій;

моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у кіберпросторі та ефективності дій системи кібербезпеки, виявлення уразливостей в інформаційних та кібер системах своїх і противника;

планування, організацію та координацію розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в кіберпросторі (Cyberspace Operation) через кіберпростір та кібероперацій (Cyber Operation);

організацію та координацію інформаційних дій у кіберпросторі (включаючи соціальні мережі).

Наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "смарт-оборони", ключовими елементами якої є високотехнологічна підготовка персоналу та збалансоване поєднання найбільш ефективних аспектів стратегій "жорсткої сили" та "м'якої сили", шляхом зваженого і узгодженого використання інструментарію стратегічних комунікацій, санкцій, переконання і застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність.

Висновки. На підставі аналізу еволюції напрямків кібербезпеки та кібероборони, тенденцій розвитку науки і техніки запропоновано найбільш раціональний варіант створення систем і структур кібербезпеки та кібероборони зі структурами освіти та науки, які б відповідали зазначеним тенденціям розвитку, з урахуванням реальних військово-політичної обстановки, національних інтересів та законодавства.

В Україні питання формування системи кібероборони знаходиться у стадії вирішення. Відповідно до чинного законодавства підготовка держави до відбиття агресії у кіберпросторі (кібероборона) є одним із головних завдань, які покладаються на Міністерство оборони та Збройні Сили України. За виконання пов'язаних за змістом та простором завдань кібероборони на цей час відповідають різноманітні, структурні підрозділи різного підпорядкування, що призводить до зниження ефективності виконання цих задач.

Спираючись на вищеперераховані принципи, для створення і розвитку системи кібероборони України доцільно:

1. Утворення та розгортання системи кібероборони держави здійснити шляхом комплексного та докорінного реформування сектору безпеки та оборони з оптимальним перерозподілом функцій, завдань, сил і засобів, ресурсів, та позбавлення від невластивих задач і функцій. Використовуючи при цьому дані аналізу результатів аудиту нормативно-правового забезпечення, ефективності виконання визначених нормативно-правовими актами функцій з використанням досвіду, найкращих підходів, технологій, методик та моделей апробованих в інших держав та тих, які довели свою ефективність та раціональність**.** Відповідно до [2, 30, 32, 33- 35] використовуючи досвід інших держав, досягти оперативних та інших спроможностей щодо удосконалення систем інформаційної і кібербезпеки, кібероборони та кіберзахисту власної інформаційної інфраструктури, забезпечення безпеки кіберпростору і соціокіберпростору та спільного захисту від кіберзагроз визначають співпрацю з НАТО, ЄС, гармонізацію з ними законодавства у цій сфері. Для України більш доцільною та ефективною, одночасно менш затратною, могла б бути німецька модель утворення Кіберсил, як самостійного виду Збройних Сил, включно систему наукового супроводження та підготовки кадрів. З точки зору бойового застосування кіберсил, більш ефективною могла б бути американська модель.

2. Здійснити заходи реформування, удосконалення і розвитку системи військової освіти і науки, зокрема в частині, що стосується розвитку системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки та кібероборони. Система кіберосвіти має забезпечити утворення, розгортання та ефективне функціонування системи кібероборони держави та включати: завчасне формування вимог професійних стандартів до фахівців кібероборони; визначення держзамовника та прогнозованих кількісних показників держзамовлення; формування (реформування) військових науково-навчальних закладів в інтегрований освітньо-науковий, дослідно-випробувальний міжвидовий та міжвідомчий військовий заклад вищої освіти – військовий університет технологій, який забезпечить здійснення на єдиній базі освітньої і наукової діяльності за високотехнологічними напрямами; забезпечення їх розвитку та матеріального стимулювання фахівців з числа науково-педагогічного складу, ад’юнктів, докторантів, слухачів тощо.

ЛІТЕРАТУРА:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 - Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris). Режим доступу: https://www.nato.int/cps/en/natohq/opinions_154462.htm

3. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

4. С.Вдовенко, Ю.Даник, С.Фараон, “Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення”. Електронний журнал політики відкритого доступу “Комп’ютерні науки та кібербезпека” Харківського національного університету імені В.Н.Каразіна. SSN 2519-2310 (Online) №1 (12) 2019. С.18-30. Режим доступу: https://periodicals.karazin.ua/cscs/issue/view/803

5. Alexander Kosenkov. Cyber Conflicts as a New Global Threat file: Режим доступу: https://www.researchgate.net/scientific-contributions/2115250763_Alexander_Kosenkov

6. О.А.Баранов, Про тлумачення та визначення поняття “кібербезпека” “Правова інформатика”, № 2(42)/2014. – С. 54-62.

7. В.Л. Бурячок Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011. – № 3 (26). – С. 104-114.

8. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа (2015). В. Б. Толубко (загальна редакція). Інформаційна на кіберберзпека: соціотехнічний аспект./ В. Л. Бурячок, . – К.: ДУТ, 2015. – 288 с.

9. В. Л. Бурячок Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок. – К.: НАУ, 2013. – 432 с.

10. В. Л.Бурячок, Г. М. Гулак, В. О. Дорошко. Завдання, форми та способи ведення воєн у кібернетичному просторі. Наука і оборона, № 3 2011. С.35-42.

11.Ю.І. Грицюк. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання, Науковий вісник НЛТУ України. – 2016. – Вип. 26.8 Національний лісотехнічний університет України Режим доступу:. http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

12.Р.В. Грищук , Ю.Г.Даник. Основи кібернетичної безпеки. Монографія. вид. трете перероблене Житомир. ЖНАЕУ, 2016. – 636 с.

13.Д.В.Дубов. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К.: Вид-во НІСД, 2011. – 30 с.

14.Д.В. Дубов. Стратегічні аспекти кібербезпеки України / Д.В. Дубов // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К.: Вид-во НІСД. – 2013. – № 4 (29). – С. 119-126.

15.Д. В. Дубов. Кіберпростір як новий вимір геополітичного суперництва: монографія /– К. : НІСД, 2014. – 328 с.. Режим доступу: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

16.Р.В. Лук'янчук. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ: зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.

17.Р. В. Лук’янчук. Деякі питання реформування системи державного управління у сфері забезпечення кібернетичної безпеки: сучасний погляд / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2013. – Вип. 2. – С. 81 -92.

18.В.В. Петров. Щодо формування національної системи кібербезпеки України / В.В. Петров // Стратегічні пріоритети: наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 127–130.

19.В.П. Шеломенцев. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.

20.М. Ю. Яцишин. Міжнародно-правова протидія кібервійнам / Яцишин М. Ю.//, збірник праць Національного авіаційного університету – 2015 – № 1 – С. 67-71

21.Putin’s asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: Режим доступу: http://www.gpoaccess.gov/congress/index.html

22. J. Andress Cyber warfare: Techniques, tactics and tools for security practitioners / Andress J., Winterfeld S., Rogers R. – Amsterdam : Syngress/Elsevier, 2011. – 289 p

23. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Режим доступу - http://csef.ru/media/articles/3990/3990.pdf

24. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

25. Конституція України [Електронний ресурс] – Режим доступу: http://zakon0.rada.gov.ua/laws/show/254

26. Закон Про оборону України: за станом на 01.07.2018 р./, затверджений ВР України від 06.12.1991, № 1932-XII. – [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12.

27. Закон України Про Збройні Сили України від 6 грудня 1991 року N 1934-XII (зі змінами), [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1934-12.

28. Закон України Про основні засади забезпечення кібербезпеки України № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс] – Режим доступу:http://zakon.rada.gov.ua/laws/show/2163-19

29. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. – 2016. – № 23.

30. Ю.Даник, С.Вдовенко, Ланцюгові ефекти в кібердіях, К., ВІКНУ імені Т.Шевченка, Зб. наукових праць випуск №64, 2019, С. 71-90.

31. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/201632. DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018 Режим доступу: https://fas.org/irp/doddir/dod/jp3_12.pdf.

33. Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee. Режим доступу: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-13-18.pdf.

REFERENCES:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 -Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris). Режим доступу - https://www.nato.int/cps/en/natohq/opinions_154462.htm

3. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Режим доступу - https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

4. Vdovenko,S Danik,Y and Faraon, S (2019), "Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення." [Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution], International electronic scientific journal Computer Science and Cybersecurity Issue 1(12) 2019 ISSN 2519-2310 (Online).p.p.18-30 – Available:https://periodicals.karazin.ua/cscs/issue/view/803

5. Kosenkov,A Cyber Conflicts as a New Global Threat file, Available: https://www.researchgate.net/scientific-contributions/2115250763_Alexander_Kosenkov

6. Baranov,A (2014) "Pro tlumachennya ta vyznachennya ponyattya kiberbezpeka", [On the interpretation and definition of cyber security], "Pravova informatyka", [Legal Informatics], No. 2 (42) / 2014 - p. 54-62.

7. Buryachok,V (2011) "Kibernetychna bezpeka – holovnyy faktor staloho rozvytku suchasnoho informatsiynoho suspilstva", [Cybernetic security - the main factor for the sustainable development of a modern information society],"Suchasna spetsialna tekhnika ",[Modern special technique] sciences works, No. 3 (26), p. 104-114.

8. Buryachok,V, Tolubko,V, Khoroshko,V and Tolyupa,S. (2015) "Informatsiyna na kiberberzpeka: sotsiotekhnichnyy aspekt",[Information on cyber-security: the sociotechnical aspect], Kyiv, DUT, 288 p.p.

9. Buryachok,V (2013) "Osnovy formuvannya derzhavnoyi systemy kibernetychnoyi bezpeky",[Fundamentals of the formation of the state system of cybernetic security], a monograph , Kyiv: NAU, 432 pp.

10. Buryachok,V, Gulak,G and Doroshko,V. (2011) "Zavdannya, formy ta sposoby vedennya voyen u kibernetychnomu prostori", [Tasks, forms and methods of conducting wars in cybernetic spacious], "Nauka i oborona", [Science and Defense], № 3, p. 35-42.

11. Grytsuk, Yu. (2016) "Kiberinterventsiya ta kiberbezpeka Ukrayiny: problemy ta perspektyvy yikh podolannya" [Ciber iintervention and cyber security of Ukraine: problems and prospects for their overcoming], Naukovyy visnyk NLTU Ukrayiny, [Scientific Bulletin of NLTU of Ukraine], vol. 26.8 National Forestry University of Ukraine http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf.

12. Grishchuk, R and. Danyk Yu. (2016) "Osnovy kibernetychnoyi bezpeky"[The basics of cybernetic security], Monograph., Zhytomyr. ZHNAEU, 636 pp.

13. Dubov, D and Ozhevan,M (2011) "Kiberbezpeka : svitovi tendentsiyi ta vyklyky dlya Ukrayiny", [Cybersecurity. World Trends and Challenges for Ukraine], Kyiv,View NISD, 2011, 30 p.p.

14. Dubov,D (2013) "Stratehichni aspekty kiberbezpeky Ukrayiny" [Strategic Aspects of Cyber security of Ukraine], "Stratehichni priorytety" [Strategic Priorities: Sciences], Kyiv,View NISD, № 4 (29), p. 119-126.

15. Dubov,D (2014) "Kiberprostir yak novyy vymir heopolitychnoho supernytstva", [Cyberspace as a new dimension of geopolitical rivalry], Monograph, Kyiv, View NISD, 328 p.p, Access Mode: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf.

16. Lukyanchuk,R. (2015) "Derzhavna polityka u sferi zabezpechennya kibernetychnoyi bezpeky v umovakh provedennya antyterorystychnoyi operatsiyi" [State policy in the field of providing cybernetic security in the context of anti-terrorist operation], "Visnyk NADU" zb. nauk. prats, [Bulletin NADU] sciences works p. 110-116.

17. Lukyanchuk, R (2013) "Deyaki pytannya reformuvannya systemy derzhavnoho upravlinnya u sferi zabezpechennya kibernetychnoyi bezpeky: suchasnyy pohlyad" [Some issues of reforming the system of public administration in the field of cybernetic security: modern view], "Visnyk NADU" zb. nauk. prats, [Visnyk NADU] sciences works, Issue 2. - p. 81 -92.

18. Petrov,V (2013) "Shchodo formuvannya natsionalnoyi systemy kiberbezpeky Ukrayiny" [Concerning the National Cybersecurity System of Ukraine], nauk.-analit. zb. "Stratehichni priorytety", [Strategic Priorities] Science-analyst. every quarter save, Kyiv, View of NISS, No. 4 (29), p. 127-130.

19. Shelomentsev,V (2012) "Pravove zabezpechennya systemy kibernetychnoyi bezpeky Ukrayiny ta osnovni napryamy yiyi udoskonalennya" [Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement], "Borotba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka)" zb. nauk. prats, [Fighting organized crime and corruption (theory and practice)] sciences works save. No. 1 (27). - P. 312-320.

20. Yatsyshyn, M. (2015) "Mizhnarodno-pravova protydiya kiberviynam" [International legal counteraction to cyberwarfaces], zbirnyk prats Natsionalnoho aviatsiynoho universytetu [The National Aviation University publication collection] № 1, p. 67-71.

21. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: http://www.gpoaccess.gov/congress/index.html

22. Andress, J., Winterfeld,S. and Rogers,R. (2011) "Cyber warfare: Techniques, tactics and tools for security practitioners" , – Amsterdam: Syngress/Elsevier, 2011. – 289 p.

23. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Available: http://csef.ru/media/articles/3990/3990.pdf

24. The National Security Strategy of Ukraine. [Stratehiia natsionalnoi bezpeky Ukrainy], approved by the Decree of the President of Ukraine dated 05/26/2015 № 287/2015.

25. Konstytucija Ukrajiny [The constitution of Ukraine] – Available: http://zakon0.rada.gov.ua/laws/show/254.

26. Zakon Pro oboronu Ukrajiny: za stanom na 01.07.2018 r. / zatverdzhenyj VR Ukrajiny vid 06.12.1991, # 1932-XII. [Law on Defense of Ukraine: as of 01.07.2018 /, approved by the Verkhovna Rada of Ukraine dated 06.12.1991, № 1932-XII] – Available: http://zakon4.rada.gov.ua/laws/show/1932-12

27. Zakon Ukrajiny Pro Zbrojni Syly Ukrajiny vid 6 ghrudnja 1991 roku N 1934-XII (zi zminamy) [Law of Ukraine On the Armed Forces of Ukraine of December 6, 1991 N 1934-XII (as amended)]. Available: http://zakon3.rada.gov.ua/laws/show/1934-12

28. Zakon Ukrayiny "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" № 2163-VIII 10/05/2017, [Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine] No. 2163-VIII of October 5, 2017. Available: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.

29. Stratehiia kiberbezpeky Ukrainy [The strategy cyber security of Ukraine.], of was approved by the Decree of the President of Ukraine dated March 15, 2016, No. 96/2016.

30. Danyk. Ju., Vdovenko S., Lancjughovi efekty v kiberdijakh [Chain effects of cyberspace action], K., VIKNU imeni T.Shevchenka, Zb. naukovykh pracj vypusk #64, 2019, S. 71-90.

31. Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy [Concept of development of the security and defense sector of Ukraine], put into effect by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.

32. DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf.

33. Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee. Available: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-13-18.pdf

д.т.н., проф. Даник Ю.Г., Вдовенко С.Г.

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ КИБЕРОБОРОНЫ ГОСУДАРСТВА

Возрастание роли и значимости решения задач кибербезопасности и кибероборонывызвано инновационным развитием информационных, электронных и кибертехнологий, которые являются движителем ряда тенденций в военном деле. Вследствие формирования и признания искусственного пятого пространства – киберпространства, отдельной сферой борьбы между государствами, включая вооруженное противоборство, вопросы кибербезопасности и киберобороны стали актуальными в обеспечении национальной безопасности и обороны развитых государств, которые особенное внимание уделяют формированию и развитию систем кибербезопасности и киберобороны, как головного фактора достижения военно-стратегического превосходства в обеспечении национальной безопасности и обороны в современных и перспективных условиях.

В статье проведено анализобщих принципов построения систем кибербезопасности и киберобороны передовых государств мира в контексте возможности и целесообразности внедрения их опыта в Украине; анализ условий, текущего состояния и проблемных вопросов формирования систем кибербезопасности и киберобороны в Украине. В частности, отсутствие основных теоретических и прикладных положений формирования системы киберобороны; отсутствие национального органа военного управления в сфере кибеообороны; рассредоточение усилий различных военно-организационных структур в решении задач кибербезопасности и отсутствие сформулированных задач киберобороны.

Предложен наиболее рациональный вариант создания систем и структур кибербезопасности и киберобороны Украины с подсистемами образования и науки, который в соответствии с современными тенденциями развития, с учетом военно-политической обстановки, национальных интересов и законодательства, обеспечит информационное, кибернетическое и когнитивное превосходство над противником и будет способствовать практической реализации принятой в странах НАТО концепции “смарт-обороны”.

Ключевые слова: кибератака, кибербезопасность, кибервлияние, кибердействия, киберзащита, кибероборона киберопераци, киберпространство, киберразведка, киберугроза, кибердар, система кибербезопасности, система киберобороны, субъекты кибербезопасности, субъекты киберобороны, объекты критической информационной инфраструктуры.

prof. Y. Danyk, S.Vdovenko

PROBLEMS AND PROSPECTS OF ENSURING A STATE CYBER DEFENSE

The growing role and importance of solving the problems of cybersecurity and cyber defense is due to the innovative development of information, electronic and cyber technologies, which are the driving force behind a number of trends in military affairs. Due to the formation and recognition of the artificial fifth space - cyberspace, as a separate area of struggle between states, including armed confrontation, issues of cybersecurity and cyber defense have become urgent in ensuring national security and defense of developed states, which pay special attention to the formation and development of cybersecurity and cyber defense systems as the main factor achievements of military-strategic superiority in ensuring national security and defense in modern variables and future conditions.

