ISSN 2311-7249 (Print)
ISSN 2410-7336 (Online)

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

№ 2(47)
2023

Науковий журнал

Засновник і видавець

Національний університет оборони України
Журнал заснований у 2008 році

Адреса редакції

Національний університет оборони України
Інститут інформаційно-комунікаційних технологій та кібероборони

Повітрофлотський проспект, 28,
Київ, 03049
sitnuou@ukr.net
http://www.sit.nuou.org.ua

телефон: (044)-271-07-31, (098)-273-48-62
факс: (044)-271-07-31

Журнал зареєстровано в Державній реєстраційній службі України
(свідоцтво КВ №20490-10290ПР)

Журнал видається
українською та англійською мовами

Журнал виходить 3 рази на рік

Наказом Міністерства освіти і науки України
№409 від 17.03.2020 р. та №886 від 02.07.2020 р.
журнал включено до Переліку наукових фахових видань України категорії "Б" в галузях "технічні науки" та "військові науки",
спеціальності – 122, 124, 253, 255

Рекомендовано до друку Вченою радою Національного університету оборони України 21 серпня 2023 року

За використання матеріалів посилання на журнал "Сучасні інформаційні технології у сфері безпеки та оборони" обов'язкове

Редакція може не поділяти точку зору авторів
Відповідальність за зміст поданих матеріалів несуть автори

Журнал індексується у наукометричних базах:
Google Academy, Index Copernicus, The Journal Impact Factor. Directory of Research Journals Indexing (DRJI)

Журнал представлений у базах даних:
Bielefeld Academic Search Engine (BASE), Directory of Open Access Journals (DOAJ), Research Bible, WorldCat.

Журнал внесений до каталогів бібліотек:
Vernadsky National Library of Ukraine.

В номері:

ISSN 2311-7249 (Print)
ISSN 2410-7336 (Online)

MODERN INFORMATION TECHNOLOGIES IN THE SPHERE OF SECURITY AND DEFENCE

№ 2(47)
2023

Scientific journal

Founder and Publisher

National Defence University of Ukraine
The journal was founded in 2008

Address:

National Defence University of Ukraine,
Institute of Information and Communication Technologies and Cyber Defense

Povitroflotskiy ave. 28, Kyiv, 03049
sitnuou@ukr.net
http://www.sit.nuou.org.ua

Telephone: (044)-271-07-31, (098)-273-48-62
Fax: (044)-271-07-31

The journal is registered in the State Registration Service of Ukraine (certificate КВ №20490-10290ПР)

The journal is published in Ukrainian and English

The journal is published thrice a year

According to the orders of the Ministry of Education and Science of Ukraine № from 17.03.2020 and №886 from 02.07.2020 the journal was included in the List of scientific professional publications of Ukraine, "B" category, "technical sciences" and "military sciences" fields, specialties 122, 124, 253, 255

Recommended to publication by the Scientific Council of the National Defence University of Ukraine 2023/08/21

The journal is indexed in the scientometric bases:
Google Academy, Index Copernicus, The Journal Impact Factor. Directory of Research Journals Indexing (DRJI)

The journal is presented in the databases:
Bielefeld Academic Search Engine (BASE), Directory of Open Access Journals (DOAJ), Research Bible, WorldCat.
The journal is added to the libraries:
Vernadsky National Library of Ukraine.

Contents:

Editorial Board

Шановні колеги!

Підбиваючи проміжні підсумки роботи нашого наукового журналу «Сучасні інформаційні технології у сфері безпеки та оборони» висловлюємо всім Вам свою щиру повагу і вдячність. Існуюча професіональна співпраця є плідною і залишається надзвичайно актуальною, особливо, в умовах війни російської федерації проти України. Маємо визнати, що з часу свого заснування, у 2008 році, журнал відзначився активною редакторською політикою стосовно належного організування публікаційного процесу, ставши вагомим науковим форумом для висвітлення передових досліджень, у першу чергу, зі стратегічно важливих військових спеціальностей, на які він зорієнтований. Такий якісно-сучасний рівень розвитку спеціалізованого наукового видання став можливим завдяки високій компетентності, наполегливій праці та глибокій відповідальності команди фахівців Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України, а також дієво налагодженим зв'язкам із вітчизняними вченими за його межами, колегами і практиками за кордоном.

Переконані, що отримані здобутки стосовно регулярної та своєчасної публікаційної роботи з видання журналу дають змогу підтримувати його змістовність на високому рівні. Перш за все, це спрямована на підготовку і друк якісних наукових праць методично-консультаційна діяльність редакційної колегії з авторами наукових публікацій. Одночасно, відбувається постійне розширення кола наукових рецензентів, зокрема зарубіжних, шляхом залучення до співпраці таких, хто сприятиме підготовці до публікації об'єктивних та інноваційно-прикладних матеріалів. Водночас, здійснюється професійний редакційний супровід і систематичне та своєчасне виконання всіх технічних процедур.

На сьогодні маємо констатувати: журнал включено до переліку наукових фахових видань України категорії «Б», в якому можна публікувати результати дисертаційних робіт на здобуття наукових ступенів доктора наук і доктора філософії в галузях «технічні науки» та «військові науки» за спеціальностями:

122 «Комп'ютерні науки» – предметна область відноситься до сфери комп'ютерних технологій, програмування, інформатики та програмного забезпечення;

124 «Системний аналіз» – стосується аналізу і оптимізації складних систем, процесів та проблем у різних галузях;

253 «Військове управління (за видами збройних сил)» – включає в себе дослідження та розроблення методів і стратегій управління військовими силами;

255 «Озброєння та військова техніка» – охоплює дослідження, розроблення й тестування військової техніки, включно зі зброєю, транспортними засобами, системами оборони тощо.

Натомість, важливим аспектом є наша спрямованість у науково-освітній сфері на роботу із використанням провідних світових технологій, ураховуючи державні інтеграційні процеси до європейської спільноти. Особливий акцент здійснюється на адаптацію військової освіти до стандартів НАТО. Врахування таких особливостей

сприяє підвищенню відкритості журналу і гармонізації процесу видання журналу зі світовими публікаційними стандартами. Разом із тим, ми робимо все можливе, щоб зробити наукові праці наших авторів більш доступними для глобальної наукової спільноти.

Попри все, першочерговою залишається якість контенту журналу. Важливо відзначити, що матеріали, надані авторами, проходять обов'язкову процедуру «сліпого» рецензування – як внутрішнього, так і, за потреби, зовнішнього. Здійснюються кроки щодо запобігання плагіату і підтримання наукової доброчесності в академічному середовищі. Весь процес публікаційної роботи, від приймання статті до її видання, здійснюється за допомогою відкритого програмного забезпечення для ведення рецензованих журналів Open Journal Systems 3. Фактично, журнал проходить внутрішньо-редакційну процедуру цифрової трансформації, відповідно до загально-глобального процесу міжнародної дигіталізації.

Варто наголосити, що означені заходи стали запорукою індексації нашого журналу в таких міжнародних наукометричних базах даних, як Google Academy, Index Copernicus, The Journal Impact Factor, Directory of Research Journals Indexing. Крім того, команда фахівців Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України прикладає максимум зусиль для досягнення журналом «Сучасні інформаційні технології у сфері безпеки та оборони» видавничих критеріїв, що гарантуватимуть його входження до провідних міжнародних наукометричних баз світового рівня. Практично, така робота сприяє цілеспрямованості щодо підвищення рейтингів вчених закладів вищої технічної та військової освіти, формуванню їхньої наукової репутації, а також є важливим фактором для конкурентних і репутаційних переваг.

У зв’язку з цим, ще раз висловлюємо всім Вам свою щиру повагу і вдячність за співпрацю та запрошуємо до продовження активного обміну науковими досягненнями і практичним досвідом на сторінках журналу «Сучасні інформаційні технології у сфері безпеки та оборони». Ми переконані, що публікація наукових досліджень як провідних вчених, так і науковців-початківців, є стимулом прогресу наукових напрямів, які журнал призначений висвітлювати, забезпечуючи зростання наукового потенціалу України. Маємо надію, що наша спільна робота стане невід'ємним внеском у Ваше наукове становлення, розвиток і кар'єрне зростання. Впевнені, що наш журнал сприятиме розширенню Ваших дослідницьких інтересів, збагатить інтелектуально і стане надійним партнером на науковому шляху. Наша команда і далі надаватиме найкращі умови для друку і здійснюватиме повний науковий супровід усіх публікаційних процесів.

Пропонуємо ознайомитися зі змістом попередніх випусків журналу на сайті http://sit.nuou.org.ua/ і запрошуємо до подальшого активного співробітництва та подання статей для майбутніх випусків.

З повагою,
Вадим МАШТАЛІР, доктор історичних наук, професор, заслужений винахідник України, полковник, начальник Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України

DOI: **10.33099/2311-7249/2023-47-2-7-11**

УДК 355.4

Ракушев Михайло Юрійович *(доктор технічних наук, старший науковий співробітник)* [1]
Кравченко Юрій Васильович *(доктор технічних наук, професор)* [2]
Пантюшенко Роман Валерійович [3]

[1] ***Національний університет оборони України, Київ, Україна***
[2] ***Київський національний університет імені Тараса Шевченка, Київ, Україна***
[3] ***Центральний науково-дослідний інститут Збройних сил України, Київ, Україна***

АНАЛІЗ СУПРОВОДЖЕННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ТЕРМІНАЛ» ПІД ЧАС ШИРОКОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

У статті проведено аналіз супроводження розробником інформаційно-телекомунікаційної системи «Термінал» для виконання завдань збору, обробки, обміну та відображення геопросторової інформації видового спостереження. Розглянуто діяльність вітчизняної компанії «Товариство з обмеженою відповідальністю "УкрСпецСистемс"» щодо вдосконалення комп'ютерної програми «Термінал» з початку широкомасштабної збройної агресії російської федерації проти України – з лютого 2022 року до травня 2023 року. Проаналізовані основні напрями з удосконалення програмного забезпечення, а саме: режими роботи, використання електронних карт і відображення обстановки, політика безпеки та адміністрування, обробка матеріалів зйомки з безпілотних літальних апаратів, передавання й обробка відео, обмін геопросторовими даними з іншими системами військового призначення, ліцензування та політика оновлення програмного забезпечення. Наведено узагальнені часові показники виходу нових версій комп'ютерної програми «Термінал» та інтенсивності внесення змін до зазначеного програмного забезпечення. За результатами проведеного аналізу обґрунтовано висновок щодо суттєвого нарощування спроможностей інформаційно-телекомунікаційної системи «Термінал» для виконання завдань збору, обробки, обміну та відображення інформації видового спостереження, а саме: добутої безпілотними літальними апаратами, трансльованої стаціонарними камерами спостереження та отримуваної від космічних апаратів видового спостереження. Підтвердженням зазначеного є суттєве розширення мережі інформаційно-телекомунікаційної системи «Термінал» протягом 16 місяців широкомасштабної збройної агресії російської федерації проти України.

Ключові слова: *інформаційно-телекомунікаційна система, супроводження програмного забезпечення, безпілотний літальний апарат, обробка зображень, геопросторова інформація.*

Вступ

Постановка проблеми. Широкомасштабна збройна агресія російської федерації проти України 24 лютого 2022 року прогнозовано активізувала низку різнопланових процесів спрямованих на нарощування спроможностей сил оборони України, зокрема, прискорила згуртування українського суспільства і світового співтовариства навколо відсічі агресії та стрибкоподібно збільшила використання у Збройних силах України (далі – ЗС України) сучасних систем збору, накопичення, обробки, обміну та відображення різнорідної геопросторової інформації. Яскравим прикладом зазначеного стало довгоочікуване прийняття на озброєння ЗС України у грудні 2022 року Автоматизованої системи управління військами (далі – АСУ) «Дзвін», розробка якої тривала щонайменше з 2006 року [1].