The article analyzes the general principles of building cybersecurity and cyber defense systems of the advanced states of the world in the context of the possibility and expediency of introducing their experience in Ukraine; analysis of the conditions, current status and problematic issues of the formation of cybersecurity and cyber defense systems in Ukraine. In particular: the lack of basic theoretical and applied provisions for the formation of a cyber defense system; lack of a national military command and control agency in the field of cyber defense; the dispersed efforts of various military organizational structures in solving cybersecurity problems and the lack of formulated cyber defense tasks.

The most rational option of creating systems and structures of cybersecurity and cyber defense of Ukraine with subsystems of education and science is proposed, which, in accordance with modern development trends, taking into account the military-political situation, national interests and legislation, will provide informational, cybernetic and cognitive superiority over the enemy and will contribute to the practical implementation of the concept of “smart defense” adopted in NATO countries.

Keywords: cyber action, cyber attack, cyber defense, cyber intelligence, cyber security, cyberspace, cyber operation, cyber threat, cyber security information infrastructure entities, cyber security infrastructure subjects.

УДК 004.056.53

к.т.н., с.н.с. **Лаптєв О.А.** (ДУТ)
к.ф.-м.н., доц. **Собчук В.В.** (ДУТ)
д.т.н., проф. **Савченко В.А.** (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-09

МЕТОД ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМИ ВИЯВЛЕННЯ, РОСПІЗНАВАННЯ І ЛОКАЛІЗАЦІЇ ЦИФРОВИХ СИГНАЛІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

В процесі виявлення, розпізнавання, та локалізації сингалу засобів негласного отримання інформації в інформаційних системах актуальним питанням є підвищення завадостійкості. В статті досліджено особливості використання фільтрів низької частоти з квадратичною та лінійною залежністю відгуку від вхідного сигналу. Показано, що принцип роботи фільтрів полягає у тому, що виконується процес підсумовування. При цьому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно, тобто корисний сигнал збільшується, а сигнал завади зменшується. Під час впливу на вхід лінійного та квадратичного фільтрів прямокутного імпульсу, який імітує сигнал сучасних цифрових засобів негласного отримання інформації, визначені необхідні для подальшого використання параметри вхідних та вихідних сигналів: математичне сподівання, коефіцієнт кореляції, дисперсія, середньоквадратичне відхилення, відношення сигналів до завад у часовому та спектральному вигляді. Обчислено коефіцієнт виграшу, який показує ефективність використання фільтрів низької частоти.

Наведено графіки огинаючої напруги на виході ідеального смугового фільтру при впливі на вхід прямокутного імпульсу з різною тривалістю – сигналу засобів негласного отримання інформації. Проведено моделювання процесу фільтрації при різних коефіцієнтах кореляції. Це підтвердило можливість виділення сигналу засобів негласного отримання інформації методом визначення двомірної щільності ймовірності сигналу завади на фоні загального сигналу.

Досліджується процес підвищення завадостійкості системи у цілому. Доведено, що використання у процесі обробки сигналів вузько-смугових фільтрів низької частоти дозволяє досягти підвищення завадостійкості системи визначення, розпізнавання та локалізації засобів негласного отримання інформації на 23 %.

Ключові слова: завадостійкість, фільтр, математичне сподівання, дисперсія, моделювання.

Вступ. Під завадою радіосигналу в роботі розуміється будь-який вид електричних коливань, який, проникаючи в радіоприймальні пристрої із зовні або виникаючи всередині його, ускладнює визначення радіосигналу. Сигнал і завада, одночасно діють на вході приймача, відтворюються на виході останнього у вигляді випадкового коливального процесу. В результаті цього неможливо точно визначити параметри сигналу. Нормальне визначення сигналу можливо тільки при певному співвідношенні потужності сигналу і завади на виході приймача. Найменша потужність сигналу, при якій забезпечується задовільне визначення сигналу, залежить від рівня завад. Ця величина потужності характеризує чутливість приймача. Здатність радіоприймального пристрою приймати із заданою якістю сигнал при наявності завад називається завадостійкістю. Покращення завадостійкості радіоприймальних пристроїв – одна з основних і найскладніших проблем радіотехніки. Для успішного вирішення її необхідно вивчити властивості та характер впливу завад на сигнал, а потім визначити способи ослаблення їх впливу на якість визначення сигналу.

Питання подолання завад мають свої особливості і у процесі виявлення, розпізнавання, та локалізації сингалу засобів негласного отримання інформації (ЗНОІ). З цією метою розглянемо питання завадостійкості при дослідженні вищезазначених процесів.

Аналіз останніх публікацій та постановка проблеми. Розгляду питання завадостійкості присвячено значну кількість публікацій. Так у [1] розглядаються технічні методи підвищення ефективності радіозв'язку, пов'язані з завадостійкістю. Розглянуто методи підвищення завадозахищеності і завадостійкості та наведено фактори, які їх формують. В якості найбільш небезпечних завад, які впливають на роботу радіостанції, виділені фактори ретрансляції, коли кореляційна функція корисного сигналу і завади приймають великі значення у порівнянні із значеннями для завади псевдоймовірної послідовності та гармонічної завади. Показано, що варіанти кодування джерела інформації принципово не впливають на стійкість радіостанцій при дії зазначених завад. Проте, питання завадостійкості під час пошуку ймовірних сигналів не розглядаються.

В роботі [2] розглядається процес завадостійкості типового тракту виявлення, складеного з послідовно включених модулів: ідеального смугового фільтра, квадратичного детектора і ідеального інтегратора. Описана методика визначення імовірнісних характеристик виявлення може бути застосована для дослідження типових трактів, складених із інших елементів, що представляє суттєвий практичний інтерес. Разом із тим, питанням впливу завади на прямокутний сигнал, що є аналогічним до сигналу засобу негласного отримання інформації, не приділяється уваги.

У статті [3] із застосуванням методів статистичної радіотехніки проаналізовано завадостійкість прийому сигналів з квадратурною амплітудною модуляцією в присутності шумової та гармонічної завади. Отримано залежності ймовірності бітової помилки від відношення сигнал/шум, від інтенсивності завади та від її розкладу щодо центральної частоти спектра корисного сигналу. Показано, що прийом сигналів з квадратурною амплітудною модуляцією сильно погіршується при наявності гармонічної завади та зі збільшенням позиційності сигналів цей вплив посилюється. Проте, визначення сигналів ЗНОІ не розглядається.

У статті [4] на основі розподілених моделей запропоновано метод приведення голосових сигналів до єдиного вікна амплітуди та часу. Також запропоновано розподілені кластеризовані схеми навчання голосових сигналів для формування опорних моделей мовних голосових звуків. Ці методи дозволяють швидко перетворити квазіперіодичні ділянки різної довжини в єдине вікно амплітуди й часу для подальшого порівняння, а також визначити оптимальну кількість кластерів, що збільшує ймовірність кластеризації. Запропоновані методи можуть бути використані в системах розпізнавання сигналів.

У роботі [5] на основі досліджень, проведених в MATLAB, була розроблена модель оптимізації для вимірювання потужності в контурах. Запропоновані алгоритми можуть бути використані при розробці характеристик різних інформаційних сигналів, в тому числі сигналів від засобів негласного отримання інформації.

В [6] досліджено вплив багатопроменевого поширення радіохвиль на передавання звукового контенту через канали з нормальним та логнормальним розподілом завад з використанням безпроводових технологій GSM та WiMAX. Для дослідження в програмному середовищі MATLAB Simulink побудовано відповідні моделі приймально-передавальних трактів з використанням елементів бібліотеки Communication System Toolbox. Разом із тим, в роботі не використовуються *фільтри низької частоти з квадратичною та лінійною залежністю відгуку від вхідного сигналу.*

В [7] запропоновано методику взаємодії мобільних технічних об'єктів в процесі передачі потоків даних в умовах впливу потужного електромагнітного поля.

Робота [8] присвячена підвищення завадостійкості інформаційних повідомлень в умовах дії потужних електромагнітних завад шляхом застосування складних сигнально-кодових конструкцій. Це дозволяє підвищити обсяг та швидкість передачі інформації. В результаті кодування інформації надкороткими імпульсами у безпроводових системах передачі

інформації проведена кількісна та якісна оцінка ефективності запропонованого методу. Проте, методам фільтрації сигналу в даній роботі не приділяється увага.

В [9] висвітлені результати досліджень щодо підвищення співвідношення сигнал / шум в системах мобільного зв'язку. Реалізація цього напрямку здійснюється за рахунок використання методів динамічної зміни потужності передавачів, організації множинного доступу і динамічного розподілу каналів зв'язку. Проте, питання розпізнавання сигналів від засобів негласного отримання інформації не вирішуються.

З аналізу сучасної літератури можна зробити висновок, що питання завадостійкості, які мають свої особливості у процесі виявлення, розпізнавання, та локалізації сингалу засобів негласного отримання інформації, практично не розглядаються. Тому на сьогоднішній день виявляється доцільним дослідити питання завадостійкості в автоматизованій системі виявлення, розпізнавання та локалізації засобів негласного отримання інформації.

Виклад основного матеріалу. Практично усі методи завадостійкості приймання сигналів засновані на принципі усереднення сигналу та завади. Даний принцип полягає у тому, що виконується процес підсумовування. При чому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно. З метою усереднення корисного сигналу та завади застосовуються лінійні системи двох типів: вузькосмугові фільтри та фільтри низької частоти. При цьому можливо оптимізувати фільтри низької частоти або вузькосмугові фільтри.

Для розгляду питання фільтрації завад, зробимо припущення, що сам вузькосмуговий фільтр не вносить спотворення в форму сигналу, який пройшов через нього. Ідеальний смуговий фільтр – це фільтр з амплітудно-частотною характеристикою виду:

$$K(\omega)=\begin{cases}1 \quad якщо \quad \omega_0-\dfrac{\Delta\omega}{2}\le|\omega|\le\omega_0+\dfrac{\Delta\omega}{2}\\ 0 \quad якщо \quad \left]-\infty,\omega_0-\dfrac{\Delta\omega}{2}\right[U\left]\omega_0+\dfrac{\Delta\omega}{2},\infty\right[\end{cases}, \tag{1}$$

де $\Delta\omega$ – полоса пропускання фільтру.

Для ідеального фільтру ефективна полоса $\Delta\ \omega_e$ та полоса на рівні $0,707-\Delta\ \omega_{\sqrt{2}}$, що дорівнює полосі прозорості фільтру $\Delta\omega$.

Для фільтрів вірним є припущення, що $\Delta\ \omega\ <<\Delta\ \omega_0$.

Частотна характеристика виразу для (1), це імпульсна перехідна характеристика, яка буде визначатися виразом:

$$h_\delta(t)=\frac{\Delta\omega}{\pi}\cdot\frac{\sin\dfrac{\Delta\omega t}{2}}{\dfrac{\Delta\omega t}{2}}\cos\omega_0 t\ . \tag{2}$$

З огляду на те, що сигнал цифрового ЗНОІ являється імпульсом [10], то можна обчислити огинаючу напруги на виході ідеального фільтра при впливі на нього прямокутного імпульсу тривалістю T:

$$x(t)=\begin{cases}X_m\cos\omega_0 t \quad якщо \quad 0\le t\le T\\ 0 \quad якщо \quad \left]-\infty,0\right[U\left]T,\infty\right[\end{cases}, \tag{3}$$

де X_m – огинаюча сигналу $x(t)$ на вході фільтру.

За допомоги теореми про огинаючу напруги вузькосмугового фільтру, запишемо вираз для огинаючою напруги на виході фільтру:

$$Y_m(t)=\frac{1}{2\pi}\int_{-\infty}^{\infty}K_{fn}(j\omega)S_{X_m}(j\omega)e^{j\omega t}dt\,, \tag{4}$$

де $S_{X_m}(j\omega) = \int_{-\infty}^{\infty} X_m e^{-j\omega t} dt$ – амплітудний спектр огинаючої сигналу $x(t)$,

K_{fn} – комплексний коефіцієнт передачі фільтра низької частоти:

$$K_{fn}(j\omega) = \begin{cases} 1 \quad якщо \quad -\frac{\Delta\omega}{2} \le |\omega| \le \frac{\Delta\omega}{2} \\ 0 \quad якщо \quad]-\infty, \frac{\Delta\omega}{2}[\ U\ ]\frac{\Delta\omega}{2}, \infty[\end{cases}. \tag{5}$$

Якщо підставити вираз (5) у вираз (4), то отримаємо вираз:

$$Y_m(t) = \frac{X_m}{2\pi}\left(Si(\Delta\omega t) - Si(\Delta\omega(t-T))\right), \tag{6}$$

де $Si(z) = \int_0^z \frac{\sin t}{t} dt$ – інтегральний синус [11].

На рис. 1 приведено графіки залежності тривалості впливаючого прямокутного імпульсу (рожевий колір – тривалість імпульсу T=1, червоний колір – T=10, зелений колір –T=15 та чорний колір – T=20) від діапазону частоти (полоси пропускання фільтру).

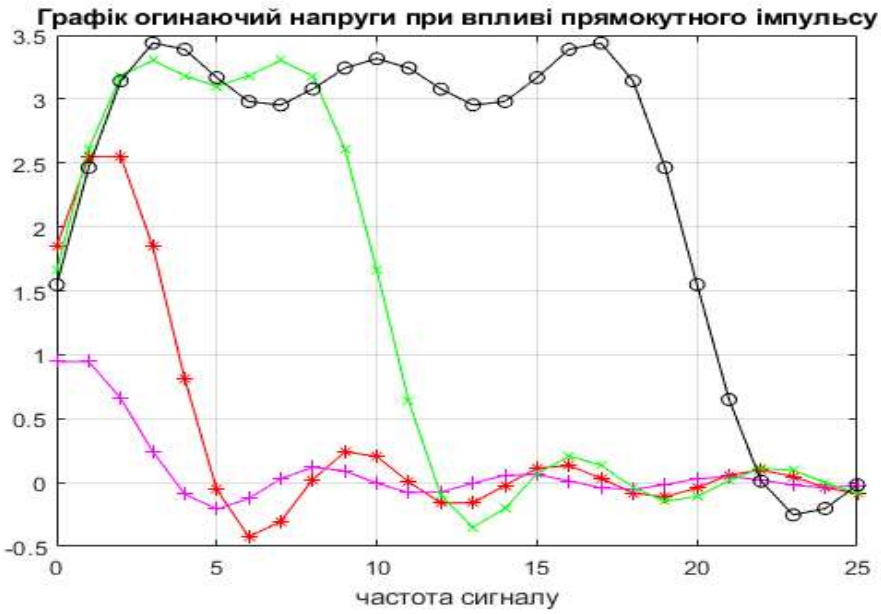


Рисунок 1 – Графік огинаючої напруги при впливі прямокутного імпульсу сигналу

З наведених графіків бачимо суттєві відмінності вхідного прямокутного імпульсу від вихідного сигналу. Спотворення вхідного імпульсу зростає при збільшення його тривалості. Це спотворення форми імпульсу можливо охарактеризувати співвідношенням тривалості фронту огинаючої імпульсу на виходи фільтра до тривалості огинаючої вихідного імпульсу.

Це свідчить про те, що короткочасні прямокутні сигнали можливо виділяти за допомогою смугового фільтру [12].

Для подальшого обчислення сигналу завади, визначимо коефіцієнт автокореляції білого шуму, який пройшов через смуговий фільтр:

$$R_w(\tau)=\frac{\int_0^{\infty}K^2(\omega)\cos\omega t dt}{\int_0^{\infty}K^2(\omega)d\omega}. \quad (7)$$

Зробивши підстановку виразу (1) у вираз (7) отримаємо:

$$R_w(\tau)=\frac{1}{\Delta\omega}\int_{\omega_0-\frac{\Delta\omega}{2}}^{\omega_0+\frac{\Delta\omega}{2}}\cos\omega\tau d\omega=\frac{\sin\left(\omega_0+\frac{\Delta\omega}{2}\right)\cdot\tau-\sin\left(\omega_0-\frac{\Delta\omega}{2}\right)\cdot\tau}{\Delta\omega\tau}, \quad (8)$$

або $$R_w(\tau)=r_w(\tau)\cos\omega_0\tau, \quad (9)$$

де $r_w(\tau)=\frac{\sin(\Delta\omega\frac{\tau}{2})}{\Delta\omega\frac{\tau}{2}}$ – огинаюча коефіцієнта автокореляції процесу на виході смугового фільтру.

В зв'язку із тим, що сигнал цифрових ЗНОІ є сигналом прямокутного імпульсу, з огинаючою тривалістю T, то вираз має вигляд [13]:

$$y_s=\begin{cases}A\cos(\omega_0+\varphi_0) & ,0\le t\le T\\ 0 &]-\infty,t[U]t,\infty[\end{cases}. \quad (10)$$

Тоді чисельні характеристики процесу фільтрації квадратичного фільтру набудуть вигляду:

$$m_1[z_{\Sigma 0}(t)]=\begin{cases}A_1\sigma_{yN}^2(1+q^2), & 0\le t\le T\\ A_1\sigma_{yN}^2=m_1[z_{N0}(t)], &]-\infty,t[U]t,\infty[\end{cases}, \quad (11)$$

де $m_1[z_{0N}(t)]$ – математичне сподівання низькочастотної флуктуації завади.

$$R_{z\Sigma 0}(t,t+\tau)=\begin{cases}\dfrac{r_{yN}^2(\tau)+2q^2r_{yN}(\tau)}{1+2q^2}=R_{z\Sigma 0}(\tau), & 0\le t\le(T-\tau)\\ r_{yN}^2(\tau)=R_{zN0}(\tau), &]-\infty,t[U]t,\infty[\end{cases}, \quad (12)$$

$R_{zN0}(\tau)$ – коефіцієнт автокореляції низькочастотної флуктуації завади.

$$D_{z\Sigma N}=\sigma_{z\Sigma N}^2(t)=\begin{cases}A_1^2\sigma_{yN}^4(1+2q^2)=\sigma_{z\Sigma 0}^2, & 0\le t\le T\\ A_1^2\sigma_{yN}^4=\sigma_{zN0}^2, &]-\infty,t[U]t,\infty[\end{cases}. \quad (13)$$

Процес у якого математичне сподівання та кореляційна функція не залежать від часу , на визначеному фіксованому інтервалу часу, називається квазістаціонарним. Тоді процес на виході фільтра не впливе на його адитивну суму сигналу та завади і буде квазістаціонарним [14].