Слід зазначити, що суттєвою ознакою АСУ «Дзвін», порівняно з подібними за функціоналом системами, що використовуються у ЗС України, є державне замовлення (та, відповідно, фінансування) її розробки і впровадження. Для решти систем характер фінансування є переважно не державним: підтримка партнерів, комерційні джерела, волонтерська допомога. Можна стверджувати, що саме державне замовлення і стало запорукою прийняття на озброєння АСУ «Дзвін», а з рештою, інакше не повинно було і статися. В якості підтвердження зазначеного, можна навести прийняття на озброєння АСУ «Ореанда-ПС», хоча в неї і не було стільки «конкурентів».

Поряд із зазначеним на сучасному етапі АСУ «Дзвін» не задовольняє у повному обсязі всі потреби зі збору, накопичення, обробки, обміну та відображення наявної геопросторової інформації, що яскраво підтверджується тим фактом, що зараз у ЗС України продовжують активно використовуватися спеціалізовані інформаційні системи, які, у тому числі, реалізують функції геоінформаційних систем військового призначення:

система ситуаційної обізнаності» «Дельта» розробки Центру інновацій та розвитку оборонних технологій Міністерства оборони України [2];

інформаційно-телекомунікаційна система «Термінал» (далі – ІТС «Термінал») розробки ТОВ «УкрСпецСистемс» [3];

бойова система управління тактичної ланки «Кропива» розробки ТОВ «Конструкторське бюро "Логіка"» [4];

програмне забезпечення ГІС Арта [5] та деякі інші.

Суттєвою ознакою наведених спеціалізованих інформаційних систем є їх інтенсивне супроводження розробниками, що обумовлено (поряд з основною причиною – зацікавленням розробника у проведенні такої діяльності) обмеженою (або взагалі відсутньою) державною участю в процесі розробки (фінансування) цих систем, та, їх відносною гнучкістю і придатністю до оперативного внесення змін за результатами експлуатації. Така ситуація потребує досліджень описаного процесу супроводження, який активно триває з початку широкомасштабної збройної агресії російської федерації проти України, так як зазначене супроводження є унікальним досвідом, щонайменше для ЗС України.

Супроводження розробником кожної із наведених систем має власні особливості, але виходячи із наявних для досліджень даних, подальший розгляд будемо проводити для ІТС «Термінал». Такий підхід, з одного боку, зменшує узагальненість проведених викладок, але з іншого боку, забезпечить їх більшу конкретність.

Аналіз останніх досліджень і публікацій.

Інформаційним ядром ІТС «Термінал» є комп'ютерна програма «Термінал». З огляду на сучасні підходи, які розглядаються в предметній галузі - програмна інженерія, супроводження програмного забезпечення (комп'ютерних програмних систем) розглядається як одна із складових його життєвого циклу, і включає в себе сукупність дій щодо: забезпечення роботи програмного забезпечення, внесення змін при виявленні помилок, адаптації програмного забезпечення до нового середовища функціонування, а також підвищення продуктивності, або поліпшення деяких характеристик програмного забезпечення. Після змін система має вирішувати ті самі задачі, а також мати план перенесення інформації в інші бази даних. Супровід, відповідно до стандартів ISO/IEC 12207 та ISO/IEC 14764, проводиться з метою виконання і модифікації програмного продукту в процесі експлуатації за умов збереження його цілісності [6].

Кількість відомих джерел в яких висвітлюється будь які відомості щодо ІТС «Термінал», через її відносну новизну не є значною [7; 8]. Але, комп'ютерна програма «Термінал», яка є інформаційним ядро ІТС «Термінал», активно супроводжується розробником у циклічній процедурі: моніторинг змін середовища функціонування ІТС «Термінал» та аналіз «відгуків» користувачів, і, подальший випуск нової (удосконаленої) версії програмного забезпечення.

Таким чином, **метою статті** є аналіз супроводження розробником інформаційно-телекомунікаційної системи «Термінал» для виконання завдань збору, обробки, обміну та відображення розвідувальної інформації видового спостереження з початку широкомасштабної агресії російської федерації проти України.

Виклад основного матеріалу дослідження

Для пояснення однієї з тенденцій щодо супроводження ІТС «Термінал», розглянемо складову діяльності ТОВ «УкрСпецСистемс» – виробництво безпілотних авіаційних комплексів (далі – БпАК). На початку 2022 року ТОВ «УкрСпецСистемс» було однією з небагатьох вітчизняних компаній, яка виробляє БпАК, що прийняті на озброєння ЗС України. Це модифікації БпАК PD-1 [3]. Водночас, до складу БпАК, окрім безпосередньо декількох безпілотних літальних апаратів (далі – БпЛА) входить, узагальнено, наземна станція (станції) управління та обробки отримуваної інформації видового спостереження з відповідним програмним забезпеченням. З високим ступенем упевненості можна стверджувати, що саме розробка зазначеного програмного забезпечення наземної складової БпАК, що прийнятий на озброєння ЗС України і було відправною точкою для ТОВ «УкрСпецСистемс» щодо діяльності зі створення ІТС «Термінал».

Компанією ТОВ «УкрСпецСистемс» на кінець 2021 року, комп'ютерна програма «Термінал» була вже розроблена та основні елементи майбутньої ІТС «Термінал» апробовані. Це забезпечило її швидке розгортання у лютому 2022 року в інтересах сил оборони Києва для збору, обробки, обміну та відображення розвідувальної інформації повітряної розвідки, що отримувалася безпілотними літальними апаратами. Огляд основних можливостей і технічних рішень, що були реалізовані в ІТС «Термінал» протягом березня 2022 року в інтересах сил оборони Києва наведено у [7].

З початку 2022 року ІТС «Термінал» значно збільшилася. Узагальнено, у ЗС України на теперішній час діє три хмари ІТС «Термінал», зведені дані для найбільшої з яких, наведено у табл. 1.

Таблиця 1

Динаміка нарощування кількості задіяних серверів для найбільшої хмари ІТС «Термінал»

Місяць, рік	02.2022	12.2022	05.2023
Кількість серверів	7	35	44

Коментуючи дані табл. 1 слід зазначити:

кількість серверів у хмарі (найбільшій з трьох), що розглядається протягом 16 місяців, зросла у 6 разів, що показує значне розширення ІТС;

загальний обсяг ІТС включає поряд з серверами, обов'язково, ще й користувачів, і їх кількість, як правило, перевищує кількість серверів. Але архітектура ІТС побудована так, що визначити їх

кількість (захищене адміністрування з кожного сервера) неможливо;

враховуючи вищезазначене, з високим рівнем достовірності динаміку збільшення ІТС «Термінал» за кількістю серверів можна прийняти за загальну оцінку нарощування її обсягу з 02.2022 до 05.2023.

Окремо слід наголосити, що закупівля обладнання для переважної більшості серверів (табл. 1) та значної кількості користувачів проводилась за не державні кошти, насамперед, це фінансова допомога волонтерських фондів. Відповідне обладнання, передавалося на баланс органів військового управління та військових частин, які підключались до ІТС «Термінал». Разом із тим, розробник приймав активну участь у пошуку відповідної волонтерської допомоги, особливо на початку 2022 року. Протягом періоду, що розглядається, було випущено 22 оновлені версії Комп'ютерної програми «Термінал». Перше оновлення – версія 2.3.1 (вихід 19.03.2022 року). Останнє оновлення (за період, що розглядається) – версія 2.3.22 (вихід 05.05.2023 року). Узагальнені дані щодо оновлення Комп'ютерної програми «Термінал» наведено у табл. 2 та на рис. 1, 2.

Додатково, на підтвердження зазначеного вище висновку, що на кінець 2021 року Комп'ютерна програма «Термінал» була вже розроблена, свідчить номер версії першого оновлення.

Таблиця 2

Відомості щодо супроводження Комп'ютерної програми «Термінал»

Зміна програмного забезпечення	2022 рік									2023 рік				Усього
	03	04	05	06	07	08	09	10	12	01	02	03	05	
Кількість оновлень (нових версій)	4	3	3	1	2	1	1	2	1	1	1	1	1	22
Кількість введених змін (нових функцій)	11	16	24	2	9	2	2	15	14	3	15	25	13	151

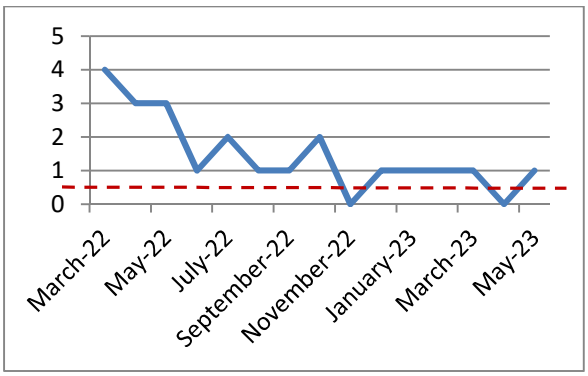


Рисунок 1 – Динаміка виходу нових версій Комп'ютерної програми «Термінал»

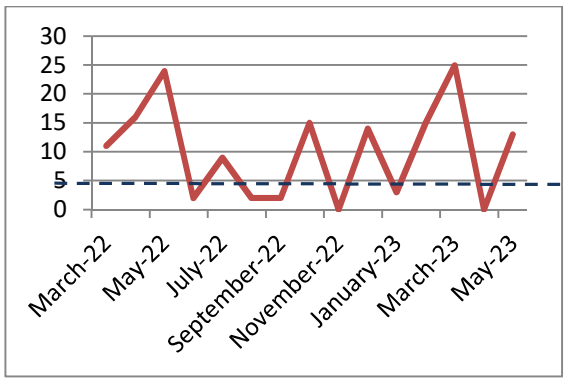


Рисунок 2 – Динаміка внесення змін до Комп'ютерної програми «Термінал»

Коментуючи дані табл. 2 їх ілюстрацію наведену на рис. 1 та рис. 2 слід зазначити:

динаміка випуску нових версій програмного забезпечення зменшилась з 4-х до 1-ї за місяць (середнє значення за досліджуваний період 1,5);

динаміка внесення змін до програмного забезпечення щодо введення нових функцій залишалась на протязі усього періоду відносно стабільною (середнє значення за досліджуваний період 10);

враховуючи вищесказане можна стверджувати, що розробник активно здійснює супроводження Комп'ютерної програми «Термінал», при чому динаміка супроводження за досліджуваний період зберігає відносно сталі показники інтенсивності.

Для подальшого аналізу наведемо режими роботи Комп'ютерної програми «Термінал». Слід зазначити, що стосовно версій, які були описані у [7], на початку 2023 року відбулись зміни назв деяких режимів. Старі назви наведено в дужках.

Основні режими Комп'ютерної програми «Термінал», з визначенням функціоналу від виробника.

1. Режим «Адміністратор» – налаштування та керування комп'ютерною програмою, створення нових операторів, керування дозволами, створення камери для відеоспостереження, створення екземпляру БпЛА, керування безпекою системи.

2. Режим «БпЛА онлайн» (змінено з «Розвідник-коригувальник з БпЛА»):

ведення розвідки місцевості в режимі on-line, ведення спостереження за ворожими об'єктами, отримання координат та відправка їх на ураження з подальшим коригуванням вогню;

нанесення на цифрову карту об'єктів, які автоматично синхронізуються між користувачами сервера.

отримання та обробка інформації від БпЛА: PD-2, RAM-2, Shark, Autel, DJI Mavic 3, Посейдон, Орлик, Bayraktar TB-2, Leleka-100.

3. Режим «Дешифрування» – автоматизація процесу визначення координат по матеріалам повітряної розвідки (фото/відео матеріалів) отриманих з БпЛА:

автоматична або ручна прив'язка матеріалів;

автоматичне визначення координат об'єктів;

автоматична побудова треку польоту;
відображення поля зору камери;
нанесення на карту об'єктів;
створення звіту (Stanag 3596);
завантаження для аналізу матеріалів (фото/відео) з БпЛА: PD-1 та PD-2, Leleka-100, коптери DJI, коптери Autel, Mapa, Yuneek, Орлик.

4. Режим «Відеоспостереження» (змінено з «Спостерігач-коригувальник системи стаціонарних відеокамер»):
ведення спостереження в режимі on-line;
автоматичне визначення координат об'єктів;
нанесення об'єктів на електронну карту;
автоматична синхронізація між користувачами сервера.

Режим підтримує роботу з PTZ камерами за допомогою протоколів керування: ISAPI, ISAPI DVR, ONVIF, Dahua, Archer, TANZ.

5. Режим «Командний центр» (змінено з «Штабний»):
нанесення на цифрову карту об'єктів, які автоматично синхронізуються між користувачами сервера;
вказування радіусів застосування ворожої техніки, аналіз та прорахунок безпечних маршрутів польотів БпЛА;
розробка оперативного бачення військових та оборонних місій.

Узагальнені дані щодо супроводження Комп'ютерної програми «Термінал» відповідно до розширення її функціоналу (поява нових функцій – останній рядок табл. 2) наведено у табл. 3 та 4.

Таблиця 3

Відомості щодо нових функцій за режимами роботи Комп'ютерної програми «Термінал» (з лютого 2022 р. до травня 2023 р.)

№	Режим роботи	Кількість нових функцій
1	Всі режими	60
2	Адміністратор	58
3	БпЛА онлайн	6
4	Дешифрування	12
5	Відеоспостереження	2
	Усього	141

Додатково, на літо 2023 року заплановано перше з 2022 року оновлення дизайну програми. Коментуючи дані табл. 3 та табл. 4 слід зазначити:

переважна частина введених нових функцій стосується усіх режимів роботи програми, водночас, режимом, до якого відноситься найбільша кількість нових функцій є режим «Адміністратор»;

значна частина удосконалень відноситься до: відображення обстановки на електронній карті (функціонал геоінформаційних систем), адміністрування та безпеки обміну даними між користувачами, розширення можливостей обробки матеріалів зйомки БпЛА та збільшити функціонал для обробки та передавання відео.

Таблиця 4

Відомості щодо функціоналу оновлень Комп'ютерної програми «Термінал» (з лютого 2022 р. до травня 2023 р.)

№	Додаткові функції	Кількість
1	Електронні карти, відображення (нанесення) обстановки, формування звітів	50
2	Адміністрування, безпека, обмін даними між серверами, права користувачів	40
3	Нові БПЛА, обробка матеріалів зйомки	28
4	Передавання та обробка відео (у т.ч. з камер відеоспостереження)	13
5	Чати, обмін даними між абонентами	8
6	Обмін даними з системами «Кропива», «Дельта», «Гермес», імпорт даних	6
7	Оновлення програмного забезпечення, ліцензування	6
	Усього	141

Окремо слід наголосити на проведеній роботі щодо обміну даними з іншими інформаційними системами, які реалізують функції геоінформаційних систем військового призначення (табл. 4). Однак, необхідно зазначити, що такий функціонал ще значно далекий від повноти.

У цілому, проведена робота забезпечила суттєве нарощування спроможностей ІТС «Термінал» для виконання завдань збору, обробки, обміну та відображення інформації видового спостереження, а саме: добутої БпЛА, трансльованої стаціонарними камерами та отримуваної від космічних апаратів видового спостереження [7], що підтверджується суттєвим розширенням системи (табл. 1).

Висновки й перспективи подальших досліджень

Таким чином, у статті проведений аналіз супроводження розробником інформаційно-телекомунікаційної системи «Термінал» для виконання завдань збору, обробки, обміну та відображення розвідувальної інформації видового спостереження з початку широкомасштабної агресії російської федерації проти України.

Наприкінці доцільно вказати на перспективи розвитку та супроводження інформаційно-телекомунікаційної системи «Термінал» з боку розробника:

подальша уніфікація комп'ютерної програми термінал «Термінал» з іншими, використовуваними у Збройних Силах України спеціалізованими системами, які реалізують функції геоінформаційних систем військового призначення (автоматизовані системи управління військами «Дзвін», «Дельта» та ін.);

відпрацювання процедури офіційного отримання від споживача інформаційно-телекомунікаційної системи «Термінал» (насамперед, Збройних сил України), результатів її використання, конкретизованих вимог до удосконалення (нових функцій) тощо.

Зазначена діяльність забезпечить суттєве збільшення ефективності супроводження інформаційно-телекомунікаційної системи

«Термінал» в частині більш раціонального використання зусиль та ресурсів ТОВ «УкрСпецСистемс».

Список бібліографічних посилань

1. Система управління «Дзвін-АС» стала на озброєння України. 08.12.2022. URL: https://mil.in.ua/uk/news/ systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/ (дата звернення: 12.03.2023). **2. Delta.** 2023. URL:https://delta.mil.gov.ua/wiki/info/ (дата звернення: 12.03.2023).. **3. Ukrspec** Systems. 2023. URL: https://ukrspecsystems.com/ (дата звернення: 12.03.2023). **4. Бойова** система управління тактичної ланки «Кропива» на службі ЗСУ та НГУ. 06.07.2020. URL: https://defence-ua.com/news/bojova_sistema_upravlinnja_ taktichnoji_lanki_kropiva_na_sluzhbi_zsu_ta_ngu_ foto-1129.html (дата звернення: 12.03.2023). **5. ГІС «Арта».** 2023. URL: https://gisarta.org/uk/index.html (дата звернення: 12.03.2023). **6. Лавріщева К. М.** Програмна інженерія : підручник. Київ, 2008. 319 с.

7. Ракушев М. Ю., Зуйко В. В., Пантюшенко Р. В. Аналіз використання інформаційно-телекомунікаційної системи «Термінал» в інтересах сил оборони Києва. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. № 2 (44). С. 54–59. DOI: 10.33099/2311-7249/2022-44-2-54-59. **8. Rakushev M., Zuiko V., Pantiushenko R., Nozdrachov O., Khomenko V., Chornomaz O.** The technique of the information and telecommunication system «Terminal» use for UAVs acquired data. *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2022. 208–212. DOI: 10.1109/ATIT58178.2022.10024215.

ANALYSIS OF THE MAINTENANCE OF THE INFORMATION AND TELECOMMUNICATION SYSTEM «TERMINAL» DURING THE LARGE-SCALE ARMED AGGRESSION OF THE RUSSIAN FEDERATION AGAINST UKRAINE

***Rakushev Mikhailo** (Doctor of Technical Sciences, Senior Researcher)* [1]
***Kravchenko Yurii** (Doctor of Technical Sciences, Professor)* [2]
Pantiushenko Roman [3]

[1] *National Defence University of Ukraine, Kyiv, Ukraine*
[2] *Taras Shevchenko National University of Kyiv*
[3] *Central Scientific and Research Institute of the Armed Forces of Ukraine*

The article provides an analysis of the maintenance provided by the developer for the information and telecommunication system «Terminal» to perform the tasks of collecting, processing, exchanging and displaying geospatial surveillance information. The activity of the domestic company «UkrSpetsSystems Limited Liability Company» was considered to improve the computer program «Terminal» from the beginning of the large-scale armed aggression of the russian federation against Ukraine – from February 2022 to May 2023. The main directions in software improvement were analyzed, namely: operating modes, use of electronic maps and situation display, security and administration policy, processing of footage from unmanned aerial vehicles, video transmission and processing, exchange of geospatial data with other military systems, licensing and software update policy. Generalized time indicators for the releases of new versions of the computer program «Terminal» are given and an intensity of changes to the software by the developer. Based on the results of the analysis, the conclusion regarding the significant increase in the capabilities of the Information and Telecommunication System «Terminal» to perform the tasks of collecting, processing, exchanging and displaying surveillance information, namely: obtained by unmanned aerial vehicles, transmitted by stationary surveillance cameras and received from surveillance spacecrafts. This is confirmed by the significant network expansion of the Information and Telecommunication System «Terminal» during 16 months of the large-scale armed aggression of the russian federation against Ukraine.

Keywords: *information and telecommunication system, software maintenance, unmanned aerial vehicle, image processing, geospatial information.*

References

1. ***The Dzvin-AS*** *control system was put into service in Ukraine,* (08 December 2022) [online]. Available at: https://mil.in.ua/uk/news/ systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/ [Accessed : 12 March 2023]. **2.** ***Delta*****,** **(**2023) [online]. Available at: https://delta.mil.gov.ua/wiki/info/ [Accessed : 12 March 2023]. **3.** ***Ukrspec*** *Systems*, (2023) [online]. Available at: https://ukrspecsystems.com/ [Accessed : 12 March 2023]. **4** ***Combat*** *control system of the tactical link «Kropyva» in the service of the Armed Forces and the National Guard of Ukraine*, (06.07.2020) [online]. Available at: https://defence-ua.com/news/bojova_sistema_upravlinnja_ taktichnoji_lanki_kropiva_na_sluzhbi_zsu_ta_ngu_foto-1129.html [Accessed : 12 March 2023]. **5.** ***GIS «Arta»*****,** (2023) [online]. Available at: https://gisarta.org/uk/index.html [Accessed 12 March, 2023]. **6. Lavrishcheva, K. M.,** (2008). *Software engineering: a textbook*. Kyiv. **7. Rakushev, M., Zuiko, V., Pantiushenko, R.,** (2022). Analysis of the use of the information and telecommunication system «Terminal» in the interests of the Kyiv defense forces. *Modern information technologies in the field of security and defense,* 2 (44), 54-59 DOI: 10.33099/2311-7249/2022-44-2-54-59. **8. Rakushev, M., Zuiko, V., Pantiushenko, R., Nozdrachov, O., Khomenko, V., Chornomaz, O.,** (2022). The technique of the information and telecommunication system «Terminal» use for UAVs acquired data. *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine,. 208-212. DOI: 10.1109/ATIT58178.2022.10024215.

DOI: **10.33099/2311-7249/2023-47-2-12-18**

УДК [519.857+519.872]:355.55

Думенко Микола Петрович ***(доктор військових наук)***

Національний університет оборони України, Київ, Україна

МЕТОД РОЗПОДІЛУ ЛЮДСЬКИХ РЕСУРСІВ МІЖ ВІЙСЬКОВИМИ ФОРМУВАННЯМИ

Успішне вирішення завдань щодо відбиття збройної агресії в умовах ведення збройної боротьби сучасності можуть вирішити лише добре підготовлені та укомплектовані війська. Метою статті є розроблення методу розподілу людських ресурсів між військовими формуваннями для підготовки кадровими органами оперативно-тактичного та оперативно-стратегічного рівнів обґрунтованих пропозицій командувачам (начальникам) до замислу операцій (бойових дій) для ухвалення рішення щодо маневру (перерозподілу) особового складу між Об'єднаними угрупуваннями військ. Під час проведення дослідження застосовано метод динамічного програмування, за допомогою якого вирішується оптимізаційна задача щодо знаходження такого оптимального розподілу людських ресурсів за m-періодів комплектування, за яких функція укомплектованості на останньому періоді комплектування буде максимальною. Оскільки укомплектованість залежить від значної кількості параметрів, які змінюються у часі, то для оптимального розподілу людських ресурсів необхідно проаналізувати та спрогнозувати зміни параметрів укомплектованості. Для цього застосовується метод прогнозування параметрів укомплектованості військових частин, який побудовано на методі нелінійної екстраполяції. Сутністю методу прогнозування укомплектованості військових частин Збройних сил України є використання логістично-ймовірнісної моделі опорного тренду комплектування, що змінюється за часом. Наукова новизна полягає в тому, що запропонований метод розроблений вперше, а практична значущість статті дозволяє вирішувати завдання, які постають перед Збройними силами України щоденно, проведення оптимального розподілу людських ресурсів між військовими формуваннями з урахуванням темпів мобілізаційного розгортання, обсягів надходження мобілізаційних людських ресурсів, безповоротних і санітарних втрат під час мобілізації та бойових дій.