Для лінійного фільтру чисельні показники процесу фільтрації приймають вигляд:

$$m_1[z_{\Sigma 0}(t)]=\frac{A_1\sigma_{y\Sigma}^2}{\sqrt{2\pi}}; \quad (14)$$

$$R_{z\Sigma 0}(\tau) \approx r_{yN}^2(\tau); \tag{15}$$

$$\sigma_{z\Sigma 0}^2 = \frac{A_1 \sigma_{y\Sigma}^2}{8\pi}\ , \tag{16}$$

де $\sigma_{y\Sigma}^2 = D_{y\Sigma}$ – дисперсія сумарного процесу на вході фільтра. Вона визначається:

$$\sigma_{y\Sigma}^2 = \sigma_{yS}^2 + \sigma_{yN}^2\,, \tag{17}$$

де $D_{ys} = \sigma_{ys}^2, D{=}_{ys}\sigma_{yN}^2$ – дисперсії сигналу та завади на вході фільтру.

Обчислимо функції взаємної кореляції $z_{N0}(t),\ \ z_{\Sigma 0}(t)$ вихідних сигналів.

У випадку сигнала із завадами, математичне сподівання для змішаного сигналу другого порядку $z_N(t),\ \ z_\Sigma(t)$ буде визначатися виразом:

$$\begin{aligned} m_1[z_N(t_1), z_\Sigma(t_2)] &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} z_N(t_1) z_\Sigma(t_2) w_2[y_N(t_1), y_\Sigma(t_2)] \times \\ &\times dy_N(t_1) dy_\Sigma(t_2) = A_2^2 \int_0^{\infty}\int_0^{\infty} y_N(t_1) y_\Sigma(t_2) w_2[y_N(t_1), y_\Sigma(t_2)] \times \\ &\times dy_N(t_1) dy_\Sigma(t_2) \end{aligned}\ . \tag{18}$$

де $w_2[z_N(t_1), z_\Sigma(t_2)]$ – двовимірна щільність ймовірності стаціонарних нормальних процесів $y_N(t),\ \ y_\Sigma(t)$. Виходячи з того, що коефіцієнт автокореляції у обох сигналів однаковий та дорівнює $R_{yN}(\tau)$, можливо записати вираз для $w_2[z_N(t_1), z_\Sigma(t_2)]$ – двовимірної щільності ймовірності у вигляді:

$$\begin{aligned} w_2[z_N(t_1), z_\Sigma(t_2)] &= \frac{1}{2\pi\ \sigma_{yN}\sigma_{y\Sigma}\sqrt{1-R_{yN}^2(\tau)}} \cdot \exp \times \\ &\times \left(-\ 1\Big/2(1-R_{yN}^2(\tau)\left[\frac{y_N^2(t_1)}{\sigma_{yN}^2} - 2R_{yN}(\tau)\frac{y_N(t_1) y_\Sigma(t_2)}{\sigma_{yN}\sigma_{y\Sigma}} + \frac{y_\Sigma^2(t_1)}{\sigma_{y\Sigma}^2}\right)\right) \end{aligned}\ . \tag{19}$$

Виконавши підстановку виду: $\frac{y_N(t_1)}{\sigma_{yN}} = x,\ \ \frac{y_N(t_2)}{\sigma_{y\Sigma}} = y$ отримаємо вираз:

$$m_1[z_N(t_1), z_\Sigma(t_2)] = \frac{A_2 \sigma_{yN}\sigma_{y\Sigma}}{2\pi\ \sqrt{1-R_{yN}^2(\tau)}} \cdot \int_0^{\infty}\int_0^{\infty} \exp\left(-\frac{x^2 - 2R_{yN}(\tau)xy + y^2}{2(1-R_{yN}^2(\tau))}\right) dxdy\ . \tag{20}$$

З метою визначення впливу коефіцієнту кореляції (взаємозв’язку сигналу та завади) на математичне сподівання (тобто впливу завади на сигнал) проведемо моделювання процесу.

Для оцінки сили зв'язку в теорії кореляції застосовується шкала англійського математика Чеддока: слабка – від 0,1 до 0,3; помірна – від 0,3 до 0,5; помітна – від 0,5 до 0,7; висока – від 0,7 до 0,9; вельми висока (сильна) – від 0,9 до 1,0.

Тому послідовно виберемо коефіцієнт кореляції для слабкої, помірної та високої сили зв’язку відповідно [15].

Результати моделювання наведено на рис. 2-4:

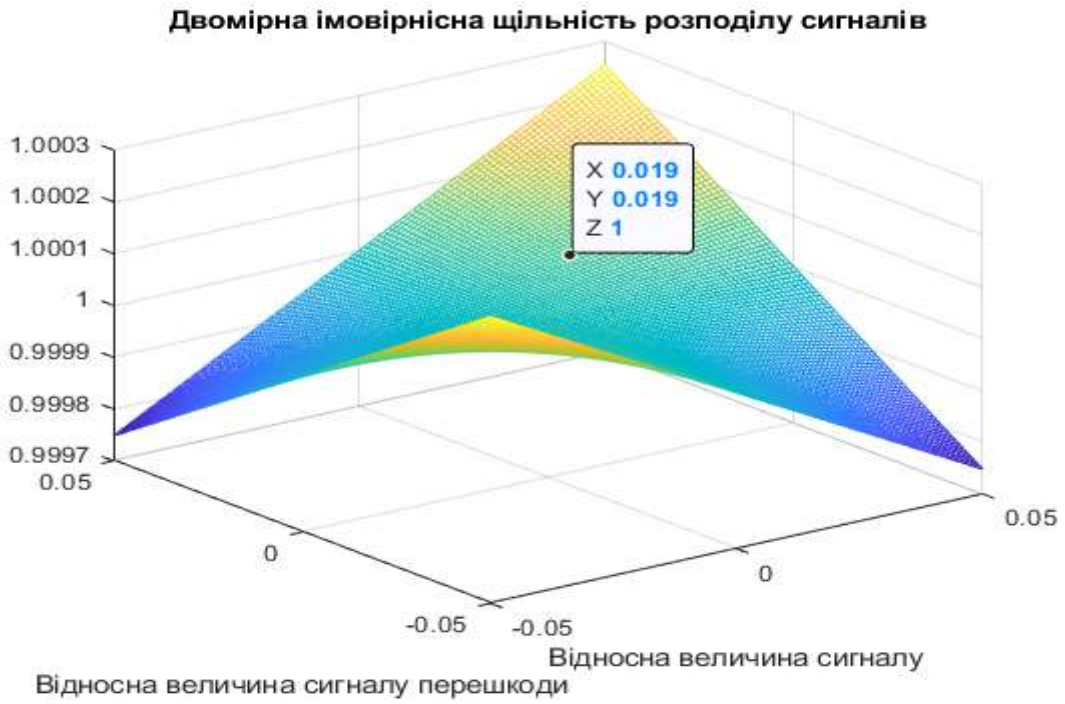


Рисунок 2 – Двовимірна щільність розподілу сигналу при R_{yN} =0,1 (слабка залежність)

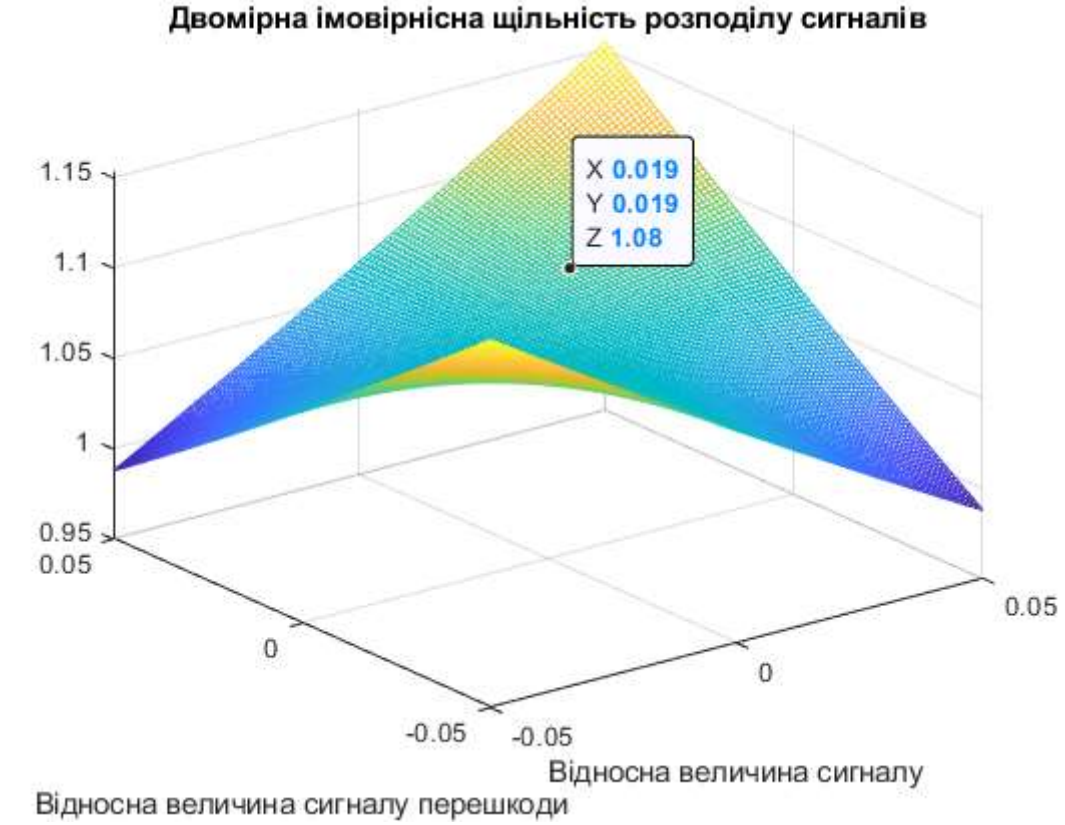


Рисунок 3 – Двовимірна щільність розподілу сигналу при R_{yN} =0,3 (помірна залежність)

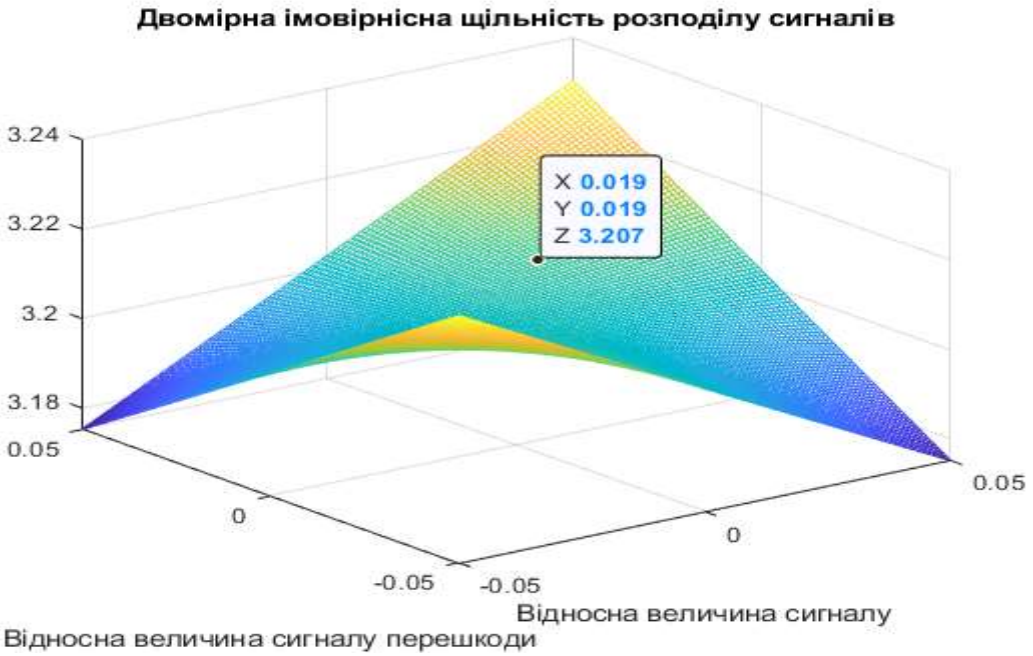


Рисунок 4 – Двомірна щільність розподілу сигналу при R_{yN}=0,9 (висока залежність)

Для проведення аналізу отриманих результатів на кожному з графіків взяли точку з однаковими координатами відносних величин сигналу та завади.

Як бачимо з наведених графіків рис. 2-4, зі збільшенням кореляційної залежності від слабкої до високої, величина щільності розподілу сигналу зростає. Це свідчить про можливість розрізнити сигнал та заваду, зменшення завади за рахунок фільтрації.

Для визначення співвідношення сигнал/завада на виході типового тракту при впливі на його вхід адитивної завади $N(t)$ та сигналу $S(t)$ маємо:

$$x(t) = S(t) + N(t). \tag{21}$$

Зробимо припущення, що сигнал та завада є стаціонарним білим шумом, з нульовим математичним очікуванням $m_1(S(t)) = m_1(N(t)) = 0$. Сигнал та завада між собою некорельовані: $m_1(S(t)(N(t)) = 0$ та визначені на тривалому часі. Тоді можливо записати вирази:

$$D_\Sigma = \sigma_\Sigma^2 = \Delta f_e S_\Sigma;\ \ D_s = \sigma_s^2 = \Delta f_e S_s;\ \ D_N = \sigma_N^2 = \Delta f_e S_N\ , \tag{22}$$

де Δf_e – ефективна смуга прозорості фільтру;

$D_\Sigma = \sigma_\Sigma^2$ – дисперсія та середньоквадратичне відхилення суміші сигналів;

$D_s = \sigma_s^2$ – дисперсія та середньоквадратичне відхилення сигналу;

$D_N = \sigma_N^2$ – дисперсія та середньоквадратичне відхилення завади;

$S_\Sigma; S_s; S_N$ – спектральні щільності відповідно суміші сигналу та завади, сигналу і завади.

Із прийнятих нами припущень виходить:

$$\sigma_\Sigma^2 = \sigma_s^2 + \sigma_N^2 \text{ або } D_\Sigma = D_S + D_N. \tag{23}$$

Низькочастотну складову напруги на виході тракту, виявлену в момент відліку $t = T$, позначимо $u_{\Sigma 0}$, напругу завади u_{N0}, напругу суми сигналу $u_{\Sigma 0}$. Необхідно відмітити, що u_{N0} та $u_{\Sigma 0}$ є випадковими величинами.

Поява сигналу на вході тракту, виявленого у момент часу $t = T$, може привести до зміни математичного сподівання низькочастотної складової напруги на виході тракту, від величини $m_1[u_{N0}(t)]$ до $m_1[u_{\Sigma 0}(t)]$. Це збільшення сигналу назвемо корисним сигналом. Запишемо для нього вираз:

$$C = m_1[u_{\Sigma 0}(T)] - m_1[u_{N0}(T)] = \Delta\, m_1[u_0(T)]. \tag{24}$$

В такому випадку, завада у той же момент часу $t = T$, буде визначатися середньоквадратичним значення флуктуації випадкової ймовірної величини:

$$N = \sigma_{u\Sigma}(T) = \left(m_1\left[u_{\Sigma 0}{}^2\ (T) \right] - m_1{}^2\ [u_{\Sigma 0}(T)] \right)^{\frac{1}{2}}. \tag{25}$$

Відношення сигнал/завада при $t = T$ буде мати вигляд:

$$\frac{C}{N} = \frac{m_1[u_{\Sigma 0}(T)] - m_1[u_{N0}(T)]}{\left(m_1\left[u_{\Sigma 0}{}^2\ (T) \right] - m_1{}^2\ [u_{\Sigma 0}(T)] \right)^{\frac{1}{2}}}. \tag{26}$$

Вирази (17 – 19) є визначенням сигналу, завади та відношенні сигнал/завада на виході приймального тракту. В подальшому, нашим завданням буде визначити сигнал, заваду та їх співвідношення через відповідні параметри на вході приймального тракту.

Цей взаємозв'язок можливо визначити двома методами: спектральним та часовим.

При часовому методі напруга на виході приймального тракту у момент часу $t = T$ буде визначатися виразом:

$$u(T) = \int_0^T h_\delta(T - t) z(t) dt, \tag{27}$$

де h_δ – імпульсна перехідна характеристика фільтру, $z(t)$ – вхідна напруга.

Математичне сподівання цей напруги при впливі на вхід суміші сигналу та завади буде мати вигляд:

$$m_1[u_\Sigma(T)] = \int_0^T h_\delta(T - t) m_1[z_\Sigma(t)] dt. \tag{28}$$

В зв'язку з тім що z_Σ – процес стаціонарний, то його математичне сподівання не залежить від часу, тоді маємо:

$$m_1[u_\Sigma(T)] = m_1[z_\Sigma(t)] \int_0^T h_\delta(T - t) dt = m_1[z_\Sigma(t)] \int_0^T h_\delta(t) dt. \tag{29}$$

Аналогічно можливо визначити математичне сподівання при впливі тільки завади:

$$m_1[u_N(T)] = m_1[z_N(t)] \int_0^T h_\delta(t) dt. \tag{30}$$

Підставляючи вирази (18) та (19) у вираз (13) отримаємо:

$$C = \Delta\, m_1[z_0(T)] \int_0^T h_\delta(t) dt, \tag{31}$$

де $\Delta\, m_1[z_0(t)] = m_1[u_{\Sigma 0}(t)] - m_1[u_{N0}(t)]$ збільшення математичного сподівання низькочастотної складової напруги на виході фільтру.