Ключові слова: *метод динамічного програмування*, *багатокритеріальна оптимізація, функція укомплектованості, об'єднане угрупування військ, укомплектованість військових формувань Збройних сил України, оптимальний розподіл людських ресурсів.*

Вступ

Постановка проблеми. У мирний час комплектування Збройних сил України (далі – ЗС України) вирішує завдання з підтримання за встановленими штатами чисельності збройних сил, яка має бути достатньою для мобілізації і служити базою для розгортання ЗС України до штатів воєнного часу. В особливий період, у разі переведення ЗС України з мирного на воєнний стан, комплектування особовим складом забезпечить своєчасне та повне мобілізаційне розгортання ЗС України. Стаття присвячена проблемі знаходження оптимального розподілу людських ресурсів між військовими формуваннями.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури за темою статті засвідчив відсутність цілеспрямованих досліджень щодо оптимального розподілу людських ресурсів між військовими формуваннями [2; 4; 9]. Існуючі методичні підходи стосуються розроблення та обґрунтування рекомендацій щодо підвищення мобілізаційної готовності військових формувань, підвищення ефективності використання мобілізаційних ресурсів в інтересах ЗС України, обґрунтування рекомендацій щодо підвищення ефективності бойового злагодження військових формувань під час відмобілізування й приведення у повну бойову готовність, вивчення досвіду деяких країн світу [3]. Проаналізоване дає можливість стверджувати, що наявні підходи до цього питання не носять послідовного характеру, однобічно розкривають результати виконання окремих процесів функціонування системи комплектування ЗС України.

Мета статті – розробити метод розподілу людських ресурсів між військовими формуваннями, який забезпечить досягнення максимальної їх укомплектованості на кінець визначеного терміну комплектування.

Виклад основного матеріалу дослідження

Метод оптимального розподілу людських ресурсів між військовими формуваннями базується на математичному методі оптимізації рішень, який дає можливість розв'язати багатокрокову задачу оптимізації розподілу людських ресурсів (методом динамічного програмування) для забезпечення досягнення максимальної їх укомплектованості на кінець визначеного терміну комплектування [1]. Для розв'язання задачі здійснюють:

аналіз даних щодо укомплектованості ЗС України та, на основі методу нелінійної екстраполяції, знаходять функції зміни чисельності військовослужбовців на визначений період комплектування, а також – функції зміни укомплектованості у цей же період;

оцінювання та прогнозування змін параметрів укомплектованості ЗС України, а саме: параметри нарощування чисельності військовослужбовців, використовуючи призов на військову службу, прийняття на військову службу за контрактом та мобілізації військовозобов'язаних, резервістів оперативного резерву першої та другої черг; параметри зменшення чисельності військовослужбовців у результаті звільнення з військової служби, демобілізації, санітарних та безповоротних втрат;

визначення функції укомплектованості, що залежить від початкових значень параметрів чисельності військовослужбовців і функцій змін чисельності військовослужбовців, які були отримані на попередньому етапі;

задача оптимального розподілу людських ресурсів сформульована та розв'язується як задача динамічного програмування.

Метод складається з 4 етапів:

І етап – аналіз даних щодо укомплектованості військових формувань ЗС України (задача нелінійної екстраполяції);

ІІ етап – оцінювання та прогнозування змін параметрів укомплектованості військових формувань ЗС України;

ІІІ етап – визначення функції укомплектованості;

IV етап – знаходження оптимального розподілу людських ресурсів між військовими формуваннями (задача динамічного програмування).

Розглянемо кожний з етапів.

І етап. Аналіз даних щодо укомплектованості військових формувань ЗС України. На цьому етапі проводиться аналіз даних щодо штатної $H(t_0)$ та штатної $S(t_0)$ чисельності військових формувань ЗС України у початковий момент часу t_0. Крім того, аналіз даних проводиться за такими складовими як:

зміни штатної чисельності через перехід на штат воєнного часу $\Delta H^{+}_{\text{ШВч}}(t)$ та формування нових військових формувань $\Delta H^{+}_{\text{ВФ}}(t)$ [4–7];

зміни штатної чисельності через перехід на штат мирного часу $\Delta H^{-}_{\text{ШВч}}(t)$ та розформування військових формувань $\Delta H^{-}_{\text{ВФ}}(t)$ [8];

зміни списочної чисельності через прийняття $\Delta S^{+}_{\text{К}}(t)$ та призов $\Delta S^{+}_{\text{П}}(t)$ на військову службу, проведення мобілізації $\Delta S^{+}_{\text{М}}(t)$, залучення військового резерву $\Delta S^{+}_{\text{ОР}-1}(t)$ і $\Delta S^{+}_{\text{ОР}-2}(t)$ та поповнення санітарних і безповоротних втрат $\Delta S^{+}_{\text{В}}(t)$ [9–12];

зміни списочної чисельності через закінчення контракту $\Delta S^{-}_{\text{К}}(t)$, звільнення з військової служби $\Delta S^{-}_{\text{П}}(t)$, демобілізації $\Delta S^{-}_{\text{М}}(t)$, зменшення військового резерву $\Delta S^{-}_{\text{ОР}-1}(t)$ і $\Delta S^{-}_{\text{ОР}-2}(t)$ та санітарних і безповоротних втрат $\Delta S^{-}_{\text{В}}(t)$ [13–14].

ІІ етап. Оцінювання та прогнозування змін параметрів укомплектованості військових формувань ЗС України (задача нелінійної екстраполяції). На цьому етапі визначаються:

функції зменшення штатної чисельності через перехід на штат мирного часу $\Delta H^{-}_{\text{ШВч}}(t)$ та розформування військових формувань $\Delta H^{-}_{\text{ВФ}}(t)$, на основі яких визначається функція зменшення штатної чисельності:

$$\Delta H^{-}(t) = \Delta H^{-}_{\text{ШВч}}(t) + \Delta H^{-}_{\text{ВФ}}(t); \qquad (1)$$

функція зміни штатної чисельності $\Delta H(t)$ на період комплектування ΔT:

$$\Delta H(t) = \Delta H^{+}(t) - \Delta H^{-}(t); \qquad (2)$$

функції збільшення $\Delta S^{+}(t)$ та зменшення $\Delta S^{-}(t)$ штатної чисельності:

$$\Delta S^{+}(t) = \Delta S^{+}_{\text{К}}(t) + \Delta S^{+}_{\text{П}}(t) + \Delta S^{+}_{\text{М}}(t) + \Delta S^{+}_{\text{ОР}-1}(t) + \Delta S^{+}_{\text{ОР}-2}(t) + \Delta S^{+}_{\text{В}}(t);$$

$$S^{-}(t) = \Delta S^{-}_{\text{К}}(t) + \Delta S^{-}_{\text{П}}(t) + \Delta S^{-}_{\text{М}}(t) + \Delta S^{-}_{\text{ОР}-1}(t) + \Delta S^{-}_{\text{ОР}-2}(t) + \Delta S^{-}_{\text{В}}(t);$$

функція зміни списочної чисельності $\Delta S(t)$ на період комплектування ΔT:

$$\Delta S(t) = \Delta S^{+}(t) - \Delta S^{-}(t). \qquad (3)$$

Для прогнозування змін параметрів укомплектованості застосовується метод нелінійної екстраполяції.

На ІІІ етапі проводиться визначення функції укомплектованості, яка залежить від початкових значень параметрів списочної та штатної чисельності і функцій змін списочної та штатної чисельності, які були отримані на попередньому етапі:

$$\boldsymbol{B(t)} = \frac{\boldsymbol{S(t_0)+\Delta S(t)}}{\boldsymbol{H(t_0)+\Delta H(t)}}. \qquad (4)$$

Для цього застосовано наступний алгоритм [15–28].

1. Побудова логістично-ймовірнісної моделі для показника укомплектованості військ прямо пропорційна добутку ймовірності укомплектованості B(t) та ймовірності створення некомплекту (1-B(t)) військ:

$$\frac{dB(t)}{dt} = -\gamma \cdot B(t) \cdot [1 - B(t)] \quad при \quad \gamma \le 0 \cdot \qquad (5)$$

2. Знаходження ймовірності $B(t)$ від часу t, після інтегрування диференційного рівняння для умов $B(t = t_{0,5}) = 0{,}5$, має наступний вигляд:

$$B(t) = \{1 + \exp[\gamma(t - t_{0,5})]\}^{-1}, \qquad (6)$$

де γ – коефіцієнт пропорційності, що кількісно дорівнює різниці протидії факторів, які перешкоджають укомплектованості військ професійно-спеціальним складом і факторів, що сприяють цьому процесу;

$t_{0,5}$ – час (місяці або роки), що відповідають моменту, коли показник укомплектованості досягне, згідно з умовами, половини від його максимального рівня.

3. Здійснення прогнозування змін показника укомплектованості на перспективному інтервалі часу та отримання оцінок параметрів

апроксимуючої функції $B(t_k)$ за результатами спостережень закону збільшення показника $B(t)$ на ретроспективному інтервалі часу, тобто за даними, коли $t_k = 0 \ldots t_m$, $k = 1 \ldots m$.

4. Складання системи рівнянь для оцінювання параметрів нелінійного прогнозного тренду:

$$B_1 = \{1 + exp[\gamma_0 (v_1 - v_{0,5})]\}^{-1}; \qquad (7)$$

$$B_m = \{1 + exp[\gamma_0 (v_m - v_{0,5})]\}^{-1}. \qquad (8)$$

5. Розв'язання системи рівнянь:

$$\gamma_0^1 = \frac{\ln\left(\frac{1}{B_1} - 1\right) - \ln\left(\frac{1}{B_m} - 1\right)}{v_m - v_1}; \qquad (9)$$

$$(v_{0,5})_0^1 = \frac{v_m \ln\left(\frac{1}{B_1} - 1\right) - v_1 \ln\left(\frac{1}{B_m} - 1\right)}{\ln\left(\frac{1}{B_1} - 1\right) - \ln\left(\frac{1}{B_m} - 1\right)} \qquad (10)$$

6. Отримання опорних значень $(t_{0,5})_0^2$ й γ_0^2 для двох значень функції, наприклад, за відомих, середньо віддалених (на ретроспективному інтервалі часу), значень аргументу $v = v_1$ та $v = v_m/2$:

$$\gamma_0^2 = \frac{\ln\left(\frac{1}{B_1} - 1\right) - \ln\left(\frac{1}{B_m/2} - 1\right)}{v_m/2 - v_1}; \qquad (11)$$

$$(v_{0,5})_0^2 = \frac{\frac{v_m}{2} \ln\left(\frac{1}{B_1} - 1\right) - v_1 \ln\left(\frac{1}{B_m/2} - 1\right)}{\ln\left(\frac{1}{B_1} - 1\right) - \ln\left(\frac{1}{B_m/2} - 1\right)}. \qquad (12)$$

7. Знаходження осереднених значень параметрів прогнозного тренду для його опорних значень $(t_{0,5})_0$ й γ_0:

$$\gamma_0 = \frac{\gamma_0^1 + \gamma_0^2}{2} = \frac{\frac{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m} - 1\right)}{v_m - v_1} + \frac{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m/2} - 1\right)}{v_m/2 - v_1}}{2}; \qquad (13)$$

$$(v_{0,5})_0 = \frac{(v_{0,5})_0^1 + (v_{0,5})_0^2}{2} = \frac{\frac{v_m ln\left(\frac{1}{B_1} - 1\right) - v_1 ln\left(\frac{1}{B_m} - 1\right)}{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m} - 1\right)} + \frac{\frac{v_m}{2} ln\left(\frac{1}{B_1} - 1\right) - v_1 ln\left(\frac{1}{B_m/2} - 1\right)}{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m/2} - 1\right)}}{2} \qquad (14)$$

Ці оцінки прогнозних параметрів підставляються у вираз (4) для отримання результуючої функції укомплектування на перспективному інтервалі часу.

8. Побудова прогнозного тренду процесу збільшення укомплектованості військ протягом часу для досягнення мети комплектування є параметрами прогнозної функції у виді:

$$B(v) = \{1 + exp[\gamma_0 (v_1 - v_{0,5})]\}^{-1}, \qquad (15)$$

де $\gamma_0 = \frac{\gamma_0^1 + \gamma_0^2}{2} = \frac{\frac{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m} - 1\right)}{v_m - v_1} + \frac{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m/2} - 1\right)}{v_m/2 - v_1}}{2}$; $\qquad (16)$

$$(v_{0,5})_0 = \frac{(v_{0,5})_0^1 + (v_{0,5})_0^2}{2} = \frac{\frac{v_m ln\left(\frac{1}{B_1} - 1\right) - v_1 ln\left(\frac{1}{B_m} - 1\right)}{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m} - 1\right)} + \frac{\frac{v_m}{2} ln\left(\frac{1}{B_1} - 1\right) - v_1 ln\left(\frac{1}{B_m/2} - 1\right)}{ln\left(\frac{1}{B_1} - 1\right) - ln\left(\frac{1}{B_m/2} - 1\right)}}{2} \qquad (17)$$

9. Розрахунок помилок оцінок параметрів функції визначаються за виразами:

$$\sigma\gamma = \left\{ \frac{(\gamma_0 - \gamma_0^1)^2 + (\gamma_0 - \gamma_0^2)^2}{2} \right\}^{1/2}; \quad (18)$$

$$\sigma(v_{0,5}) = \left\{ \frac{((v_{0,5})_0 - (v_{0,5})_0^1)^2 + ((v_{0,5})_0 - (v_{0,5})_0^2)^2}{2} \right\}^{1/2}. \quad (19)$$

За таких умов графік залежності укомплектованості військ $B(v)$ від часу v має вигляд, який наведено на рисунку 1.

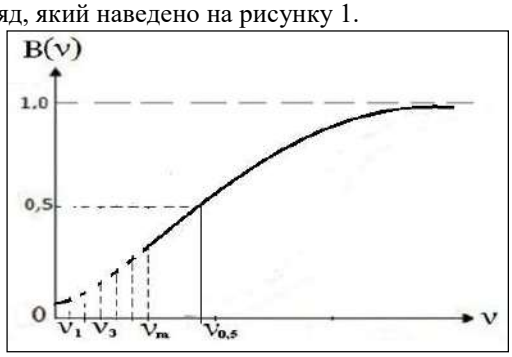


Рисунок 1 – Графік залежності укомплектованості військ $B(v)$ від часу v

10. Визначення довірчих інтервалів прогнозного тренду збільшення рівня показника укомплектованості військ та побудова верхньої і нижньої межі можливих змін рівня укомплектованості військ.

11. Для визначення маневру особовим складом доцільно визначити рівень порогу достатньої величини нормованого показника укомплектованості за наступним критерієм:

у разі потреби, використання термінового маневру особовим складом між військовими частинами доцільно здійснювати в термін, що дорівнює $t = t_1$;

в іншому разі, доцільно його здійснювати в термін, що дорівнює $t = t_3$;

якщо існує невизначеність в доцільності маневру особовим складом під час комплектування військ, потрібно ухвалювати рішення про маневр особовим складом в термін $t = t_2$. Графік визначення часу здійснення маневру мобілізаційними людськими ресурсами між Об'єднаними угрупуваннями військ (далі – ОУВ) наведено на рис. 2.

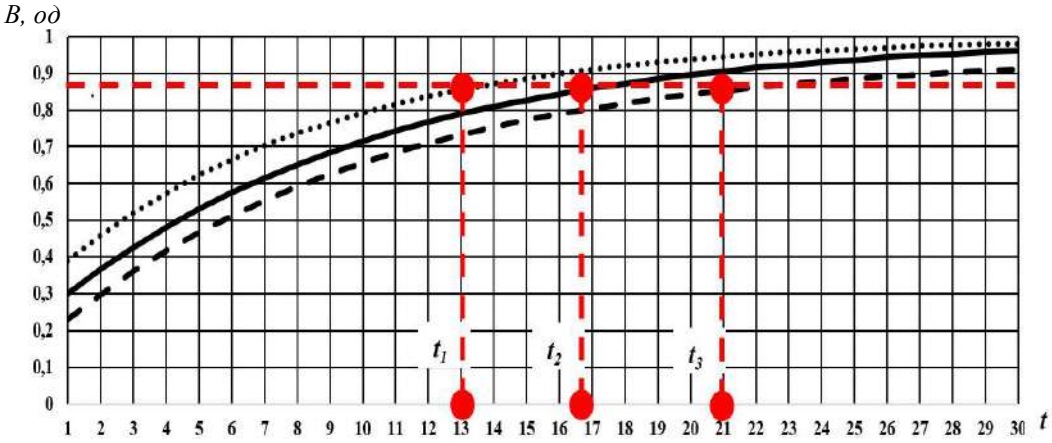


Рисунок 2 – Графік визначення часу здійснення маневру мобілізаційними людськими ресурсами між ОУВ

На четвертому етапі здійснюється формулювання задачі оптимального розподілу людських ресурсів як задача динамічного програмування. Для вирішення оптимізаційної задачі необхідно знайти такий оптимальний розподіл людських ресурсів $S = (s_1, s_2, \ldots, s_m)$, за якого укомплектованість військових формувань:

$$B(H(t), S(t)) = \prod_{i=1}^{m} b_i(\Delta H_i(t), \Delta S_i(t)), \quad (20)$$

де $b_i(\Delta H_i(t), \Delta S_i(t)) = \dfrac{g(\Delta S_i(t))}{f(\Delta H_i(t))}$;

$g(\Delta S_i(t))$ та $f(\Delta H_i(t))$ – функції змін списочної та штатної чисельності на і-му періоді комплектування, за m періодів комплектування буде максимальною $B(H(t), S(t)) = B_{\max}$.

Алгоритм знаходження оптимального розподілу людських ресурсів $S = (s_1, s_2, \ldots, s_m)$ такий:

1. Складається основне функціональне рівняння Річарда Беллмана: – оцінювання укомплектованості на i-му періоді комплектування:

$$B_i(\Delta H_i, \Delta S_i) = \max_{\substack{0 \le \Delta H_i \le \Delta H_{max} \\ 0 \le \Delta S_i \le \Delta S_{max}}} \{ b_i(\Delta H_i, \Delta S_i) B_{i+1}(\delta_i(\Delta H_i, \Delta S_i), \Delta H_i, \Delta S_i) \}, \quad (21)$$

де $\delta_i(\Delta H_i, \Delta S_i) = \dfrac{\psi(\Delta S_i)}{\varphi(\Delta H_i)}$ – оцінювання укомплектованості на i-му періоді комплектування.

2. Записується система рівнянь для умовних приростів укомплектованості:

$$B_{m-1}(\Delta H_{m-1},\Delta S_{m-1})=\max_{\substack{0\le\Delta H_i\le\Delta H_{max}\\0\le\Delta S_i\le\Delta S_{max}}}\{b_{m-1}(\Delta H_{m-1},\Delta S_{m-1})B_m(\delta_m(\Delta H_m,\Delta S_m),\Delta H_m,\Delta S_m)\};$$

$$B_{m-2}(\Delta H_{m-2},\Delta S_{m-2})=\max_{\substack{0\le\Delta H_i\le\Delta H_{max}\\0\le\Delta S_i\le\Delta S_{max}}}\{b_{m-2}(\Delta H_{m-2},\Delta S_{m-2})B_{m-1}(\delta_{m-1}(\Delta H_{m-1},\Delta S_{m-1}),\Delta H_{m-1},\Delta S_{m-1})\}; \quad (23)$$

… … … … … … … … … …

$$B_1(\Delta H_1,\Delta S_1)=\max_{\substack{0\le\Delta H_i\le\Delta H_{max}\\0\le\Delta S_i\le\Delta S_{max}}}\{b_1(\Delta H_1,\Delta S_1)B_2(\delta_2(\Delta H_2,\Delta S_2),\Delta H_2,\Delta S_2)\},$$

де $B_m(\Delta H_m,\Delta S_m)=\max_{\substack{0\le\Delta H_i\le\Delta H_{max}\\0\le\Delta S_i\le\Delta S_{max}}}\frac{g(\Delta S_m)}{f(\Delta H_m)}$ – умовний оптимальний приріст укомплектованості.

3. Розраховуються оптимальні значення розподілу людських ресурсів на кожному періоді комплектування та формується стратегія (план) оптимального розподілу людських ресурсів між військовими формуваннями, за якого досягається оптимальний розподіл людських ресурсів між військовими формуваннями:

$$\boldsymbol{s_{m-1}(\Delta H_{m-1},\Delta S_{m-1})},\ \boldsymbol{s_{m-2}(\Delta H_{m-2},\Delta S_{m-2})},\ \ldots$$
$$\ldots, s_1(\Delta H_1,\Delta S_1); \quad (24)$$
$$s_i=s_i(\Delta H_{i-1},\Delta S_{i-1});\qquad S=(s_1,s_2,\ldots,s_m).$$

Результати розрахунку оптимального розподілу людських ресурсів між військовими формуваннями $\Delta S_1^1, \ldots \Delta S_n^1$ (ОУВ – 1, ОУВ – 2, ОУВ – n) показано в таблиці 1.

Таблиця 1

Результати розрахунку оптимального розподілу людських ресурсів між військовими формуваннями

Оперативне угруповання військ	Черга мобілізації (k_1)	Черга мобілізації (k_2)	…	Черга мобілізації (k_m)
ОУВ-1	ΔS_1^1	ΔS_1^2	...	ΔS_1^m
ОУВ-2	ΔS_2^1	ΔS_2^2	...	ΔS_2^m
…	...	...	...	...
ОУВ-n	ΔS_n^1	ΔS_n^2	...	ΔS_n^m

Показником ефективності цього методу є цільова функція укомплектованості, а критерієм оптимального розподілу людських ресурсів є досягнення максимуму цільової функції на кінцевому періоді комплектування. За таких умов, значення функції укомплектованості повинно бути не менше 0,95.

Таким чином, сутність запропонованого методу полягає у тому, що метод дозволяє знайти оптимальний розподіл людських ресурсів між військовими формуваннями на основі даних щодо комплектування військових формувань у попередніх періодах комплектування та вимог до укомплектованості їх у наступні періоди, що забезпечить досягнення максимальної їх укомплектованості на кінець визначеного терміну комплектування. Метод, на відміну від існуючих, враховує темпи мобілізаційного розгортання, обсяги надходження мобілізаційного людських ресурсів та безповоротні і санітарні втрати під час мобілізації та бойових дій

Висновки й перспективи подальших досліджень

Розроблений у статті метод розподілу людських ресурсів між військовими формуваннями, дав змогу зробити низку логічних підсумків.