Дисперсія флуктуацій на виході фільтру низьких частот визначається:

$$D_{u\Sigma} = \sigma^2_{u\Sigma} = \left(m_1\left[u_\Sigma{}^2\ (T) \right] - m_1{}^2\ \left[u_\Sigma(T) \right] \right) . \tag{32}$$

З виразу:

$$u^2_\Sigma(T) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h_\delta(T - t_1, T) h_\delta(T - t_2, T) z_\Sigma(t_1) z_\Sigma(t_2) dt_1 dt_2 \tag{33}$$

маємо:

$$m_1[u^2_\Sigma(T)] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h_\delta(T - t_1, T) h_\delta(T - t_2, T) m_1[z_\Sigma(t_1) z_\Sigma(t_2)] dt_1 dt_2 ; \tag{34}$$

$$\begin{aligned} D_{u\Sigma} = \sigma^2_{u\Sigma}(T) = & \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h_\delta(T - t_1, T) h_\delta(T - t_2, T) \times \\ & \times m_1[z_\Sigma(t_1) z_\Sigma(t_2)] dt_1 dt_2 - m_1^2[z_\Sigma(t)] \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h_\delta(T - t_1, T) h_\delta(T - t_2, T) \times \\ & \times h_\delta(T - t_2, T) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h_\delta(T - t_1, T) h_\delta(T - t_2, T) \times \\ & \times m_1[z_\Sigma(t_1) z_\Sigma(t_2)] dt_1 dt_2 - m_1^2[z_\Sigma(t)] dt_1 dt_2 \end{aligned} . \tag{35}$$

Зробимо заміну: $\tau = t_2 - t;\ \ d\tau = dt_2;\ \ t = t_2;\ \ dt = dt_1$ Тоді будемо мати:

$$D_{u\Sigma} = \sigma^2_{u\Sigma} = \sigma^2_{z\Sigma}[\int_{-\infty}^{\infty} Q_h(\tau, T) R_{z\Sigma}(\tau) d\tau], \tag{36}$$

де $$Q_h(\tau, T) = \int_{-\infty}^{\infty} h_\delta(T - t\ , T) h_\delta(T - t - \tau, T) dt\ ; \tag{37}$$

$$R_z(\tau) = \frac{m_1\left[z_\Sigma(t) z_\Sigma(t + \tau) \right] - m_1{}^2\ \left[z_\Sigma(t) \right]}{\sigma^2_{z\Sigma}}, \tag{38}$$

де $R_{z\Sigma}(\tau)$ – коефіцієнт автокореляції, $D_{z\Sigma} = \sigma^2_{z\Sigma}$ – дисперсія процесу при впливі на вхід суми сигналу та завади.

Приймаємо, що згідно виразу (37) завада : $N = \sigma_{u\Sigma}(T)$ тоді будемо мати:

$$N = \sigma_{u\Sigma}(T) = \sigma_{\Sigma 0}[\int_{-\infty}^{\infty} Q_h(\tau, T) R_{z\Sigma}(\tau) d\tau]^{\frac{1}{2}}. \tag{39}$$

У зв’язку з тим, що головним фактором визначення сигналу ЗНОІ є енергетичний спектр, знайдемо вираз для завади у спектральному вигляді.

Для цього скористаймось теоремою Вінера-Хінчіна, яка встановлює взаємозв’язок між функцією кореляції та спектральної щільності потужності $g(\omega)$:

$$K(\tau) = \int_{-\infty}^{\infty} g(\omega) e^{j\omega t} d\omega. \tag{40}$$

Тоді отримуємо:

$$N=\left(\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}h_\delta(T-t,T)h_\delta(T-t-\tau,T)dt\times[\int_{-\infty}^{\infty}g_{z\Sigma 0}(\omega)e^{j\omega\tau}d\omega]d\tau\right)^{\frac{1}{2}}=$$

$$=\left(\int_{-\infty}^{\infty}g_{z\Sigma 0}(\omega)d\omega\int_{-\infty}^{\infty}h_\delta(T-t,T)dt\int_{-\infty}^{\infty}h_\delta(T-t-\tau,T)e^{j\omega\tau}d\tau\right)^{\frac{1}{2}}=$$

$$=\left(\int_{-\infty}^{\infty}g_{z\Sigma 0}(\omega)K_T(j\omega)d\omega\int_{-\infty}^{\infty}h_\delta(T-t,T)e^{j\omega(T-\tau)}dt\right)^{\frac{1}{2}}=$$

$$=\left(\int_{-\infty}^{\infty}g_{z\Sigma 0}(\omega)\left|K_T(j\omega)\right|^2d\omega\right)^{\frac{1}{2}}=\left(\int_{-\infty}^{\infty}G_{z\Sigma 0}(\omega)\left|K_T(j\omega)\right|^2d\omega\right)^{\frac{1}{2}} \quad , \quad (41)$$

де $K_T(j\omega)$ – комплексна частотна характеристика фільтра низької частоти;

$g_{z\Sigma 0}(\omega)$ – спектральна щільність потужності низькочастотних флуктуацій на виході фільтру на всій частотній осі.

$$G_{z\Sigma 0}(\omega)=\begin{cases}2g_{z\Sigma 0}(\omega)=\dfrac{2\sigma_{z\Sigma 0}^2}{\pi}\int_0^{\infty}R_{z\Sigma 0}(\tau)\cos\omega\tau d\tau, & \omega>0\\ 0, & \omega<0\end{cases}, \quad (42)$$

де $G_{z\Sigma 0}(\omega)$ – спектральна щільність потужності сигналу $z_{\Sigma 0}(t)$, визначена тільки в області позитивних частот.

Таким чином, вираз для співвідношення сигнал/завада на виході типового радіотехнічного тракту в режимі визначення сигналу завади на фоні сигналу приймає вигляд:

У часовому вигляді:

$$\frac{C}{N}=\frac{\Delta\, m_1[z_0(t)]\int_0^T h_\delta(t)dt}{\sigma_{\Sigma 0}[\int_{-\infty}^{\infty}Q_h(\tau,T)R_{z\Sigma 0}(\tau)d\tau]^{\frac{1}{2}}}. \quad (43)$$

Спектральна форма запису:

$$\frac{C}{N}=\frac{\Delta\, m_1[z_0(t)]K_T(0)}{[\int_{-\infty}^{\infty}G_{z\Sigma 0}(\omega)\left|K_T(j\omega)\right|^2d\omega]^{\frac{1}{2}}}. \quad (44)$$

Окрім співвідношення сигнал/завада, характеристикою фільтра є коефіцієнт виграшу, який визначається виразом:

$$K_B=\frac{C/N_{вих}}{C/N_{вх}}. \quad (45)$$

Зробивши підстановку виразу (43) у вираз (45), отримаємо:

$$K_B=[\frac{\Delta\, m_1[u_0(T)]}{\sigma_{u\Sigma 0}(T)}]/[\frac{\Delta\, m_1[z_0(T)]}{\sigma_{z\Sigma 0}(T)}]=[\frac{\Delta\, m_1[u_0(T)]}{\Delta\, m_1[z_0(T)]}]/[\frac{\sigma_{u\Sigma 0}(T)}{\sigma_{z\Sigma 0}(T)}], \quad (46)$$

де $\frac{\Delta\, m_1[u_0(T)]}{\Delta\, m_1[z_0(T)]}]$, $[\frac{\sigma_{u\Sigma 0}(T)}{\sigma_{z\Sigma 0}(T)}]$ – визначають приріст математичного сподівання та середньоквадратичного відхилення низькочастотних флуктуацій у результаті обробки вхідного сигналу фільтром низьких частот.

Таким чином з метою підвищення завадостійкості системи визначення, розпізнавання та локалізації, потрібним є використання фільтра низьких частот. За допомогою цього значно понижуються або зовсім виключаються з аналізу завади низьких частот.

Аналіз напрямків розвитку сучасних засобів негласного отримання інформації показують тенденції переходу їх роботи у діапазон високих частот. Тобто сигнал передачі інформації зміщується у діапазон високих частот, у якому процес визначення, розпізнавання та локалізації ЗНОІ є доволі складним.

Виключивши з аналізу завади нижніх частот ми вже значно скоротимо процес пошуку ЗНОІ, та підвищимо завадостійкість системи у цілому.

Висновки. Досліджено особливості використання фільтрів низьких частот з метою підвищення завадостійкості автоматизованої системи визначення, розпізнавання та локалізації засобів негласного отримання інформації. Показано, що принцип роботи фільтрів полягає у тому що виконується процес підсумовування. При цьому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно. Тобто при підсумовуванні корисний сигнал збільшується, а сигнал завади зменшується.

З урахуванням особливості сигналу ЗНОІ, визначені параметри сигналів (математичне сподівання, коефіцієнт кореляції, дисперсію, середньоквадратичне відхилення) та виходи лінійного та квадратичного фільтрів при впливі на вхід прямокутного імпульсу, який імітує сигнал сучасних цифрових засобів негласного отримання інформації.

Отримано графіки огинаючої напруги на виході ідеального смугового фільтру при впливі на вхід прямокутного імпульсу (сигнал ЗНОІ), різної тривалості.

Результатами моделювання процесу фільтрації, при різних коефіцієнтах кореляції, підтвердили можливість виділення сигналу ЗНОІ методом визначення двовимірної щільності ймовірності сигналу завади на фоні загального сигналу.

Доведено, що використання у процесі обробки сигналів вузько-смугових фільтрів низької частоти дозволяє досягти підвищення завадостійкості системи визначення, розпізнавання та локалізації засобів негласного отримання інформації на 23 %.

ЛІТЕРАТУРА:

1. Абед Ахмед, Хассан Абед, Жуков В.М. Анализ помехоустойчивости радиостанции при воздействии организованных помех. Журнал «Весник тамбовского технического университета». Том 22, № 1, 2016 [Електронний ресурс] Режим доступу: https://elibrary.ru/item.asp?id=25503107 (5.09.2019).

2. Пархоменко А.Н., Шоцький Б.І. Завадостійкість типового тракту при виявленні сигналів з флуктуаційною амплітудою. Міжнародній науково-технічний журнал. [Електронний ресурс] Режим доступу: http://radio.kpi.ua/article/view/S002134701982040219 (14.11.2019).

3. Куликов Г.В., Нестеров А.В., Лелюх А.А. Помехоустойчивость приема сигналов с квадратурной амплитудной манипуляцией в присутствии гармонической помехи. Журнал радиоэлектроники, № 11, 2018 [Електронний ресурс] Режим доступу: http://jre.cplire.ru/jre/nov18/9/text.pdf (21.07.2019).

4. Fedorov E., Alrababah H., Nehad A. The distribution for mation method of reference patterns of vocal speech sounds. International Journal of Advanced Trends in Computer Science and Engineering. 2017. Vol. 6 (3), May - June, P. 35 – 39.

5. Ara Jullion A. Abello, Gabriele Francesca Y., Domingo, Maria Jamelina T. Joven, Samanta Alexis S. Malubay. Power Measurement Model Optimizationusing using MATLAB. International Journal of Advanced Trends in Computer Science and Engineering. 2019. Vol. 8, № 3, May – June. P. 538 – 542.

6. Бакіко В.М., Попович П.В,. Швайченко В.Б. Визначення завадостійкості каналу зв’язку за випадкового впливу завад. Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. . – Харків : НТУ "ХПІ", 2018. № 14 (1290). С. 7 – 10.

7. Churyumov G., Tokarev V., Tkachov V., Partyka S. Scenario of Interaction of the Mobile Technical Objects in the Process of Transmission of Data Streams in Conditions of Impacting the Powerful Electromagnetic Field. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). 21-25 Aug. 2018. P. 183 – 186.

8. Serkov O. Breslavets V., Tolkachov M., Kravets V. Method of coding information distributed by wireless communication lines under conditions of interference. Advanced Information Systems. 2018. Vol. 2, No. 2. P. 145 – 148.

9. Serkov O.A., Churyumov G.I. On the issue of solving the problem of electromagnetic compatibility of the wireless telecommunication systems. Applied radio electronics. Sci. and Tech. Jour. 2017. Vol. 16, No. 3,4. P. 117 – 121.

10. Лаптєв О.А., Половінкін І.М, Клюковський Д.В., Барабаш А.О. Модель пошуку засобів негласного отримання інформації на основі диференціальних перетворень. Sciences of Europe. Praha, Czech Republic. 2019. Vol. 1. No 43. P. 59 – 62.

11. Пухов Г.Е. Дифференциальные спектры и модели. К.: Наукова думка, 1990. 188 с.

12. Laptev A.A., Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V. The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi. International Journal of Advanced Research in Science, Engineering and Technology. India. 2019. Vol. 6, Issue 7. P. 10101 – 10105.

13. Лаптєв О.А., Войченко Т.О., Кудюкін П.В., Степаненко В.І. Метод оцінки параметрів сигналу засобів несанкціонованого знімання інформації на основі кореляційно-регресійного аналізу. Науковий журнал "Наукоємні технології". К.: НАУ, 2019. № 3 (43). С. 313 – 320.

14. Qualifying Requirements QR-160D (2004). Environmental Conditions and Test Procedures for Airborne Equipment, ARIAC. 2004.

15. Aaron Don M. Africa, Ara Jyllian A. Abello, Zendrel G. Gacuya, Isaiah Kyle A. Naco, Victor Antonio R. Valdes. Face Recognition Using MATLAB. International Journal of Advanced Trends in Computer Science and Engineering. 2019. Vol. 8, № 4. July-August. P. 1110 – 1116.

REFERENCES:

1. Abed Akhmed, Khassan Abed, Zhukov V.M. Analiz pomehoustoychivosti radiostantsii pri vozdeystvii organizovannyih pomeh. Zhurnal «Vesnik tambovskogo tehnicheskogo universiteta».Tom 22, № 1, 2016 [Elektronnyi resurs] Rezhym dostupu: https://elibrary.ru/item.asp?id=25503107 (5.09.2019).

2. Parkhomenko A.N., Shotskyi B.I. Pereshkodostiikist typovoho traktu pry vyiavlenni syhnaliv z fluktuatsiinoiu amplitudoiu. Mizhnarodnii naukovo-tekhnichnyi zhurnal. [Elektronnyi resurs] Rezhym dostupu: http://radio.kpi.ua/article/view/S002134701982040219 (14.11.2019).

3. Kulikov G.V., Nesterov A.V., Lelyuh A.A. Pomehoustoychivost priema signalov s kvadraturnoy amplitudnoy manipulyatsiey v prisutstvii garmonicheskoy pomehi. Zhurnal radioelektroniki, № 11, 2018 [Elektronniy resurs] Rezhym dostupu: http://jre.cplire.ru/jre/nov18/9/text.pdf (21.07.2019).

4. Fedorov E., Alrababah H., Nehad A. The distribution for mation method of reference patterns of vocal speech sounds. International Journal of Advanced Trends in Computer Science and Engineering. 2017. Vol. 6 (3), May - June, P. 35 – 39.

5. Ara Jullion A. Abello, Gabriele Francesca Y., Domingo, Maria Jamelina T. Joven, Samanta Alexis S. Malubay. Power Measurement Model Optimizationusing using MATLAB. International Journal of Advanced Trends in Computer Science and Engineering. 2019. Vol. 8, № 3, May – June. P. 538 – 542.

6. Bakiko V.M., Popovich P.V,. Shvaychenko V.B. Viznachennya zavadostiykosti kanalu zv'yazku za vipadkovogo vplivu zavad. Visnyk Nats. tehn. un-tu "HPI" : zb. nauk. pr. . – Kharkiv : NTU "HPI", 2018. № 14 (1290). S. 7 – 10.

7. Churyumov G., Tokarev V., Tkachov V., Partyka S. Scenario of Interaction of the Mobile Technical Objects in the Process of Transmission of Data Streams in Conditions of Impacting the Powerful Electromagnetic Field. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). 21-25 Aug. 2018. P. 183 – 186.

8. Serkov O. Breslavets V., Tolkachov M., Kravets V. Method of coding information distributed by wireless communication lines under conditions of interference. Advanced Information Systems. 2018. Vol. 2, No. 2. P. 145 – 148.

9. Serkov O.A., Churyumov G.I. On the issue of solving the problem of electromagnetic compatibility of the wireless telecommunication systems. Applied radio electronics. Sci. and Tech. Jour. 2017. Vol. 16, No. 3,4. P. 117 – 121.

10. Laptev O.A., Polovinkin I.M, Klyukovskiy D.V., Barabash A.O. Model poshuku zasobiv neglasnogo otrimannya informatsiyi na osnovi diferentsialnyh peretvoren. Sciences of Europe. Praha, Czech Republic. 2019. Vol. 1. No 43. P. 59 – 62.

11. Pukhov G.E. Differentsialnyie spektryi i modeli. K.: Naukova dumka, 1990. 188 s.

12. Laptev A.A., Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V. The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi. International Journal of Advanced Research in Science, Engineering and Technology. India. 2019. Vol. 6, Issue 7. P. 10101 – 10105.

13. Laptiev O.A., Voichenko T.O., Kudiukin P.V., Stepanenko V.I. Metod otsinky parametriv syhnalu zasobiv nesanktsionovanoho znimannia informatsii na osnovi koreliatsiino-rehresiinoho analizu. Naukovyi zhurnal "Naukoiemni tekhnolohii". K.: NAU, 2019. № 3 (43). S. 313 – 320.

14. Qualifying Requirements QR-160D (2004). Environmental Conditions and Test Procedures for Airborne Equipment, ARIAC. 2004.

15. Aaron Don M. Africa, Ara Jyllian A. Abello, Zendrel G. Gacuya, Isaiah Kyle A. Naco, Victor Antonio R. Valdes. Face Recognition Using MATLAB. International Journal of Advanced Trends in Computer Science and Engineering. 2019. Vol. 8, № 4. July-August. P. 1110 – 1116.

к.т.н., с.н.с. Лаптев А.А., к.ф.-м.н., доц. Собчук В.В., д.т.н., проф. Савченко В.А.