Для досягнення потрібного рівня укомплектованості у визначені терміни може здійснюватися маневр людським мобілізаційним ресурсом між військовими формуваннями.

Маневр особовим складом між Об'єднаними угрупуваннями військ у разі потреби доцільно здійснювати відповідно до директивних документів Генерального штабу Збройних сил України. Водночас, терміни маневру (перерозподілу) мобілізаційних людських ресурсів між Об'єднаними угрупуваннями військ визначаються залежно від темпів їх комплектування. Для кожного Об'єднаного угрупування військ рішення щодо маневру приймається або у момент часу t_1 (формування резерву мобілізаційних людських ресурсів для здійснення маневру) або у моменту часу t_3 (використання резерву мобілізаційного людських ресурсів).

Під час планування операцій (бойових дій) потрібно здійснювати постійний аналіз ходу комплектування Об'єднаних угрупувань військ та надавати пропозиції командувачам (начальникам) для ухвалення рішення щодо маневру (перерозподілу) особового складу між Об'єднаними угрупуваннями військ для досягнення порогового рівня укомплектованості 0,95±0,03.

Враховуючи потребу в фахівцях кадрових органів під час поставки мобілізаційних людських ресурсів необхідно: у мирний час – підготовити та приписати до відповідних кадрових органів військовозобов'язаних, які мають споріднену військово-облікову спеціальність; у воєнний час – під час мобілізації призвати цих фахівців для проведення роботи щодо прийому мобілізаційних

людських ресурсів та розподілу їх між Об'єднаними угрупуваннями військ і подальшого їх кадрового супроводження та демобілізації.

Здійснювати доукомплектування кадрових органів відповідно до замислу застосування військ (сил) з урахуванням прогнозу укомплектованості Об'єднаних угрупувань військ протягом терміну комплектування та сформувати План комплектування Об'єднаних угрупувань військ для ухвалення відповідних рішень.

У перспективі – розробити спеціальне програмне забезпечення розрахунку та розподілу людських ресурсів між військовими формуваннями.

Список бібліографічних посилань

1. Вентцель Е. С. Исследование операций: задачи, принципы, методология. 2–е изд. Москва: Наука, 1988. 208 С. 84–107. **2. Шуляк П. І.** Модель стану військовонавченого резерву з урахуванням перепідготовки та якісних кваліфікаційних показників. *Труди акад.* Київ: НАОУ, 2007. № 3(76). С. 8–17. **3. Шуляк П. І., Розумовський О. О., Гришин О. Л.** Методичний підхід до оцінювання достатності обсягів військового резерву людських ресурсів за умови впровадження служби в резерві за контрактом. *Зб. наук. пр. ЦНДІ ЗС України*. 2007. № 1(39). С. 13–19. **4. Прогнозування** здатності області, регіону задовольнити потребу військ (сил) у людських мобілізаційних ресурсах. НДР шифр «Фактор–М» / ЦНДІ ЗС України, наук. кер. Павловський О. В. Київ. 2020–2021, ДР 0120U000026д. **5. Про затвердження** структури військового резерву людських ресурсів (зі змінами): Постанова Кабінету Міністрів України від 12.11.2014 № 607 URL: https://zakon.rada.gov.ua/laws/show/607-2014-%D0%BF#Text (дата звернення: 30.06.2023). **6. Про затвердження** Порядку організації та ведення військового обліку призовників і військовозобов'язаних та резервістів: Постанова Кабінету Міністрів України від 30.12.2022 № 1487 URL: https://zakon.rada.gov.ua/laws/show/1487-2022-%D0%BF#Text (дата звернення: 30.06.2023). **7. Про Єдиний** державний реєстр призовників, військовозобов'язаних та резервістів: Закон України від 16.03.2017 № 1951–VIII. URL: https://zakon.rada.gov.ua/laws/show/1951-19#Text (дата звернення: 30.06.2023). **8. Обґрунтування** рекомендацій щодо обсягів підготовки та накопичення резерву особового складу мобілізаційних ресурсів для потреб ЗС України. Розробка рекомендацій щодо визначення потреб ЗС України у офіцерах запасу для їх доукомплектування на особливий період та поповнення втрат у воєнний час: звіт про НДР шифр «Ресурс–резерв» (проміж.) / ЦНДІ ЗС України; наук. кер. Розумовський О. О. Київ. 2010. 65 с. № ДР 0101U000998. **9. Обґрунтування** рекомендацій щодо формування оперативного резерву першої черги ЗС України: звіт про НДР шифр «Постулат–Р» / ЦНДІ ЗС України; наук. кер. Павловський О. В. Київ. 2018. 60 с. **10. Про затвердження** Порядку ведення Єдиного державного реєстру призовників, військовозобов'язаних та резервістів: Наказ МО України від 28.03.2022 № 94 URL: https://zakon.rada.gov.ua/laws/show/z0378-22#Text (дата звернення: 30.06.2023). **11. Про затвердження** Переліку випадків, за якими громадяни України знімаються з військового обліку військовозобов'язаних: Наказ МО України від 20.12.2017 № 684. URL: https://zakon.rada.gov.ua/laws/show/z0073-18#Text (дата звернення: 30.06.2023). **12. Про затвердження** Методики визначення військових втрат, завданих Україні внаслідок збройної агресії Російської Федерації**:** Наказ МО України від 14.09.2022 № 277. URL: https://zakon.rada.gov.ua/laws/show/z1471-22#Text (дата звернення: 30.06.2023). 13**. Щодо нової класифікації** та обліку втрат особового складу ЗС України: методичний посібник. Київ : ГШ ГК ЗС України, 21.10.2019. **14. Про затвердження** Змін до Положення про військово-лікарську експертизу в ЗС України: Наказ МО України від 18.03.2021 № 70. URL: https://zakon.rada.gov.ua/laws/show/z0431-21#Text (дата звернення: 30.06.2023). **15. Sang M. Lee, Laurence J. Moore, Taylor Bernard W. III.** Management science. USA. Allyn and Bacon, Inc., 1981. 910 p. **16. Справочник** по теории автоматического управления / под ред. А. А. Красовского. Москва: Наука, Гл. ред. физ.-мат. лит., 1987. 712 с. **17. Сигорский В. П.** Математический аппарат инженера. Киев: Техніка, 1977. 765 с. **18. Румчев В. Г., Конин А. Л.** Кадровые подсистемы АСУ: математические модели / под ред. И. А. Ушакова. Москва: Радио и связь, 1984. 248 с. **19. Феллер В.** Введение в теорию вероятностей и ее приложения: пер. англ. В 2 т. Москва: Мир, 1984. Т. 1. С. 69–72, 386–458. **20. Корн Г., Корн Т.** Справочник по математике для научных сотрудников и инженеров. Москва: Наука, 1984. 831 с. **21. Кетков Ю. Л., Кетков А. Ю., Шульц М. М.** MATLAB 6.x: программирование численных методов. Санкт–Петербург: БХВ, 2004. 672 с. **22. Юрков Б. Н.** Исследование операций: учебн. Москва : ВИА 1990. 205 с. **23. Бешелев С. Д., Гурвич Ф. Г.** Математико–статистические методы экспертных оценок. Москва: Статистика, 1974. 160 с. **24. Сухарев А. Г., Тимохов А. В., Федотов В. В.** Курс методов оптимизации. Москва: Наука, 1986. 328 с. **25. Карманов В.** Математическое программирование. Москва: Наука, 1973. 241 с. **26. Алексеев Е. Р., Чеснокова О. В.** MATLAB 7: самоучитель. Москва: НТ Пресс, 2006. 464 с. **27. Глушков В. М.** Кібернетика. Питання теорії і практики. (Наука. Світогляд. Життя) / В. М. Глушков. Москва: Наука, 1986. 488 с. **28. Кириченко І. О., Раскін Л. Г.** Математичні основи теорії вогневих дуелей : монографія. Харків : Військ. Ін-т ВВ МВС України, 2005. 292 с.

METHOD OF DISTRIBUTION OF HUMAN RESOURCES BETWEEN MILITARY FORMATIONS

***Dumenko Mykola** (Doctor of Military Sciences)*

National Defense University of Ukraine, Kyiv, Ukraine

Only well-trained and well-equipped troops can successfully fight off armed aggression in modern warfare. The paper focuses on developing a method of military personnel distribution between battle units in order to prepare operational-tactical and operational-strategic substantiated proposals to commanders (chiefs) for planning operations (combat operations) to make decisions on the maneuvers (redistribution) of military

personnel between the battle groups. Dynamic programming method was used to optimize distribution of human resources during m-periods of staffing, during which the staffing function in the last staffing period will be maximal. Since staffing depends on a significant number of parameters that change over time, it is necessary to analyze and forecast changes in staffing parameters for the optimal distribution of military personnel. To achieve that, the method of forecasting parameters of the military units staffing is used, which is based on non-linear extrapolation method. The idea of the method of military units staffing forecasting of the Armed Forces of Ukraine is in using logistic-probabilistic model of the reference staffing trend that changes over time. The scientific novelty is in the fact that the proposed method was developed for the first time, and the practical significance of the article allows solving the tasks that the Armed Forces of Ukraine face on a daily basis, carrying out the optimal distribution of military personnel between military units, taking into account mobilization deployment rate, numbers and rate of mobilized personnel arrival, irreversible and sanitary losses during mobilization and military operations.

Key words: *dynamic programming method, multi-criteria optimization, staffing function, unified battle groups, staffing of military units of the Armed Forces of Ukraine, optimal distribution of military personnel.*