МЕТОД ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМЫ ОБНАРУЖЕНИЯ, РАСПОЗНАВАНИЯ И ЛОКАЛИЗАЦИИ ЦИФРОВЫХ СИГНАЛОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В процессе выявления, распознавания и локализации сигнала средств негласного получения информации в информационных системах актуальным вопросом является повышение помехоустойчивости. В статье исследованы особенности использования фильтров низкой частоты с квадратичной и линейной зависимостью отклика на входной сигнал. Показано, что принцип работы фильтров заключается в том, что выполняется процесс суммирования. При этом, полезный сигнал суммируется когерентно, а сигнал помехи – некогерентно, то есть полезный сигнал увеличивается, а сигнал помехи уменьшается. При воздействии на вход линейного и квадратичного фильтров прямоугольного импульса, который имитирует сигнал современных цифровых средств негласного получения информации, определены необходимые для дальнейшего использования параметры входных и выходных сигналов: математическое ожидание, коэффициент корреляции, дисперсия, среднеквадратическое отклонение, отношение сигнала к помехе во временном и спектральном виде. Вычислено коэффициент выигрыша, которой показывает эффективность использования фильтров низкой частоты. Приведены графики огибающей напряжения на выходе идеального полосового фильтра при воздействии на вход прямоугольного импульса с разной продолжительностью – сигнала средств негласного получения информации.

Проведено моделирование процесса фильтрации при разных коэффициентах корреляции. Это подтвердило возможность выделения сигнала средств негласного получения информации методом определения двухмерной плотности вероятности сигнала помехи на фоне общего сигнала. Исследуется процесс повышения помехоустойчивости системы в целом. Доказано, что использование в процессе обработки сигналов узкополосных фильтров низкой частоты позволяет добиться повышения помехоустойчивости системы определения, распознавания и локализации средств негласного получения информации на 23%.

Ключевые слова: помехоустойчивость, фильтр, математическое ожидание, дисперсия, моделирование.

PhD Laptev O., PhD Sobchuk V., Prof. Savchenko V.

A METHOD OF INCREASING THE IMMUNITY OF A SYSTEM FOR DETECTING, RECOGNIZING AND LOCALIZING DIGITAL SIGNALS IN THE INFORMATION SYSTEMS

In the process of detection, recognition, and localization of the single means of silent retrieval of information in information systems, the urgent issue is the increase of noise immunity. The article explores the features of using low-pass filters with a quadratic and linear response dependence on the input signal. It is shown that the principle of operation of the filters is that the summation process is performed. In this case, the useful signal is summed coherently, and the interference signal is incoherent, that is, the useful signal increases, and the interference signal decreases. When exposed to inputs, linear and quadratic filters, a rectangular pulse that simulates the signal of modern digital non-voice information, the parameters necessary for use in the future, such as mathematical expectation, correlation coefficient, variance, root mean square, the ratio of signals to interference in temporal and spectral form. We have determined a

payoff ratio that shows the efficiency of using low pass filters. The graphs of the envelope voltage at the output of the ideal bandpass filter when exposed to the input of a rectangular pulse - the signal of the means of silent information acquisition, with different duration.

The filtration process was simulated at different correlation coefficients, which confirmed the possibility of signal isolation of the means of silent information acquisition by the method of determining the two-dimensional probability density of the interference signal and the background of the general signal. The process of increasing the noise immunity of the system as a whole is considered, it is proved that the increase of noise immunity by 23 % of the system of identification, recognition and localization of the means of silent retrieval of information is achieved by using, in the process of signal processing, narrow-band filters of low frequency.

Keywords: noise immunity, filter, mathematical expectation, variance, modeling.

ЗАГАЛЬНІ ПИТАННЯ

УДК 355/359.08

к.т.н., доц. **Черних Ю.О.** (ВІ КНУ)
Черних О.Б. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-10

СИСТЕМА ПІДГОТОВКИ ОФІЦЕРСЬКИХ КАДРІВ У РЕСПУБЛІЦІ БІЛОРУСЬ

У статті проаналізовано досвід підготовки офіцерських кадрів для збройних сил республіки Білорусь. Проведено аналіз структури системи військової освіти збройних сил республіки Білорусь. Наведено основні нормативно-правові акти, на підставі яких організовано навчання. військових фахівців. Розглянуто мережу військових навчальних закладів для підготовки офіцерів тактичної, оперативно-тактичної та оперативно-стратегічної ланок військового управління. Означено відомості щодо ролі та міста цивільної університетської освіти і базової військової освіти у загальної системі підготовки військового фахівця.

Аналіз концепції, структури, цілей, змісту і технологій підготовки офіцерського складу в збройних силах Республіки Білорусь показує, що система військової освіти відображає сучасний етап розвитку збройних сил, а також національну культурну специфіку країни. Освіта і виховання офіцерських кадрів здійснюється на вітчизняних культурних і військових традиціях з урахуванням менталітету білоруського народу. Головним напрямком підготовки офіцерів є їх фундаментальна військово-професійна підготовка як у військовій, так і в цивільній сферах. В першу чергу, проводиться підготовка громадянина - патріота своєї батьківщини.

Зміст навчання офіцерів будується за двома сходами військової освіти. Кожна ступінь військової освіти закінчується отриманням певного рівня кваліфікації. Основними загальними тенденціями розвитку вищої білоруської військової школи є: поліпшення якості відбору абітурієнтів, індивідуалізація навчання курсантів і слухачів, стабілізація їх числа на сучасному рівні; подальша інформатизація навчального процесу, впровадження мультимедійних засобів навчання тощо.

Реформа вищої військової освіти в Білорусі триває в руслі загальноєвропейського розвитку. Однак, вона не встає на шлях простого копіювання військових освітніх моделей інших країн, а враховує досвід, традиції військової школи, національні особливості становлення і розвитку вітчизняних збройних сил.

Ключеві слова: збройні сили республіки Білорусь, система військової освіти, підготовка офіцерів, рівень підготовки.

Постановка проблеми. Творче використання міжнародного досвіду підготовки військових фахівців (ВФ) за кордоном набуває особливої актуальності в умовах подальшого реформування збройних сил (ЗС) України. Проводячи дослідження закордонного досвіду будівництва та реформування ЗС інших країн, у тому числі їхньої складової - системи військової освіти, бачимо, що в кожній країні він має специфічне національне підґрунтя. Водночас у військовій педагогічній практиці різних країн світу існують загальні методичні підходи, які доцільно враховувати і використовувати. На наш погляд, цікаво дослідити трансформацію та побудову систем військової освіти (СВО) ЗС країн, що раніш входили до складу колишнього Радянського Союзу, зокрема у збройних силах республіки Білорусь (РБ). У статті наведено аналіз досвіду підготовки офіцерів у ЗС республіки Білорусь, що виконаний під час проведення дослідження у рамках науково-дослідної роботи «Науково-організаційні засади проектування основних вимог до змісту підготовки офіцерських кадрів з вищою освітою для Збройних Сил України» (шифр - Підготовка-П).

Аналіз останніх досліджень і публікацій. Висвітленню досвіду підготовки військових фахівців для збройних сил інших країн присвячено низку публікацій вітчизняних та зарубіжних авторів, зокрема, Болгарії [1]; Великої Британії [2], країн Балтії [3, 4], Німеччини [5, 6, 7], Польщі [8], Сполучених Штатів Америки [9-11]; Франції [12, 13] та ін. Це пов'язано з тим, що підготовка військових фахівців у цих країнах відображає найхарактерніші риси

сучасного підходу до створення освітніх структур та їх функціонування. Разом з тим, слід зазначити, що незважаючи на різноманітність публікацій щодо систем військової освіти в інших країнах, у першу чергу, провідних країн-членів НАТО, дослідження сучасного стану системи військової освіти у ЗС Республіки Білорусь, у тому числі підготовки офіцерських кадрів, наражаються на такі проблеми: неповнота та недостатня аналітичність джерельної бази; нехтування необхідністю ґрунтовного вивчення досвіду підготовки військових фахівців у країнах, що мають невеликі за чисельністю ЗС тощо.

Метою статті є проведення аналізу сучасного стану підготовки офіцерських кадрів для ЗС республіки Білорусь для врахування її досвіду під час проведення подальшої реформи національної СВО.

Виклад основного матеріалу. Структура і зміст військової освіти в РБ мають загальні та особливі риси в порівнянні з системами військової освіти інших країн. Система підготовки військових фахівців являє собою ступеневу систему безперервного навчання військових кадрів, починаючи від початкової військової підготовки молоді, до навчання офіцерів оперативно-стратегічного рівня. Навчання на кожній із ступенів СВО завершується отриманням певних рівнів кваліфікації. Рівні кваліфікації є вирішальною умовою при розробці освітніх стандартів підготовки, навчальних планів і навчальних програм для відповідної ступені військової освіти.

Структурно підготовка військових фахівців містить такі складові: початкова військова підготовка молоді; професійна військова підготовка; вища освіта військових фахівців; підвищення кваліфікації та перепідготовка офіцерських кадрів.

Система вищої освіти військових фахівців РБ є складовою державної системи вищої освіти країни, основними завданнями якої є:

підготовка, перепідготовка та підвищення кваліфікації офіцерських кадрів, науково-педагогічних і наукових працівників вищої кваліфікації для збройних сил та інших військових формувань;

підготовка та підвищення кваліфікації офіцерів запасу, а також посадових осіб державних органів та інших організацій у сфері воєнної безпеки та оборони;

організація та проведення фундаментальних і прикладних наукових досліджень у сфері забезпечення національної безпеки держави.

Інтегрованість військової освіти в систему вищої освіти РБ визначається єдиною законодавчою базою, загальною структурою освіти та єдиними термінами навчання для одержання певного ступеня освіти, єдиними освітніми стандартами і вимогами, загальними методологічними вимогами до змісту програм навчання за спеціальностями підготовки.

Загальні вимоги до випускників вищих навчальних закладів РБ визначені на законодавчому рівні [14] та міністерством освіти РБ [15]: випускник повинен мати достатній рівень знань і вмінь у сфері соціально-гуманітарних, природознавчих, загальнопрофесійних і спеціальних навчальних дисциплін, а також дисциплін спеціалізації для здійснення соціально-професійної діяльності; випускник повинен уміти поповнювати свої знання, аналізувати історичні та сучасні проблеми соціально-економічного і духовного життя суспільства, знати ідеологію білоруської держави, моральні та правові норми, уміти враховувати їх у своїй професійній діяльності та життєдіяльності; випускник повинен володіти державними мовами (білоруською, російською), однією або декількома іноземними мовами.

Виходячи з цього, підготовка офіцерських кадрів для збройних сил здійснюється на підставі державного замовлення відповідно до кодексу РБ про освіту [14], з урахуванням специфічних особливостей військової професії, реальних матеріальних та фінансових ресурсів, які можуть бути виділені для цього, забезпечення соціального захисту офіцерів при звільненні їх у запас.

Відповідно до згаданого вище кодексу вища освіта підрозділяється на два щаблі. На І-ої ступені вищої освіти забезпечується підготовка фахівців, які володіють фундаментальними і спеціальними знаннями, вміннями і навичками, з присвоєнням кваліфікації спеціаліста з вищою освітою. Вища освіта І-ої ступені дає право на продовження освіти на ІІ-ої ступені

вищої освіти і на працевлаштування за отриманою спеціальністю (напрямку спеціальності, спеціалізації) та присвоєною кваліфікацією. Термін отримання вищої освіти І-го ступеня з денною формою навчання становить від 4-х до 5-ти років. На ІІ-ої ступені вищої освіти реалізується освітня програма вищої освіти ІІ-ого ступеня, що формує знання, вміння і навички науково-педагогічної та науково-дослідної роботи, або освітня програма вищої освіти ІІ-го ступеня з поглибленою підготовкою фахівця, які забезпечують отримання ступеня магістра. Термін отримання вищої освіти ІІ-го ступеня становить від одного року до двох років [14].

Освітні стандарти вищої освіти розробляються для кожної спеціальності (напряму спеціальності) і встановлюють вимоги до змісту професійної діяльності фахівця, його компетентностей, змісту навчально-програмної документації, рівню освіти осіб, які вступають на навчання для здобуття вищої освіти, форм і термінів здобуття певного ступеню вищої освіти, організації освітнього процесу, максимальному обсягу навчального навантаження студентів, курсантів, слухачів, рівня підготовки випускників, їх підсумкової атестації. Розробку освітніх стандартів вищої освіти організовує міністерство освіти і здійснює її спільно з навчально-методичними об'єднаннями в сфері вищої освіти та організаціями-замовниками кадрів. Освітні стандарти вищої освіти затверджуються міністерством освіти за погодженням із зацікавленими державними органами, в підпорядкуванні яких знаходяться установи вищої освіти і (або) для яких здійснюється підготовка кадрів.

Вища освіта військових фахівців – це ступенева освіта, що отримується на базі загальної середньої освіти у вищому військовому навчальному закладі (на військових факультетах цивільних університетів) за державною ліцензією на підготовку фахівців 2-х ступенів вищої освіти (спеціаліст (за Болонською системою - бакалавр) і магістр) та за освітніми програмами вищої освіти, які відповідають певним кваліфікаційним вимогам, передбачають державну атестацію випускників та отримання ними документа про освіту державного зразка (рис.1). Вимоги до змісту, обсягу, рівня підготовки військових фахівців встановлюються відповідно до потреб збройних сил та певних освітніх стандартів.

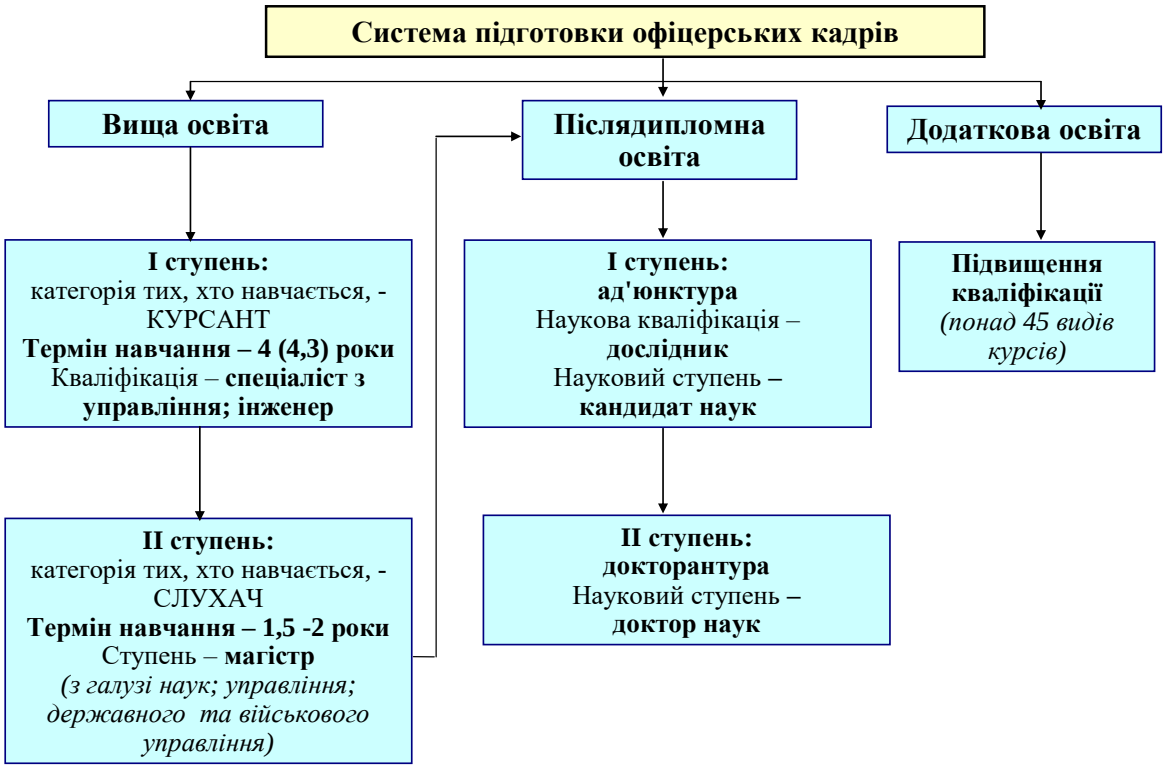


Рисунок 1 – Ступенева система підготовки офіцерських кадрів у РБ

Підготовка офіцерських кадрів *тактичного рівня військового управління* здійснюється, в основному, за встановленими спеціальностями у освітньої галузі «Військова справа» та у деяких цивільних освітніх галузях, у яких здійснюється підготовка фахівців з вищою освітою за спорідненими з військовими спеціальностями [16].

В освітній галузі «Військова справа» підготовка офіцерів проводиться у 4-х групах спеціальностей:

- управління підрозділами і забезпечення їх діяльності (включає 19 спеціальностей, випускник отримує кваліфікацію - спеціаліст з управління або інженер);
- військово-інженерна діяльність (включає 12 спеціальностей, випускник отримує кваліфікацію – інженер або спеціаліст з управління);
- військово-адміністративна діяльність в міжнародних відносинах, забезпечення управління військових формуваннями на оперативно-стратегічному рівні (включає 1 спеціальність, випускник отримує кваліфікацію, магістр державного та військового управління);
- «закрита група» (включає 11 спеціальностей).

Кожна з спеціальностей підготовки може мати від 2-х до 10-ти спеціалізацій. Термін підготовки на I ступені вищої освіти становить, як правило, 4 роки, на II ступені вищої освіти – до 2-х років.

За результатами реформування СВО, на теперішній час РБ має повний цикл підготовки офіцерських кадрів. Підготовка офіцерів для ЗС здійснюється за 123 спеціальностями та спеціалізаціями у військових та цивільних вищих навчальних закладах Білорусі. Загальний набір для підготовки офіцерських кадрів тактичної ланки військового управління у 2019 році становив 792 особи, у тому числі для збройних сил - 663 осіб; державного прикордонного комітету – 41 особа; внутрішніх військ міністерства внутрішніх справ – 72 особи, міністерства з надзвичайних ситуацій – 4 особи, міністерства внутрішніх справ – 12 осіб) [17].