References

1. Venttspils, E. S. (1988). *Operations Study: objectives, principles, methodology*. 2-nd ed. Moscow: Science, 84–107. **2. Shuliak, P. I.** (2007). *Model of military reserve status taking into account retraining and qualitative qualification indicators.* Works acad. Kyiv: NAOU, 3(76), 8–17. **3. Shuliak, P. I., Rozumovskyi, O. A., Grishin, O. L.** (2007). *Methodological approach to estimation of the sufficiency of military reserves of human resources provided the service is implemented in the reserve under the contract.* Collection of scientific papers. CRSI of the AF of Ukraine, 1(39), 13–19. **4. *Forecasting*** *the region's ability to satisfy the need for troops (forces) in human mobilization resources. The Research work code is «Factor-M»* / the Central Research Institute of the Armed Forces of Ukraine, scientific adviser Pavlovskyi O. V. Kyiv: 2020-2021, DR 020U000026d. **5. *On approval*** *of the structure of the military reserve of human resources (with changes)* [online], (2014). Resolution of Cabinet of Ministers of Ukraine. № 607, 12 November. Available at: <https://zakon.rada.gov.ua/laws/show/607-2014-%D0%BF#Text> [Accessed 30 June 2023]. **6. *On approval*** *of the Procedure for the organization and maintenance of military records of conscripts and conscripts and reservists* [online], (2022). Resolution of Cabinet of Ministers of Ukraine. № 1487, 30 December. Available at: <https://zakon.rada.gov.ua/laws/show/1487-2022-%D0%BF#Text> [Accessed 30 June 2023]. **7. *About the Unified*** *State Register of conscripts, military servants and reservists* [online], (2017). Law of Ukraine, № 1951–VIII, 16 March. Available at: <https://zakon.rada.gov.ua/laws/show/1951-19#Text> [Accessed 30 June 2023]. **8. *Substantiation*** *of recommendations on volumes of preparation and accumulation of reserve of personnel of mobilization resources for needs of the Armed Forces of Ukraine. Development of recommendations on defining the needs of the Armed Forces of Ukraine in the reserve offices for their additional staffing for a special period and replenishment of losses in military time:* Report on the Research work code «Resource-reserve» (*interim), (*2010). DR № 0101U000998. Kyiv: Central Research Institute of the Armed Forces of Ukraine; scientific adviser. Rozumovskyi O. O. **9. *Substantiation*** *of recommendations on formation of operational reserve of the first stage of the Armed Forces of Ukraine*: Report on the NDU of the code «postulate-R», (2018). Kyiv: The Central Scientific Research Institute of the Armed Forces of Ukraine; of scientific adviser Pavlovskyi O. V., 60. **10. *On approval*** *of the Procedure for maintaining the Unified State Register of conscripts, military servants and reservists* [online], (2022). Order of the Ministry of Defence of Ukraine № 94, 28 March. Available at: <https://zakon.rada.gov.ua/laws/show/z0378-22#Text> [Accessed 30 June 2023]. **11. *On approval*** *of the List of cases in which citizens of Ukraine are removed from the military register of conscripts* [online], (2017). Order of the Ministry of Defence of Ukraine. № 684, 20 December. Available at: <https://zakon.rada.gov.ua/laws/show/z0073-18#Text> [Accessed 30 June 2023]. **12. *On approval of the Methodology*** *for determining military losses caused to Ukraine as a result of the armed aggression of the Russian Federation* [online], (2022). Order of the Ministry of Defence of Ukraine. № 277, 14 September. Available at: <https://zakon.rada.gov.ua/laws/show/z1471-22#Text> [Accessed 30 June 2023]. **13. *Regarding*** *the new classification and accounting of losses of the Armed Forces of Ukraine*: methodological manual, (2019). Approved by the Head of the Chief of General Staff - Commander in Chief of the Armed Forces of Ukraine, 21 October. **14. *On approval*** *of amendments to the Regulation on military medical examination in the Armed Forces of Ukraine* [online], (2021). Order of the Ministry of Defence of Ukraine. № 70, 18 March. Available at: <https://zakon.rada.gov.ua/laws/show/z0431-21#Text> [Accessed 30 June 2023]. **15. Sang, M. Lee, Laurence, J. Moore, Taylor, Bernard W. III**. (1981). *Management science*: USA, Allyn and Bacon, Inc.. 910. **16. *Manual*** *for automatic control theory* (1987) / edited by A. A. Krasovskyi. Moscow: Science, Main editor of physical and mathematical literature, 712. **17. Sigorskyi, V. P.** (1977). *Mathematical apparatus of the engineer*. Kyiv: Engineering, 765. **18. Rumchev, V. G., Konin, A. L.** (1984) *HR subsystems of ACS: mathematical models* / edited by I. A. Ushakova. Moscow: Radio and communication, 248. **19. Feller, V.** (1984). *Introduction to probability theory and its applications:* translation from English in 2 books. Moscow: Mir,. T. 1., 69-72, 386-458. **20. Korn, G., Korn, T. A**. (1984). *Guide to maths for scientists and engineers.* Moscow: Science, 831. **21. Ketkov, Yu. L., Ketkov, A. Yu., Shultz, M. M.** (2004). *MATLAB 6.x: programming numerical methods*. St. Petersburg: BHV. 672. **22. Yurkov, B. N**. (1990). *Operations Study*: Manual. Moscow: VIA, 205. **23. Beshelev, C. D. Gurvich, F. G.** (1974). *Mathematical and statistical methods of expert assessments.* Moscow: Statistics, 160. **24. Suharev, A. G., Timokhov, A. V., Fedotov, V. V.** (1986). *Course of optimization methods*. Moscow: Science, 328. **25. Karmanov, V.** (1973). *Mathematical programming*. Moscow: Science, 241. **26. Alekseev, E. R., Chesnokova, O. V.** (2006). *MATLAB 7: self-taught.* Moscow: NT Press, 464. **27. Glushkov, V. M.** (1986). Cybernetics. Questions of theory and practice. (Science. World view. Life) / V. M. Glushkov. Moskva: Science, 488. **28. Kirichenko, I. O., Raskin, L. G.** (2005). *Mathematical bases of theory of fire duels*: monograph. Kharkiv: Military Institute of internal forces of Ministry of Internal Affairs of Ukraine, 292.

DOI: **10.33099/2311-7249/2023-47-2-19-24**

УДК 621.396.67

Нагорнюк Олександр Анатолійович *(кандидат технічних наук)*
Авсієвич Роман Олексійович

Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна

МЕТОД РОЗПІЗНАВАННЯ ВИДУ МОДУЛЯЦІЇ РАДІОСИГНАЛІВ КОСМІЧНИХ СИСТЕМ ЗВ'ЯЗКУ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ

Метою статті є вдосконалення методу розпізнавання виду модуляції радіосигналів, побудованих відповідно до телекомунікаційного стандарту ETSI EN 302 307 – 1, в умовах апріорної параметричної невизначеності із застосуванням кумулянтів. Актуальність дослідження за обраною тематикою полягає в тому, що означений телекомунікаційний стандарт є досить поширеним в інформаційних системах. Водночас він передбачає використання значного різноманіття сигнально-кодових конструкцій. Відсутність даних про вид модуляції унеможливлює налаштування демодулюючої апаратури. В свою чергу, потреба встановлення виду модуляції радіосигналів за відсутності апріорних даних, досить часто, виникає під час проведення радіомоніторингу частотного ресурсу, а також під час функціонування когнітивних радіосистем. Удосконалений в статті метод розпізнавання виду модуляції радіосигналів стандарту ETSI EN 302 307 – 1 базується на кумулянтному аналізі та методі мінімальної метрики. Вибір змішаних кумулянтів вищих порядків як модуляційних ознак, обумовлено їх властивістю адитивності та тим, що значення кумулянтів від третього і вище порядків дорівнюють нулю для величин із нормальним законом розподілення ймовірностей. Використання методу мінімальної метрики дозволяє в подальшому добавити інші види модуляції, що можуть розпізнаватися вдосконаленим методом, без суттєвої зміни самого методу (потрібно лише додати нові значення кумулянтів до еталонного алфавіту). Метод має порівняно низьку обчислювальну складність за рахунок використання лише чотирьох значень кумулянтів (C40, C42, C61, C63). Для підвищення ймовірності правильного розпізнавання виду модуляції в умовах наявних похибок синхронізації за несучою частотою запропоновано вдосконалити метод кумулянтного аналізу, шляхом використання кумулянтів розрахованих для модифікованих фазових сузір'їв. Перевагою модифікованих сузір'їв є їх інваріантність до залишкових значень несучої частоти. Перевірка результатів здійснювалася у програмному середовищі «MATLAB» відповідно до методу статистичних випробувань Монте-Карло. Результати моделювання показали, що вдосконалений метод кумулянтного аналізу дозволяє розпізнати вид модуляції із ймовірністю близькою до 1 за відношення сигнал-шум від 7 дБ під час використання звичайних фазових сузір'їв та за відношення сигнал-шум від 14 дБ у процесі використання модифікованих фазових сузір'їв. Використання модифікованих фазових сузір'їв дозволяє здійснювати обробку радіосигналів у випадку наявності залишків несучого коливання, що не враховується іншими авторами під час розгляду методів визначення виду модуляції радіосигналів, заснованих на кумулянтному аналізі. Враховуючи той факт, що телекомунікаційний стандарт ETSI EN 302 307 – 1 використовується у багатьох телекомунікаційних системах, отримані результати можуть бути використані в системах цифрової обробки радіосигналів, що застосовуються підрозділами сектору безпеки і оборони України.

Ключові слова: *радіосигнал, телекомунікаційна система, автоматизація, модуляція, кумулянтний аналіз, метод мінімальної метрики.*

Вступ

Постановка проблеми. Телекомунікаційний стандарт ДСТУ «ETSI EN 302 307 – 1:2017 (ETSI EN 302 307 – 1:2014, IDT). Друге покоління структури кадрів, канального кодування та системи модуляції для супутникових систем мовлення, інтерактивних послуг, збору новин та інших широкосмугових застосувань. Частина 1. DVB-S2» (далі – ETSI EN 302 307 – 1) унормовує широкосмугову передачу даних в інформаційних системах. Станом на червень 2023 року, зазначений телекомунікаційний стандарт є одним із найбільш поширених у космічних системах зв'язку. Так, зазначений стандарт використовується для організації телекомунікаційних мереж з багатостанційним доступом, через які може передаватися мультимедійний трафік (відео, аудіо та дані). Широкому використанню телекомунікаційного стандарту ETSI EN 302 307 – 1 в космічних системах сприяли: можливість організації радіоканалів із значною пропускною здатністю, ефективне використання частотного ресурсу, універсальність, значне різноманіття сигнально-кодових конструкцій та режимів роботи.

Впровадження у практичне використання даного стандарту відбулося у 2005 році. У квітні 2021 року вийшло його оновлення, яке покращує спектральну ефективність та завадозахищеність радіоканалів, що сприяє використанню цього телекомунікаційного стандарту мобільними абонентами. Однак, під час проведення радіомоніторингу частотного ресурсу, а також в межах функціонування когнітивних радіосистем, враховуючи значне різноманіття сигнально-кодових конструкцій, передбачених стандартом ETSI EN 302 307 – 1, виникає апріорна параметрична невизначеність, зокрема, щодо виду модуляції у радіосигналах. Крім того, виробники обладнання можуть вносити зміни у телекомунікаційне обладнання з метою захисту інформації або створення оригінального обладнання з функціоналом відмінним від визначеного стандартом.

Аналіз останніх досліджень і публікацій. Ведення радіомоніторингу в умовах параметричної невизначеності вимагає застосування методів «сліпого» оцінювання радіосигналів для розпізнавання виду модуляції. Зазначені методи використовуються в радіосистемах з підтримкою технології «Множинний вхід множинний вихід» (Multiple Input Multiple Output (MIMO)), а також в програмно-визначених та когнітивних системах передачі інформації [2; 3]. Наукометричні бази містять значну кількість інформації щодо розпізнавання видів модуляції радіосигналів на фоні шумів з використанням методів «сліпого» оцінювання, зокрема: методи, що базуються на відношенні правдоподібності, метод розпізнавання видів модуляції з використанням значень моментів сигналу, метод гістограм миттєвих амплітуд та фазових станів, методи засновані на використанні величин статистики вищих порядків та інші [4 – 10].

У результаті вивчення особливостей кожного з наведених методів встановлено, що основними недоліками існуючих підходів є обмежена кількість видів модуляції, що розпізнаються, низька ймовірність правильного розпізнавання сигналів з близькими за формою фазовими сузір'ями, вплив на ймовірність правильного розпізнавання сузір'я похибок синхронізації, складність реалізації, вимогливість до обчислювальних ресурсів, необхідність наявності апріорної параметричної інформації та чутливість до відповідності сигналу прийнятій моделі.

Враховуючи зазначені недоліки, широкого розповсюдження набули методи засновані на теорії розпізнавання образів з використанням величин статистики вищих порядків [10]. Зазначені методи базуються на порівнянні теоретичних та розрахованих значень кумулянтів вищих порядків. Водночас значення кумулянтів не залежать від величини адитивного гауссівського шуму. Також, використання кумулянтів дозволяє розпізнавати широке різноманіття видів цифрової модуляції [12].

Метою статті є вдосконалення методу розпізнавання виду модуляції радіосигналів, що заснований на кумулянтному аналізі під час здійснення прийому даних в умовах апріорної невизначеності.

Виклад основного матеріалу дослідження

Суть методу визначення виду модуляції радіосигналів в умовах апріорної невизначеності із застосуванням кумулянтного аналізу полягає в розрахунку змішаних кумулянтів радіосигналу, порівнянні отриманих значень з теоретичними та прийнятті рішення про вид модуляції на основі найбільшого збігу розрахованих та теоретичних значень [5; 6].