На військових факультетах провідних цивільних університетів РБ (загальний набір на навчання у 2019 році склав 286 осіб) здійснюється підготовка таких спеціалістів: фахівців гуманітарного профілю, РХБЗ - військовий факультет Білоруського державного університету; фахівців зв'язку та інформаційних систем - військовий факультет Білоруського державного університету інформатики і радіоелектроніки; фахівців інженерних, автомобільних, бронетанкових військ, фінансової служби, промислового цивільного будівництва - військово-технічний факультет Білоруського національного технічного університету; фахівців транспортних військ - військово-транспортний факультет Білоруського державного університету транспорту; фахівців медичної служби - військово-медичний факультет Білоруського державного медичного університету; фахівців тилового профілю та фізичної підготовки - військовий факультет Гродненського державного університету; фахівців авіаційно-інженерного профілю - військовий факультет Білоруської державної академії авіації. Ті, хто навчаються на військових факультетах, мають статус курсанта [16].

Військова академія Республіки Білорусь є основним військовим навчальним закладом збройних сил [18]. Академію створено на базі двох училищ - Мінського вищого військового інженерного і Мінського вищого військового командного. На цей час Військова академія входить в число найбільших ВНЗ країни.

Підготовка офіцерів з вищою освітою здійснюється (рис. 2): на I-му ступені вищої освіти - за 24-ма спеціальностями; на II-му ступені вищої освіти - за 16-ма спеціальностями, в тому числі: в магістратурі з поглибленою підготовкою фахівців (практико орієнтовний напрям) - за 8-ма спеціальностями; в магістратурі з підготовки до науково-педагогічної діяльності (науково орієнтовний напрям) - за 8-ма спеціальностями.

На I-му ступені вищої освіти за очною формою навчаються курсанти (майбутні офіцери тактичного рівня військового управління). Термін навчання становить 4 роки. Випускникам присвоюється кваліфікація «спеціаліст з управління» або «інженер» (в залежності від спеціальності) і первинне офіцерське звання «лейтенант» (рис. 2).

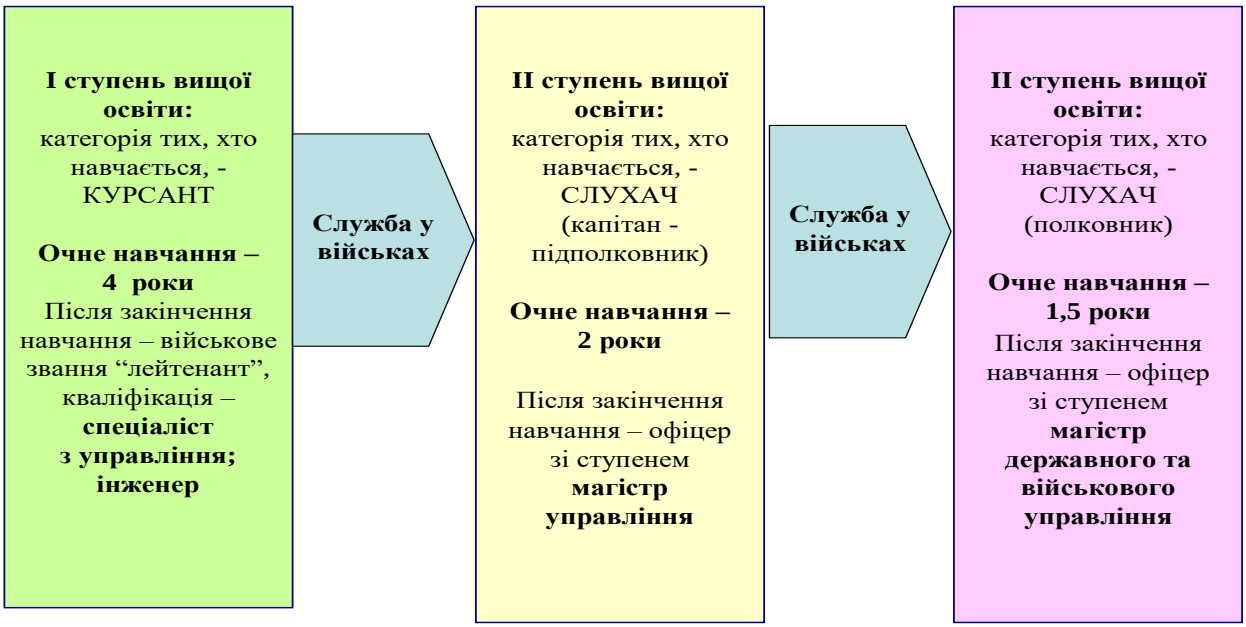


Рисунок 2 – Підготовка офіцерських кадрів командного фаху

Шість факультетів академії (загальновійськовий; зв'язку та автоматизованих систем управління; протиповітряної оборони; військової розвідки; авіаційний; внутрішніх військ) практично повністю забезпечують потребу збройних сил в офіцерських кадрах. Загальний набір на навчання у 2019 році склав 501 особу (в тому числі для збройних сил - 412 осіб; державного прикордонного комітету – 22 особи; внутрішніх військ міністерства внутрішніх справ – 63 особи, міністерства з надзвичайних ситуацій – 4 особи) [17].

Ті, хто навчаються в академії на цьому ступені, мають статус курсанта. Заняття з курсантами проводять понад 700 висококваліфікованих викладачів, з них 230 осіб мають наукові ступені та вчені звання, в тому числі 15 – вчене звання професора. Деякі з них мають почесні звання заслуженого діяча науки і техніки, заслуженого працівника вищої школи, заслуженого винахідника і раціоналізатора.

Академія має в своєму розпорядженні необхідну навчальну матеріально-технічну базу. У навчальних корпусах розміщені лекційні аудиторії, спеціалізовані класи, кабінети, лабораторії, які оснащені новітньою електронно-обчислювальною технікою. Бібліотека має достатню кількість примірників необхідної технічної та іншої спеціальної літератури, підручників та навчальних посібників, читальні зали для самостійної та позааудиторної роботи. Академія обладнана сучасними навчально-тренувальними комплексами і тренажерами. Відмінна спортивна база сприяє роботі багатьох спортивних секцій.

На загальновійськовому факультеті академії [19] здійснюється підготовка командирів мотострілецьких підрозділів (набір у 2019 році - 40 осіб); танкових підрозділів (набір у 2019 році - 20 осіб), командирів підрозділів ракетних військ та артилерії (набір у 2019 році – 40 осіб); фахівців тилу із забезпечення паливно-мастильними матеріалами (набір у 2019 році - 11 осіб); фахівців з ідеологічної роботи у військових підрозділах (набір у 2019 році – 16 осіб); військових психологів (набір у 2019 році - 14 осіб, у тому числі 3 жінки); фахівців з експлуатації наземних систем озброєння (артилерії та ракетного озброєння) - (набір у 2019 році - 28 осіб). До складу факультету входять: командування, батальйон курсантів і 6 кафедр: тактики (загальновійськових підрозділів); вогневої підготовки; побудови та експлуатації бронетанкового озброєння; тилового забезпечення; бойового застосування підрозділів ракетних військ і артилерії; побудови та експлуатації ракетно-артилерійського озброєння.

На факультеті зв'язку та автоматизованих систем управління [19] здійснюється підготовка військових зв'язківців (набір у 2019 році - 48 осіб, у тому числі 4 жінки); фахівців з автоматизованих систем обробки інформації (набір у 2019 році – 20 осіб); фахівців з експлуатації АСУ (набір у 2019 році - 16 осіб). До складу факультету входять: командування, батальйон курсантів, 2 кафедри: автоматизованих систем управління військами; зв'язку, а також навчальний польовий вузол зв'язку.

На факультеті протиповітряної оборони [19] навчаються фахівці з експлуатації радіотехнічних систем ППО (набір у 2019 році - 60 осіб). До складу факультету входять: командування, дивізіон курсантів та 3 кафедри: тактики і озброєння радіотехнічних військ; тактики і озброєння зенітних ракетних військ; тактики і озброєння ППО сухопутних військ.

На факультеті військової розвідки [19] здійснюється підготовка командирів підрозділів військових розвідників (набір у 2019 році - 14 осіб), командирів підрозділів спеціального призначення (набір у 2019 році - 25 осіб), командирів повітряно-десантних підрозділів (набір у 2019 році - 14 осіб), а також фахівців з радіоелектронної розвідки (набір у 2019 році – 13 осіб) та радіоелектронної боротьби (набір у 2019 році - 13 осіб). До складу факультету входять: командування, батальйон курсантів і 3 кафедри: розвідки та іноземних армій; радіоелектронної розвідки і радіоелектронної боротьби; сил спеціальних операцій і військової розвідки.

На авіаційному факультеті [19] проводиться підготовка військових льотчиків фронтової авіації (набір у 2019 році - 5 осіб), армійської авіації (набір у 2019 році – 7 осіб), фахівців з управління повітряним рухом та бойового управління авіацією (набір у 2019 році – 12 осіб), фахівців інженерно-авіаційної служби (набір у 2019 році - 25 осіб, у тому числі 4 жінки). До складу факультету входять: командування, батальйон курсантів; 2 кафедри: льотної підготовки та бойового застосування авіації; авіаційної техніки та озброєння; а також аеродромна база, де проводяться практичні заняття; льотно-методичний відділ, який організовує льотну і парашутно-десантну підготовку.

На факультеті внутрішніх військ [19] проходять навчання командири підрозділів внутрішніх військ (набір у 2019 році - 60 осіб). До складу факультету входять: командування, батальйон курсантів; 3 кафедри: оперативно-тактичної підготовки внутрішніх військ; спеціальних та інженерно-технічних дисциплін; юридичних дисциплін; а також науково-дослідна лабораторія, курси перепідготовки та підвищення кваліфікації, підрозділи забезпечення.

Вступники на навчання проходять конкурсний відбір, мета якого полягає у визначенні доцільності навчання кожного з них у військовому навчальному закладі. Для підготовки на первинні офіцерські посади до Військової академії та військових факультетів на конкурсній основі приймаються громадяни Білорусі, які мають загальну середню освіту, у віці від 17 років до 21 року, або які проходять строкову військову службу, службу в резерві, або які пройшли строкову військову службу (військову службу за контрактом) у віці не старше 23 років, або які проходять військову службу за контрактом, у віці не старші 25 років, придатні за станом здоров'я, професійно-психологічними показниками, фізичної підготовленості для проходження військової служби на певних офіцерських посадах за відповідними військово-обліковими спеціальностями.

Навчальний процес у Військовій академії та на військових факультетах організований поетапно. Протягом перших трьох місяців навчання курсанти опановують військову спеціальність в ході початкової професійної підготовки (навчальних зборів). У цей період проводяться навчальні заняття з тактики, тактико-спеціальної, вогневої та інженерної підготовки, а також інших дисциплін бойової підготовки. Особлива увага приділяється вивченню нормативних документів, законів, постанов уряду РБ, що визначають права і обов'язки курсантів та офіцерів, їх майнову та іншу відповідальність перед державою при звільненні зі збройних сил раніше терміну, встановленого контрактом на проходження військової служби (розміри грошової компенсації за навчання). Вивчаються структура системи підготовки офіцерів у вищому військовому навчальному закладі, варіанти реалізації

можливостей кожного з тих, хто навчається, у тому числі при виникненні проблем із засвоєння програми вищої школи. Фінальною частиною зборів є укладення контракту на навчання між кандидатом в курсанти та командуванням військового навчального закладу (військового факультету). Тільки після укладення контракту та прийняття військової присяги вступник переходить із категорії «кандидат в курсанти» в категорію «курсант».

Перші чотири семестри все курсанти навчаються за єдиною програмою вищої школи. Разом з цим, підготовка проводиться строго диференційовано за спеціальностями і спеціалізаціями, які передбачають різні ступені інтеграції в академічні програми вищої школи. Надалі поряд з отриманням знань з соціально-гуманітарних, загальнонаукових та загальнопрофесійних навчальних дисциплін курсанти удосконалюють свою військову підготовку із загальновійськових і спеціальних дисциплін. Під час їх вивченні курсанти навчаються керувати підрозділом відповідно до обраної спеціальності, вдосконалюють свою вогневу і тактичну виучку, вчаться водити бойові машини, в тому числі й автомобілі тощо. Починаючи з 3-го курсу навчання, курсанти проходять військові стажування (практики) у військових частинах на посадах сержантів та офіцерів.

Курсанту, який закінчив навчання на І-ому ступені вищої освіти, здав встановлені навчальною програмою іспити, пройшов атестацію до присвоєння першого військового звання офіцерського складу, присвоюється військове звання «лейтенант». Після завершення навчання випускники проходять військову службу на первинних офіцерських посадах. Загальний рівень підготовки випускників дозволяє призначати їх без додаткової підготовки на посади офіцерів до батальйонної (дивізійної) ланки, а також на певні посади у штабах військових частин і з'єднань. Найбільш обдаровані випускники академії, які виявили схильність до дослідницької діяльності, при наявності клопотання з боку їх наукових керівників, можуть направлятися для подальшого навчання на ІІ-ому ступені (до магістратури). У подальшому вони можуть проходити підготовку в ад'юнктурі академії.

Підготовка *офіцерів оперативно-тактичного рівня* (рис. 2) здійснюється, в основному, на факультеті генерального штабу Військової академії РБ за навчальними програмами підготовки офіцерського складу командно-штабного та інженерного профілю на ІІ-му ступені вищої освіти (підготовка магістрів). Термін навчання визначається відповідними програмами підготовки та становить до 2-х років.

До складу факультету генерального штабу входять 4 кафедри: військової стратегії; оперативного мистецтва і тактики; державного і військового управління; видів забезпечення.

Підготовка здійснюється за спеціальностями: «Управління з'єднаннями і частинами сухопутних військ» (в тому числі за спеціалізаціями: «Сухопутні війська», «Ракетні війська і артилерія», «Війська зв'язку», «Радіо- та радіотехнічна розвідка», «Радіоелектронна боротьба», «Інженерні війська», «Війська РХБЗ», «Військова і спеціальна розвідка», «Внутрішні війська», «Мобілізаційна робота у військах і військових комісаріатах»); «Управління з'єднаннями і частинами військ протиповітряної оборони»; «Управління з'єднаннями і частинами військово-повітряних сил»; «Управління технічним забезпеченням з'єднань і військових частин»; «Управління тиловим забезпеченням з'єднань і військових частин»; «Ідеологічна робота в з'єднаннях і військових частинах збройних сил». Загальний щорічний набір становить близько 80 осіб.

За окремими військовими спеціальностями підготовка білоруських офіцерів здійснюється у військових академіях Російської Федерації.

Підготовка *офіцерів оперативно-стратегічного рівня* (рис. 2) здійснюється на факультеті генерального штабу Військової академії Республіки Білорусь за спеціальністю «Військово-адміністративна діяльність в міжнародних відносинах, забезпечення управління військових формуваннями на оперативно-стратегічному рівні». Щорічний набір складає близько 10-12 слухачів. Окремі офіцери проходять підготовку в Академії генерального штабу збройних сил Російської Федерації.

Підготовка *офіцерських кадрів вищої наукової кваліфікації* (рис. 3) реалізується на 2-ох ступенях післядипломної освіти - в ад'юнктурі та докторантурі. В ад'юнктурі навчання

здійснюється за денною та заочною формами, а також у формі здобування наукового ступеню, в докторантурі – за денною формою та шляхом здобування наукового ступеню.

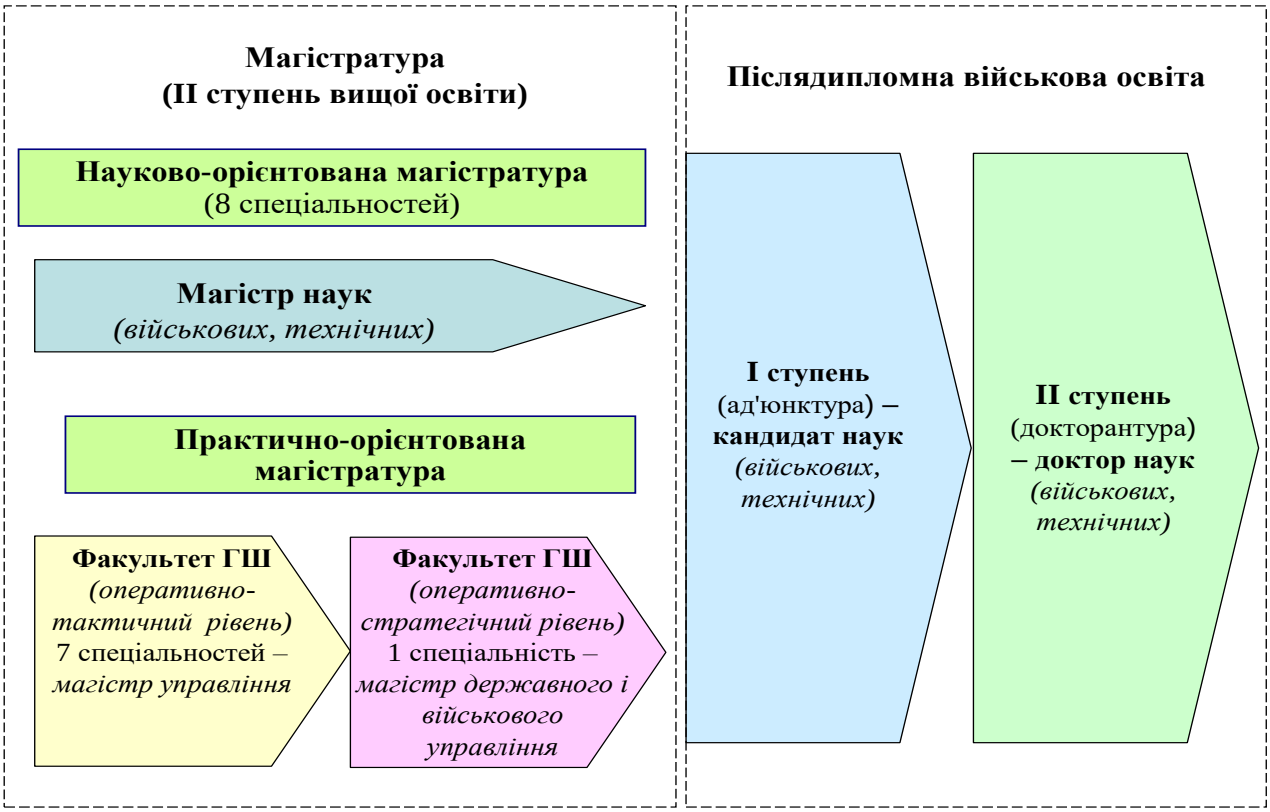


Рисунок 3 – Підготовка офіцерських кадрів вищої наукової кваліфікації

Підготовка в ад'юнктурі відкрита за 11-ма науковими спеціальностями, а в докторантурі - за 7-ма науковими спеціальностями. Терміни навчання в ад'юнктурі: денна форма - не більше 3 років; заочна форма - не більше 4 років; у формі здобування наукового ступеню - не більше 5 років. Освітня програма ад'юнктури забезпечує здобуття наукової кваліфікації «дослідник». Термін підготовки офіцера в докторантурі становить до 3-х років.

Підвищення кваліфікації та перепідготовка офіцерських кадрів здійснюються у Військової академії та інших вищих навчальних закладах на постійно діючих короткострокових курсах (понад 45 різних видів курсів). В основу системи підвищення кваліфікації покладається принцип підготовки офіцерів за посадовим призначенням, а при визначенні змісту навчання - принцип опори на знання та вміння, що їх набули офіцери під час навчання у вищих навчальних закладах та під час проходження військової служби. В основу змісту програм перепідготовки та підвищення кваліфікації військових фахівців покладається принцип безперервної військової освіти з максимальним забезпеченням відповідності рівня їх підготовки вимогам функціональних обов'язків згідно з посадовим призначенням.

З метою підготовки мобілізаційних ресурсів на військових факультетах і військових кафедрах певних цивільних вищих навчальних закладів здійснюється навчання студентів за програмами підготовки офіцерів запасу, а також молодших командирів (більш ніж за 50-ма військово-обліковими спеціальностями).

Підготовка офіцерів безпосередньо в процесі проходження військової служби проводиться в ході проведення зборів (методичних, командирських, за фахом); планових занять з предметів бойової підготовки (від командира взводу до командира батальйону, дивізіону, включно) і в системі професійно-посадової підготовки (в управліннях з'єднань і

військових частин); індивідуальної підготовки (в ході самостійної роботи, виконання індивідуальних завдань); при практичному виконанні обов'язків військової служби.

Висновки. Реформа вищої військової освіти в Білорусі триває в руслі загальноєвропейського розвитку. Однак, вона не встає на шлях простого копіювання військових освітніх моделей інших країн, а враховує досвід, традиції військової школи, національні особливості становлення і розвитку вітчизняних збройних сил.

За поглядами керівництва ЗС РБ [20], основними перевагами системи підготовки офіцерського складу є: можливість відстеження військовослужбовця на всіх етапах його службової діяльності, виявлення його нахилів і здібностей, а також економія державних коштів. Серед вад військової освіти Білорусі відмічаються такі: недостатність кваліфікованого викладацького складу, зокрема, відсутність офіцерів з досвідом служби у стратегічних ланках військового управління, а також миротворчої діяльності та участі в бойових діях; застаріла методологія в підходах до розвитку воєнної науки, що впливає на організацію навчального процесу; застарілі методики викладання навчальних дисциплін, особливо на командно-штабному факультеті та факультеті генерального штабу Військової академії.

ЛІТЕРАТУРА

1. Черних, Ю.О. Система підготовки офіцерських кадрів у збройних силах республіки Болгарія /Ю.О. Черних, О.Б. Черних //Зб. наук. праць ВІКНУ ім. Т. Шевченка. – 2018. – Вип. № 59. – С. 204-215.

2. Богунов, С.О. Основи організації та функціонування системи військової освіти Великобританії – аналітичний огляд /С.О. Богунов, Ю.О. Черних, О.Б. Черних //*Військова освіта.* – 2017.- № 2 (36). – С. 234-245.

3. Богунов, С.О. Організація підготовки офіцерів для збройних сил республіки Литва /С.О. Богунов, Ю.О. Черних, О.Б. Черних //Військова освіта. – 2018. – № 1 (37). – С. 272-285.

5. Мітягін, О.О. Система підготовки військових фахівців у збройних силах країн Балтії: досвід для України» // О.О. Мітягін, О.Б. Черних, Ю.О. Черних //*Науковий вісник інноваційних технологій.* – 2018. – № 1(17). – С. 49-61.

5. Гацко М. Профессиональная подготовка унтер-офицеров и сержантов в зарубежных армиях / М. Гацко *// Зарубежное военное обозрение.* – 2009. – № 5. – С. 21-28.

6. Лазукин, В. Подготовка офицерских кадров в ВС ФРГ /В. Лазукин // *Зарубежное военное обозрение.* – 2008. – № 2. – С. 26-30.

7. Черних, Ю.О. Основи організації та функціонування системи військової освіти Німеччини – аналітичний огляд» /Ю.О. Черних, О.Б Черних//*Зб. наук. праць ВІКНУ ім. Т. Шевченка.* – 2017. – вип. № 57. – С. 238-248.

8. Черних, О.Б. Аналіз сучасного стану системи військової освіти республіки Польща: досвід для України /О.Б. Черних, О.О. Мітягін, Ю.О. Черних //*Військова освіта.*– 2017. – № 1 (35). – С. 200-208.

9. Владимирова, С. Исследования в области совершенствования профессионализма личного состава вооруженных сил США /С. Владимирова, А. Стрелецкий // *Зарубежное военное обозрение.* – 2006. – № 5. – С. 15-19.

10. Приходько, Ю.І. Підготовка військових фахівців у провідних країнах світу: основоположні засади та тенденції /Ю.І. Приходько //*Педагогічні науки: теорія, історія, інноваційні технології.* – 2017. – № 3 (67). – С. 285-299.

11. Толок, І.В. Особливості підготовки військових фахівців тактичного рівня у ВВНЗ США та окремих країн НАТО / І.В. Толок, Ю.М. Супрунов //*Військова освіта.* – 2018. – № 1 (37) – С. 259-271.

12. Колесов, П. Сен-Сирская специальная военная школа вооруженных сил Франции /П. Колесов, А. Стрелецкий //Зарубежное военное обозрение. –2006. – № 6. – С. 26-32.

13. Черних, Ю.О. Основи організації та функціонування системи військової освіти Франції – аналітичний огляд /Ю.О. Черних, О.Б. Черних //*Зб. наук. праць ВІКНУ ім. Т. Шевченка.* – 2017. – Вип. № 56. – С. 249-257.

14. Кодекс Республики Беларусь об образовании: с изм. и доп. по состоянию на 21 сент. 2016 г. - Минск: Нац. центр правовой информ. Респ. Беларусь, 2016.

15. Постановление министерства образования Республики Беларусь от 28 февраля 2001 г. № 16 Об утверждении и введении в действие руководящего документа Республики Беларусь «Система стандартов в сфере образования. Система оценки соответствия. Порядок предоставления статусов

высшим учебным заведениям» [Електронний ресурс] /Режим доступу/ http://pravo.by/document/?guid=3871&p0=W20105201.

16. Военное образование в Республике Беларусь [Електронний ресурс] /Режим доступу/ https://www.mil.by/ru/education/.

17. Контрольные цифры приема граждан в учреждения образования Республики Беларусь, в которых осуществляется подготовка кадров для вооруженных сил, других войск и воинских формирований Республики Беларусь, в 2019 году [Електронний ресурс] /Режим доступу/ https://www.mil.by/ru/education/priem/.

18. Об образовании Военной академии Республики Беларусь: Указ Президента Республіки Беларусь, 17 мая 1995 г., № 192.

19. Информация о факультетах и перечень специальностей [Електронний ресурс] /Режим доступу/ https://varb.mil.by/faculties/.

20. Пузиков, М.В. Система военного образования в Республике Беларусь : актуальные вопросы функционирования и направления совершенствования / М. В. Пузиков // Армия. - 2013. - №1-2. - С. 26 - 31.

REFERENCES:

1. Chernykh, Yu.O., Chernykh, O.B.,. (2018). Systema pidhotovky ofitserskykh kadriv u zbroynykh sylakh respubliky Bolhariya [Officer training system in the armed forces of the republic of Bulgaria]. Zb. nauk. prats VIKNU im. T. Shevchenka, 59, 204-215. (in Ukrainian).

2. Bohunov, S.O., Chernykh, Yu.O., Chernykh, O.B. (2017). Osnovy orhanizatsiyi ta funktsionuvannya systemy viyskovoyi osvity Velykobrytanyy - analitychnyy ohlyad [Basics of organization and functioning of the Great Britain military education system - analytical review]. Military education, 2 (36), 234-245. (in Ukrainian).

3. Bohunov, S.O., Chernykh, Yu.O., Chernykh, O.B. (2018). Orhanizatsiya podhotovky ofitseriv dlya zbroynykh syl respubliky Lytva [Organisation of officer training for the armed forces of the republic of Lithuania]. Military education, 1 (37), 272-285. (in Ukrainian).

4. Mityahin, O.O., Chernykh, O.B., Chernykh, Yu.O. (2018). Systema pidhotovky viyskovykh fakhivtsiv u zbroynykh sylakh krayin Baltiyi: dosvid dlya Ukrayiny [Educational system for military specialists in the armed forces of the Baltic countries: experience for Ukraine].Scientific Bulletin of innovative technologies, 1(17), 49-61. (in Ukrainian).

5. Gatsko, M. (2009). Professional'naya podgotovka unter-ofitserov i serzhantov v zarubezhnykh armiyakh [Professional training of non-commissioned officers and sergeants in foreign armies]. Foreign military review, 5, 21-28. (in Russian).

6. Lazukin, V. (2008). Podgotovka ofitserskikh kadrov v VS FRG [Training of officer cadres in the Armed Forces of the FRG]. Foreign military review, 2, 26-30. (in Russian).

7. Chernykh, Yu.O., Chernykh, O.B.,. (2017). Osnovy orhanizatsiyi ta funktsionuvannya systemy viyskovoyi osvity Nimechchyny – analitychnyy ohlyad [Basics of organization and functioning of the Germany military education system - analytical review] Zb. nauk. prats VIKNU im. T. Shevchenka, 57, 238-248. (in Ukrainian).

8. Chernykh, O.B.,. Mityahin, O.O,. Chernykh, Yu.O, (2017). Analiz suchasnoho stanu systemy viyskovoyi osvity respubliky Polshcha: dosvid dlya Ukrayiny [The current state analysis of the military education system of the republic of Poland: experience for Ukraine]. Military education, 1 (35), 200-208. (in Ukrainian).

9. Vladimirova, S., Streletskiy,A. (2006). Issledovaniya v oblasti sovershenstvovaniya professionalizma lichnogo sostava vooruzhennykh sil SSHA [Studies in the field of improving the professionalism of the personnel of the US armed forces]. Foreign military review, 5, 15-19. (in Russian).

10. Prykhodko, Yu.I., (2017). Pidhotovka viyskovykh fakhivtsiv u providnykh krayinakh svitu: osnovopolozhni zasady ta tendentsiyi [Training of military specialists in leading countries of the world: fundamental principles and trends]. Pedagogical sciences: theory, history, innovative technologies, 3 (67), 285-299. (in Ukrainian).

11. Tolok, I.V., Suprunov Yu.M. (2018). Osoblyvosti pidhotovky viyskovykh fakhivtsiv taktychnoho rivnya u VVNZ SSHA ta okremykh krayin NATO [Peculiarities of training of tactical-level military specialists]. Military education, 1 (37), 259-271. (in Ukrainian).

12. Kolesov, P., Streletskii, A. (2006). Sen-Sirskaya spetsial'naya voyennaya shkola vooruzhennykh sil Frantsii [Saint-Sire Special Military School of the French Armed Forces]. Foreign military review, 6, 26-32. (in Russian).

13. Chernykh, Yu.O., Chernykh, O.B.,. (2017). Osnovy orhanizatsiyi ta funktsionuvannya systemy viyskovoyi osvity Frantsiyi – analitychnyy ohlyad [Basics of organization and functioning of the French military education system - analytical review]. Zb. nauk. prats VIKNU im. T. Shevchenka, 56, 249-257. (in Ukrainian).

14. Kodeks Respubliki Belarus' ob obrazovanii: s izm. i dop. po sostoyaniyu na 21 sent. 2016 g. - Minsk: Nats. tsentr pravovoy inform. Resp. Belarus', 2016. (in Russian).

15. Postanovleniye ministerstva obrazovaniya Respubliki Belarus' ot 28 fevralya 2001. „Ob utverzhdenii i vvedenii v deystviye rukovodyashchego dokumenta Respubliki Belarus' „Sistema standartov v sfere obrazovaniya. Sistema otsenki sootvetstviya. Poryadok [Decree of the Ministry of Education of the Republic of Belarus dated February 28, 2001, 16. On Approval and Enactment of the Guiding Document of the Republic of Belarus“ System of Standards in the field of Education. Conformity assessment system. The procedure for granting statuses to higher educational institutions] Available at: http://pravo.by/document/?guid=3871&p0=W20105201. (in Russian).

16. Voyennoye obrazovaniye v Respublike Belarus' [Military education in the Republic of Belarus] Available at: https://www.mil.by/ru/education/.(in Russian).

17. Kontrol'nyye tsifry priyema grazhdan v uchrezhdeniya obrazovaniya Respubliki Belarus', v kotorykh osushchestvlyayetsya podgotovka kadrov dlya vooruzhennykh sil, drugikh voysk i voinskikh formirovaniy Respubliki Belarus', v 2019 godu [Benchmarks for admitting citizens to educational institutions of the Republic of Belarus, in which personnel are trained for the armed forces, other troops and military units of the Republic of Belarus, in 2019] Available at: https://www.mil.by/ru/education/priem/. (in Russian).

18. Ob obrazovanii Voyennoy akademii Respubliki Belarus' [On the formation of the Military Academy of the Republic of Belarus:] Ukaz Prezidenta Resp. Belarus', 17 maya 1995 g., (in Russian).

19. Informatsiya o fakul'tetakh i perechen' spetsial'nostey [Information about faculties and a list of specialties] Available at: https://varb.mil.by/faculties/. (in Russian).

20. Puzikov, M.V., (2013). The military education system in the Republic of Belarus: current issues of functioning and the direction of improvement [The military education system in the Republic of Belarus: current issues of functioning and the direction of improvement] /M.V. Puzikov// *Arm*, 1-2, 26 – 31. (in Russian).

Ph.D.Chernykh J, Chernykh O.

OFFICER TRAINING SYSTEM IN THE ARMED FORCES OF THE REPUBLIC OF BELARUS

Analysis of the foreign experience of the organisation and reformation of the armed forces in other countries, with the respective systems of military education being an integral part, reveals the specific national aspect of such activities in each country. In the meantime, there are some general methodological approaches used in military pedagogic practice across different countries of the world to be practicably considered and applied.

The article examines the experience of officers' training for the armed forces of the Republic of Belarus. The article provides information on the existing network of military educational institutions for the officer training of tactical, operational-tactical and operational-strategic level of military command. Requirements for admission to military educational institutions for the officer training of different levels of training has been given. The terms of military specialists' training on tactical, operational-tactical and operational-strategic level have been defined. The analysis of the content of officer training for different armed services of the armed forces and different levels of military administration has been conducted.

We used the system of the general scientific methods of theoretical and empirical research, in particular, the theoretical-methodological analysis of the problem and the relevant scholarly resources, systematization and generalization of the scientific information pertaining to the essence and content of the set objectives, monitoring of the existing system of military specialists training in the Armed Forces of the republic of Belarus, scientific generalisation, the general scientific methods of logical and comparative analysis, systems approach, peer review, analysis and interpretation of the obtained theoretical and empirical data.

An analysis of the concept, structure, goals, content and technologies of officers' training inthe armed forces of the Republic of Belarus shows that the military education system reflects the current stage of development of the armed forces, as well as the national cultural specificity of the country. Education and training of officers is carried out on the basis of national cultural and military traditions, taking into account the mentality of the Belarusian people. The main direction of officers' training is their

fundamental military and professional training in both the military and civilian fields. First of all, the training of the citizen – patriot of his homeland is carried out.

The content of the officers' training is based on two military education levels. Each level of military education ends with a certain level of qualification. It is possible to distinguish the general tendencies of development of the higher Belarusian military school: improvement of the quality of applicants' selection, individualization of training of cadets and trainees, stabilization of their number at the present level; further informatization of the educational process, introduction of multimedia learning tools. The reform of higher military education in Belarus continues in line with pan-European development. However, it does not embark on the path of simply copying military educational models of other countries, but takes into account the experience, traditions of the military school, national peculiarities of formation and development of national armed forces. Certainly, the positive elements of the experience of the Belarusian army can be used in the training of officers in the Ukrainian Armed Forces under the conditions of gradual transition to the recruitment on a contract basis.

Key words: military education system; the armed forces of Belarus; officer training experience.

ДАНІ ПРО АВТОРІВ

Барабаш Олег Володимирович, доктор технічних наук, професор, завідувач кафедри вищої математики Державного університету телекомунікацій, https://orcid.org 0000-0003-1715-0761.

Бойчук Антоніна Анатоліївна, кандидат економічних наук, завідувач кафедри підприємництва та спеціальних дисциплін Хмельницького навчально-наукового інституту Тернопільського національного економічного університету, https://orcid.org/0000-0001-6701-6419.

Бойчук Вадим Олександрович, кандидат технічних наук, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0002-7584-6153.

Бойчук Марія Вадимівна, магістрант кафедри інженерії програмного забезпечення Хмельницького національного університету, https://orcid.org/0000-0002-9560-7854.

Бурдюг Олег Володимирович, науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка.

Ванієв Пулат Шевкетович, курсант Військового інституту Київського національного університету імені Тараса Шевченка спеціальність Геодезія та землеустрій, спеціалізація Геоінформаційні системи і технології, https://orcid.org/0000-0001-9999-5017.

Вдовенко Сергій Григорович, полковник, магістр державного військового управління в сфері оборони, доцент кафедри зв'язку та автоматизованих систем управління Інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0001-8139-7975.

Галахов Євген Миколайович, старший викладач кафедри вищої математики Державного університету телекомунікацій.

Даник Юрій Григорович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, https://orcid.org/0000-0001-6990-8656.

Дружинін Володимир Анатолійович, доктор технічних наук, професор, професор кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-5340-6237.

Жиров Генадій Борисович, кандидат технічних наук, старший науковий співробітник, доцент кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-7648-7992.

Зацерковний Віталій Іванович, доктор технічних наук, завідуючий кафедри геоінформатики ННІ «Інститут геології» Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0003-2346-9496.

Індутний Дмитро Григорович, курсант Військового інституту Київського національного університету імені Тараса Шевченка спеціальність Геодезія та землеустрій, спеціалізація Геоінформаційні системи і технології, https://orcid.org/0000-0002-4122-3994.

Кольцов Руслан Юрійович, кандидат технічних наук, доцент кафедри геоінформаційних систем і технологій Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-8441-9575.

Комарова Лариса Олексіївна, доктор технічних наук, старший науковий співробітник, професор кафедри «Телекомунікації» ОНАЗ ім. О.С. Попова, Одеса, https://orcid.org/0000-0002-9776-0879.

Костенко Олена Михайлівна, доктор технічних наук, професор, Полтавська державна аграрна академія, https://orcid.org/0000-0001-5997-342X.

Кошовий Микола Дмитрович, доктор технічних наук, професор, Лауреат Державної премії України в галузі науки і техніки, завідувач кафедри інтелектуальних вимірювальних

систем та інженерії якості, Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», http://orcid.org/0000-0002-9465-4467.

Лаптєв Олександр Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри систем інформаційного та кібернетичного захисту Державного університету телекомунікацій, https://orcid.org/0000-0002-4194-402X.

Лєнков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-7689-239X.

Муратов В.В., аспірант кафедри інтелектуальних вимірювальних систем та інженерії якості, Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», https://orcid.org/0000-0001-7684-5649.

Мясіщев Олександр Анатолійович, доктор технічних наук, професор, завідувач кафедри "Комп'ютерні системи та мережі", Хмельницький національний університет, https://orcid.org/0000-0003-1269-425X.

Пампуха Ігор Володимирович, кандидат технічних наук, доцент, начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-4807-3984.

Савков Павло Анатолійович, кандидат технічних наук, начальник кафедри геоінформаційних систем і технологій Військового інституту Київського національного університету імені Тараса Шевченка https://orcid.org/0000-0002-0197-0610.

Савченко Віталій Анатолійович, доктор технічних наук, професор, директор навчально-наукового інституту захисту інформації Державного університету телекомунікацій, http://orcid.org/0000-0002-3014-131X.

Сєлюков Олександр Васильович, доктор технічних наук, старший науковий співробітник, заступник директора ТОВ «Укрспецконсалтинг», https://orcid.org/0000-0001-7979-3434.

Синявська Ірина Костянтинівна, ад'юнкт (штатний) науково-організаційного відділення Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-2645-994X.

Собчук Валентин Володимирович, кандидат фізико-математичних наук, доцент, доцент кафедри вищої математики Державного університету телекомунікацій, http://orcid.org/0000-0002-4002-8206.

Цьопа Наталія Володимирівна, кандидат технічних наук, доцент кафедри технічної кібернетики факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». https://orcid.org/0000-0002-3215-0711.

Черних Ольга Борисівна, старший науковий співробітник науково-дослідного відділу військової освіти і науки центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняхівського, https://orcid.org/0000-0001-9865-5598.

Черних Юрій Олексійович, кандидат технічних наук, доцент, Заслужений працівник освіти, провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-0780-6627.

Четверіков Іван Олександрович, кандидат технічних наук, доцент, доцент кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка.

АЛФАВІТНИЙ ПОКАЗЧИК

УВАГА!

Редакційна колегія «Збірника ВІКНУ» здійснює незалежне («сліпе») експертне рецензування наданих до друку рукописів та перевірку їх на плагіат. Рецензування здійснюється за анонімною формою як для авторів, так і для рецензентів.

УВАГА! ЗМІНИЛИСЯ ВИМОГИ ДО ОФОРМЛЕННЯ СТАТЕЙ!
(Статті, що не відповідають вимогам, прийматися до розгляду не будуть!)

ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

Обов'язкові елементи статті – УДК, назва статті, анотація трьома мовами, вступ та постановка задачі (проблеми), виклад основного матеріалу, висновки, список літератури (References), дані про авторів трьома мовами.

Загальні вимоги до технічного оформлення статей:

Обсяг рукопису – не менше 4 повних аркушів українською, англійською або російською мовами.

Формат аркуша - **А4 (210 х 297 мм)**.

Розмір полів: верхнє, нижнє, праве, ліве – **2 см.**

Основний шрифт – **Times New Roman №12,** через міжрядковий інтервал - **1,0.** Абзац має становити **10 мм.**

Основний текст статті повинен мати такі необхідні елементи:

постановка задачі чи проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано **розв'язання даної проблеми** і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання цілей статті;

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

висновки з даного дослідження і перспективи подальшого розвитку у даному напрямку.

Анотація до статті виконується українською, англійською та російською мовами. Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (3-5 термінів).

Якщо основною мовою статті є українська або російська, то анотація англійською мовою повинна бути розширеною та мати загальний обсяг не менш ніж **1800** знаків, включаючи ключові слова.

Якщо основною мовою статті є англійська, то анотація українською мовою повинна бути розширеною та мати загальний обсяг не менш ніж **1800** знаків, включаючи ключові слова.

Список літератури (References) повинен включати не менш 12 джерел, з яких 50% видані за останні 10 років. При цьому не менш 25 % джерел повинно відноситися до іноземної періодики. Самоцитування авторів у списку літератури не повинно бути, як правило, більш за 15 %.

Якщо основною мовою статті є українська або російська, то оформлюються два списки літератури:

перший (список літератури на мові оригіналу джерела) – згідно наказу МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

На адресу редколегії (03680. м. Київ, вул Ломоносова 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:

рецензія відомого в Україні фахівця в конкретній предметній галузі, оформлена встановленим порядком, сканкопія - на електронну адресу редакції;

експертний висновок, завірений печаткою, про можливість відкритого публікування.

У відомостях про авторів (українською, російською та англійською мовами) наводиться:

– прізвище, ім’я та по батькові;

– науковий ступінь, вчене звання, посада;

– назва установи, де працює автор, її місце розташування (місто, країна);

– обліковий запис автора ORCID (повинен відображати назву установи, де працює автор, та його наукові публікації);

– адреса електронної пошти.

Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

– запис завжди починається з прізвища автора, потім, через кому, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються «and» без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлено «and» без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводять у "лапках";

– назва журналу або книги завжди виділяється курсивом;

– ім'я видавця вказується перед місцем видання;

– коми використовують для поділу елементів запису;

– для джерел українською або російською мовою, що наводяться у References, назви статей журналів, глав в книгах наводять латиницею (транслітерацією) у "лапках" та перекладом на англійську мову у квадратних дужках. Онлайн-конвертер з української мови для транслітерації: http://translit.kh.ua/?passport.

Приклади оформлення References за стилем Harvard British Standards Institution

Книга (ДСТУ 8302:2015)

Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х.: Вид. Рожко С. Г., 2017. 276 с.

Книга (Harvard style BSI)

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), ”Informatsiino-psykholohichna borotba u voiennii sferi: monohrafiia” [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

Стаття із періодичного видання (ДСТУ 8302:2015)

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75-78.

Стаття із періодичного видання (Harvard style BSI)

Karpenko, D.V. (2017),"Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75-78.

Дисертація (ДСТУ 8302:2015)

Белозеров, И.В. Религиозная политика: дис. … канд. ист. наук: 07.00.02; защищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

Дисертація (Harvard style BSI)

Belozerov, I.V. (2002),"Relyhyoznaia polytyka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7-15. Режим доступу до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7-15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution наведено на сайті ***Національної бібліотеки України імені В. І. Вернадського*** та онлайн генератора посилань ***Cite This For Me***.

Редакційна колегія: e-mail: lenkov_s@ukr.net

Шрифт

СХЕМА ОФОРМЛЕННЯ СТАТЕЙ У «ЗБІРНИК ВІКНУ»

УДК

науковий ступінь, вчене звання
ініціали та прізвище автора (співавторів)
Місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. **Степанов С.В.** (ВІКНУ)
к.т.н., с.н.с. **Українець О.В.** (ВІКНУ)
к.т.н. **Саленко В.Д.** (ВІКНУ)

12 пт жирний

КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ ЖЕСТІВ

11 пт *курсив, жирний*

Для керування електронними пристроями, для сучасного користувача важливими критеріями є такі, як: зручність та простота керування. Для того щоб надати користувачу такі можливості та зручності в використанні, є досить доцільною розробка системи, яка б надавала такі можливості. Керування системою, яка працює на основі жестів, є надзвичайно перспективним, та може суттєво полегшити користувачу роботу з нею, тому що, жести які потрібні для керування системою, можуть бути інтуїтивно зрозумілими користувачу, порівняно з іншими системами які працюють за допомогою комбінацій клавіш.

Для вирішення задач керування за допомогою жестів, пропонується програмно-апаратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу виконує відповідну роль в системі, наприклад знаходить точку інтересу з множини чи вираховує глибину сцени. Також в системі є ядро, яке відповідає за аналіз модифікаторів та жестів. На основі даних модулів стає можливо створити систему, яка б працювала на основі жестів. Але для створення даної системи, потрібно вирішити певні задачі, такі як: сегментація, скелетизація, спостереження. Кожна з яких містить в собі відповідні математичні моделі та визначення. Запропонований програмно-апаратний комплекс для керування природніми жестами. Суть програмно-апаратного комплексу полягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував роботу знаходячись частково віддалено від робочого місця, чи маніпулював інструментами на відстані, тобто за допомогою жестів. Використання пропонованого програмно-апаратного комплексу дозволить покращити показники стерильності в операційних, підвищити технічну безпеку під час виконання безпосередньої роботи користувача з приладами.

Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, точка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, спостереження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ

12 пт

НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ: постановка проблеми (задачі) **у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;** аналіз останніх досліджень **і публікацій, в яких започатковано** розв'язання даної проблеми **і на які спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується дана стаття, формулювання цілей статті (**постановка завдання**), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих** наукових результатів**;** їх практичного значення та результатів експерименту чи впровадження; висновки **з даного дослідження і перспективи подальших досліджень у даному напрямку. Література.**

Таблиці

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно розміщувати по

Рисунки

центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт – **Times New Roman № 12**). Рисунки повинні бути виконані за допомогою редактора **Word,** згруповані і являти собою один графічний об'єкт. Формули та позначення по тексту обов'язково набирати за допомогою **Equation Editor** - редактора формул **Word**, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний – **12 pt**. великі індекси – **10 pt** , малі індекси – **7 pt**, великі символи – **14 pt**. малі символи – **10 pt**: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт **Times New Roman**, для решти стилів – шрифт **Symbol**, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно наказу МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 пт **ЗРАЗОК**

1. Лєнков С.В., Толок І.В., Цицарєв В.М., Лєнков Є.С. Моделювання процесів витрачання та поповнення ресурсу угрупування технічних об’єктів. *Системи озброєння і військова техніка*. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Лєнков Є.С., Цицарєв В.М., Проценко Я.М. Моделювання процесу відмов об’єктів, що відновлюються з ієрархічною конструктивною структурою. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

ЗРАЗОК

11 пт

1. Ljenkov, S.V., Tolok, I.V., Tsytsarev, V.N. and Ljenkov, Ye.S. (2018), “Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv” [Modeling of processes of expenditure and resource replenishment grouping of technical objects], Systems of Arms and Military Equipment, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Ljenkov, Je.S., Cycarjev, V.M. and Procenko, Ja.M. (2017), “Modeljuvannja procesu vidmov ob’jektiv, shho vidnovljujut'sja z ijerarhichnoju konstruktyvnoju strukturoju” [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 55, pp. 30-39.

Рецензент: д.т.н., проф. ПІБ (вказується посада, кафедра, університет)

ЗРАЗОК

11 пт **Рецензент: д.т.н, проф. Сіроокий В.В.,** провідний науковий співробітник кафедри інформаційних технологій Київського національного університету імені Тараса Шевченка

Російською мовою ЗРАЗОК

11 пт ***курсив, жирний***

д.т.н., проф. Степанов С.В., к.т.н., с.н.с. Украинец О.В., к.т.н. Саленко В.Д.

УПРАВЛЕНИЕ ЭЛЕКТРОННЫМИ УСТРОЙСТВАМИ С ПОМОЩЬЮ ЖЕСТОВ

Для управления электронными устройствами, для современного пользователя важными критериями являются такие, как: удобство и простота управления. Для того чтобы предоставить пользователю такие возможности и удобства в

использовании, достаточно целесообразной разработка системы, которая бы предоставляла такие возможности. Управление системой, которая работает на основе жестов, чрезвычайно перспективным и может существенно облегчить пользователю работу с ней, потому что, жесты, которые нужны для управления системой, могут быть интуитивно понятными пользователю, по сравнению с другими системами работающих с помощью комбинаций клавиш.

Для решения задач управления с помощью жестов, предлагается программно-аппаратный комплекс, который построен на основе различных модулей, каждый из которых в свою очередь выполняет соответствующую роль в системе, например, находит точку интереса из множества или высчитывает глубину сцены. Также в системе есть ядро, которое отвечает за анализ модификаторов и жестов. На основе данных модулей становится возможно создать систему, которая бы работала на основе жестов. Но для создания данной системы, нужно решить определенные задачи, такие как: сегментация, скелетизации, наблюдения. Каждая из которых содержит в себе соответствующие математические модели и определения. Предложенный программно-аппаратный комплекс для управления природными жестами. Суть программно-аппаратного комплекса заключается в том, чтобы обеспечить пользователя таким интерфейсом, чтобы он выполнял работу находясь частично удалено от рабочего места, или манипулировал инструментами на расстоянии, то есть с помощью жестов. Использование предлагаемого программно-аппаратного комплекса позволит улучшить показатели стерильности в операционных, повысить техническую безопасность при выполнении непосредственной работы пользователя с приборами.

Ключевые слова: искусственный интеллект, контроллеры, модули, жесты, глубина сцены, точка интереса, анализ модификаторов, анализ жестов, сегментация, скелетизации, наблюдения.

Анотація англійською мовою повинна бути розширеною та мати зальний обсяг не менш 1800 знаків.

Англійською мовою ЗРАЗОК

11 пт курсив, жирний

Prof. Stepanov S.V., Ph.D. Ukrainets O.V., Ph.D. Salenko V.D.

CONTROL ELECTRONIC DEVICES USING GESTURES

For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene. Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.

Keywords: artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.

Дані про авторів (прізвище, ім'я по батькові, науковий ступінь, вчене звання, місце роботи) наводяться трьома мовами: українською, російською, англійською), ORCID (https://orcid.org)

ЗРАЗОК

11 пт

Степанов Сергій Вікторович, доктор технічних наук, професор, головний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1202-6512-1234

Українець Олексій Васильович, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1204-6512-1235

Саленко Володимир Дмитрович, кандидат технічних наук, науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1201-6512-1236

Степанов Сергей Викторович, доктор технических наук, профессор, главный научный сотрудник Военного института Киевского национального университета имени Тараса Шевченко

Украинец Алексей Васильевич, кандидат технических наук, старший научный сотрудник, ведущий научный сотрудник Военного института Киевского национального университета имени Тараса Шевченко

Саленко Владимир Дмитриевич, кандидат технических наук, научный сотрудник Военного института Киевского национального университета имени Тараса Шевченко

Stepanov Sergij, doctor of technical sciences, professor, Chief Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine)

Ukrainets Oleksij, candidate of Technical Sciences, Senior Researcher, Leading Researcher of the Military Institute of Kyiv National Taras Shevchenko University (Kiev, Ukraine)

Salenko Volodymyr, candidate of engineering sciences, Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine)

РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ

ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ «ЗБІРНИКА ВІКНУ»

Редакційна політика «Збірника ВІКНУ» заснована на принципах об'єктивності та неупередженості при відборі статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності при відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

У «Збірнику ВІКНУ» сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах «Збірника ВІКНУ»: http://miljournals.knu.ua/index.php/zbirnuk; http://mil.univ.kiev.ua/page/lib/31

ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, що вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності:

– керується принципами неупередженості, наукової етики рецензування, захисту – інтелектуальної власності,

– несе відповідальність за рівень наукового наповнення журналу,

– виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;

– залишає за собою право направити рукопис на розгляд сторонньому рецензенту, у тому числі ретельний відбір через «сліпе» рецензування, відхилити статтю або повернути її на доопрацювання;

– може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення,

– має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про даний факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проекту не можуть бути відтворені повністю або частково в будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. При використанні опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

– несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань а також за те, що в матеріалах не міститься інформація з обмеженим доступом;

– повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у даній роботі, якщо вони не були отримані самим автором;

– забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, і бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

№ 66

Усі матеріали надруковані в авторській редакції.
Деякі статті не рецензуються, у зв'язку з пріоритетною кваліфікацією авторів або через сумніви редколегії у змісті.

Підписано до друку 20.12.19 р.
Авт. друк. Арк. 11. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ломоносова 81

т. 521-32-89