Завдяки властивості адитивності під час аналізу сигналів з адитивним гауссівським шумом, метод на основі кумулянтів дозволяє забезпечити високу ймовірність правильного розпізнавання виду модуляції при низьких відношеннях сигнал-шум (далі – ВСШ).

Зазначені методи ефективні у випадку відновлення на приймальному боці частотної синхронізації. У випадку ж наявності залишкових значень несучого коливання доцільно використовувати модифіковані фазові сузір'я з розрахованими у статті значеннями кумулянтів.

Вихідні дані для дослідження такі: сигнал на передавальному боці сформовано відповідно до вимог ETSI EN 302 307 – 1, проте на окремих ділянках він має один з чотирьох видів цифрової модуляції: QPSK; 8PSK; 16APSK; 32APSK. Параметри маніпуляції на ділянці сигналу, що підлягає аналізу – постійні, а попередня інформація про їх можливі значення відсутня, що відповідає умовам апріорної параметричної невизначеності. Під час поширення сигналу він піддається впливу каналу, що описується гаусівською моделлю [11]. У такому разі відліки сигнальної суміші на виході аналого-цифрового перетворювача складаються з корисного сигналу та адитивного гаусівського шуму $\xi(t)$ [11]:

$$r(k,U_i)=a_i e^{j\left(2\pi f_c\frac{k}{F_s}+\theta\right)}\sum_{i=1}^{I}s_i^X g\left(\frac{k}{F_s}-(i-1)T-\varepsilon T\right)+\xi(t), \quad (1)$$

де a_i – амплітуда сигналу;

f_c – частота несучого коливання;

θ – початкова фаза несучого коливання;

T – символьний період;

s_i^X – комплексні символи кінцевого алфавіту маніпуляції X, значення яких подано в стандарті ETSI EN 302 307 – 1;

Fs – частота дискретизації;

ε – похибка тактової синхронізації;

$g(n)$ – імпульсна характеристика формуючого фільтра.

k – номер відліку в масиві.

Слід вважати, що на попередніх етапах обробки сигналу визначені параметри f_c, θ, T та ε, здійснені операцій корекції частоти несучого

коливання, символьної швидкості, еквалайзування [11]. Необхідно розпізнати вид модуляції сигналу за його фазовим сузір'ям.

Математично кумулянти p-порядку C_p – визначаються як коефіцієнти розкладання в ряд Маклорена логарифму характеристичної функції [8]:

$$\ln G(u) = \sum_{p=1}^{\infty} \frac{(iu)^p}{p!} C_p , \quad (2)$$

де p – порядок кумулянта.

Змішані кумулянти порядку p з кількістю комплексно-спряжених відліків q визначаються як [8]:

$$C_{pq} = Cum\left[\underbrace{r(k),...,r(k)}_{p-q}, \underbrace{r^*(k),...,r^*(k)}_{q}\right], \quad (3)$$

де $r^*(k)$ – спряжене значення комплексного відліку.

Кумулянт p-го порядку C_p визначається як сума початкових моментів до p-го порядку включно [8]:

$$C_p = Cum(r_1(n), r_2(n),..., r_p(n)) =$$
$$\sum_{\forall \vartheta} (-1)^{q-1}(q-1)! E\left[\prod_{j\in\vartheta_1} r(j)\right]...E\left[\prod_{j\in\vartheta_b} r_j\right] r(j) \quad (4)$$

де $\vartheta = (\vartheta_1, \vartheta_2,..., \vartheta_b)$ – множина всіх можливих розкладань індексів.

Під час розпізнавання виду модуляції можуть використовуватися змішані кумулянти до восьмого порядку включно *C20, C21, C40, C41, C42, C60, C61, C62, C63, C80, C81, C82, C83, C84*. Отримані із (3) вирази для їх розрахунку через значення змішаних моментів подано у [12].

Значення змішаного кумулянта C_{21} відповідає енергії сигналу. Для забезпечення можливості порівняння змішаних кумулянтів, розрахованих для сигналів з різними енергетичними характеристиками необхідно отримати їх нормовані значення [12].

$$C_{pq}^N = \frac{C_{pq}}{\left(C_{21} - D_\xi\right)^{p/2}}, \quad (5)$$

де C_{pq}^N – нормоване значення змішаного кумулянта;

D_ξ – дисперсія адитивного гауссівського шуму.

Для забезпечення можливості роботи методу автоматичного розпізнавання виду модуляції сигналів супутникових телекомунікаційних систем стандарту ETSI EN 302 307 – 1 в умовах наявних похибок синхронізації за частотою несучого коливання доцільно використовувати кумулянти розраховані для модифікованих фазових сузір'їв, що визначаються як

$$r^R(n) = r(n) \cdot r^*(n-m), \quad (6)$$

де $r^R(n)$ – відліки сигналу із модифікованим фазовим сузір'ям;

$r^*(n-m)$ – комплексно-спряжений відлік масиву даних r, зсунутий на m позицій.

Перевагою модифікованих сузір'їв є їх інваріантність до залишкових значень несучої частоти. Теоретичні значення кумулянтів звичайних та модифікованих фазових сузір'їв до 8-го порядку включно для чотирьох можливих видів модуляції стандарту ETSI EN 302 307 – 1 подано у табл. 1.

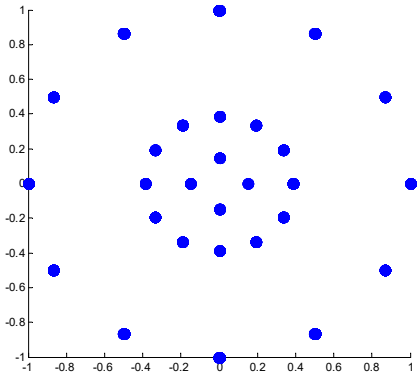
Таблиця 1

Теоретичні значення кумулянтів звичайних та модифікованих фазових сузір'їв

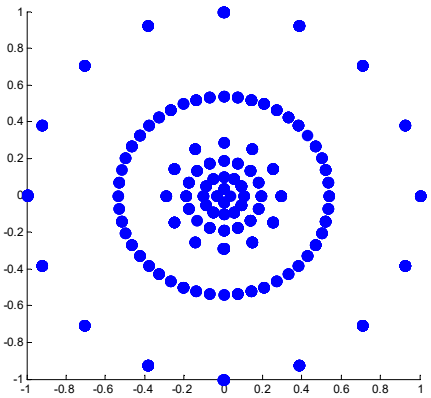
Змішаний кумулянт	Вид модуляції							
	QPSK		8PSK		16APSK		32APSK	
Значення	Звич.	Модиф.	Звич.	Модиф.	Звич.	Модиф.	Звич.	Модиф.
C20	0	0	0	0	0	0	0	0
C21	1	1	1	1	1	1	1	1
C40	1	1	0	0	0	0	0	0
C41	0	0	0	0	0	0	0	0
C42	-1	-1	-1	-1	-0.78	-0.48	-0.64	-0.12
C60	0	0	0	0	0	0	0	0
C61	-4	-4	0	0	0	0	0	0
C62	0	0	0	0	0	0	0	0
C63	4	4	4	4	2.48	0.82	1.72	-0.62
C80	-34	-34	1	1	0	0	0	0
C81	0	0	0	0	0	0	0	0
C82	34	34	0	0	-0.22	0	0.06	0
C83	0	0	0	0	0.03	0	0.06	0
C84	-34	-34	-33	-33	-17	-2.23	-10.3	4.68

З табл. 1 видно, що кумулянти звичайних та модифікованих фазових сузір'їв QPSK та 8PSK сигналів є однаковими. Це пояснюється тим, що звичайні та модифіковані сузір'я вказаних видів модуляції мають однаковий вигляд, поданий в [1].

Враховуючи вказане на рис. 1 наведено вигляд модифікованих фазових сузір'їв лише для модуляцій 16APSK та 32APSK.



а)



б)

Рисунок 1 – Модифіковані фазові сузір'я:
а) 16APSK; б) 32APSK

Проаналізувавши значення в табл. 1 можна зробити висновок, що під час побудови методу розпізнавання виду модуляції не потрібно використовувати всі значення кумулянтів, оскільки їх загальна сукупність має інформаційну надлишковість. Тому в методі використовується лише 4 кумулянти: C40, C42, C61, C63. Такий підхід значно зменшує розрахункову складність методу.

Прийняття рішення про вид модуляції здійснюється методом мінімальної метрики, що ґрунтується на пошуку мінімальної просторової відстані до векторів з відомими значеннями кумулянтів видів модуляцій поданих у табл. 1. Просторова відстань d_m розраховується як:

$$d_m = \left(\sum_{n=1}^{4} \left| C_n - C_n^m \right| \right), \qquad (7)$$

де C_n – розраховане значення n-го кумулянта;

C_n^m – теоретичне значення n-го кумулянта, що відповідає можливому m-му виду модуляції.

Рішення про вид модуляції приймається за мінімумом значення d_m. Отже, метод автоматичного розпізнавання виду модуляції сигналів супутникових телекомунікаційних систем стандарту ETSI EN 302 307 – 1 оснований на кумулянтному аналізі сигналів складається з таких операцій:

1. Розраховуються нормовані значення кумулянтів для відліків сигналу r(k) за формулами (3)-(5).

2. Визначається мінімальна метрика між отриманим набором кумулянтів та набором кумулянтів поданих в табл. 1.

3. Відповідно до отриманої метрики приймається рішення про вид модуляції сигналу, що підлягає аналізу.

У випадку наявних похибок синхронізації за частотою несучого коливання замість звичайних фазових сузір'їв використовуються їх модифіковані варіанти та повторюється послідовність операцій 1–3.

Перевірку ефективності методу автоматичного розпізнавання виду модуляції сигналів супутникових телекомунікаційних систем стандарту ETSI EN 302 307 – 1 в умовах апріорної невизначеності здійснено відповідно до вимог статистичного моделювання та методів Монте-Карло в програмному середовищі «MATLAB».

Сигнальні суміші формувались шляхом генерування радіосигналів із QPSK, 8PSK, 16APSK, 32APSK (кількість символів змінювалась в межах 1000-30000) та додавання до них шуму, модель якого описувалась нормальним законом розподілу ймовірностей. Відношення сигнал-шум (далі – ВСШ) змінювалося у діапазоні від 0 до 15 дБ з дискретністю 1 дБ. Для кожного значення ВСШ проведено 500 операцій із розпізнавання виду модуляції. У результаті статистичного моделювання отримано графічні залежності ймовірності правильного розпізнання виду модуляції від ВСШ, які зображені на рис. 2.

Із рис. 2а,б видно, що ймовірність правильного розпізнавання залежить від виду модуляції та типу фазового сузір'я. Для звичайних фазових сузір'їв ймовірність правильного розпізнавання PSK сигналів є близькою до 1 за ВСШ від 3 дБ, а APSK сигналів – за ВСШ від 6 дБ (рис. 2а). Ймовірність правильного розпізнавання виду модуляції QPSK, 8PSK та 32APSK за модифікованими фазовими сузір'ями є близькою до 1 за ВСШ від 10 дБ, а модуляції 16APSK – за ВСШ від 14 дБ (рис. 2б).

Використання модифікованих фазових сузір'їв потребує більш високої якості вхідного сигналу (ВСШ має бути вищим в середньому на 5 дБ), однак дозволяє здійснювати розпізнавання в умовах наявних залишкових значень несучої частоти.

Аналізуючи рис. 2 (в, г) можна зробити висновок, що зміна кількості символів сигналу, за якими здійснюється розпізнавання, в межах 1000–30000 знаків не призводить до суттєвої зміни ймовірності правильного розпізнавання.

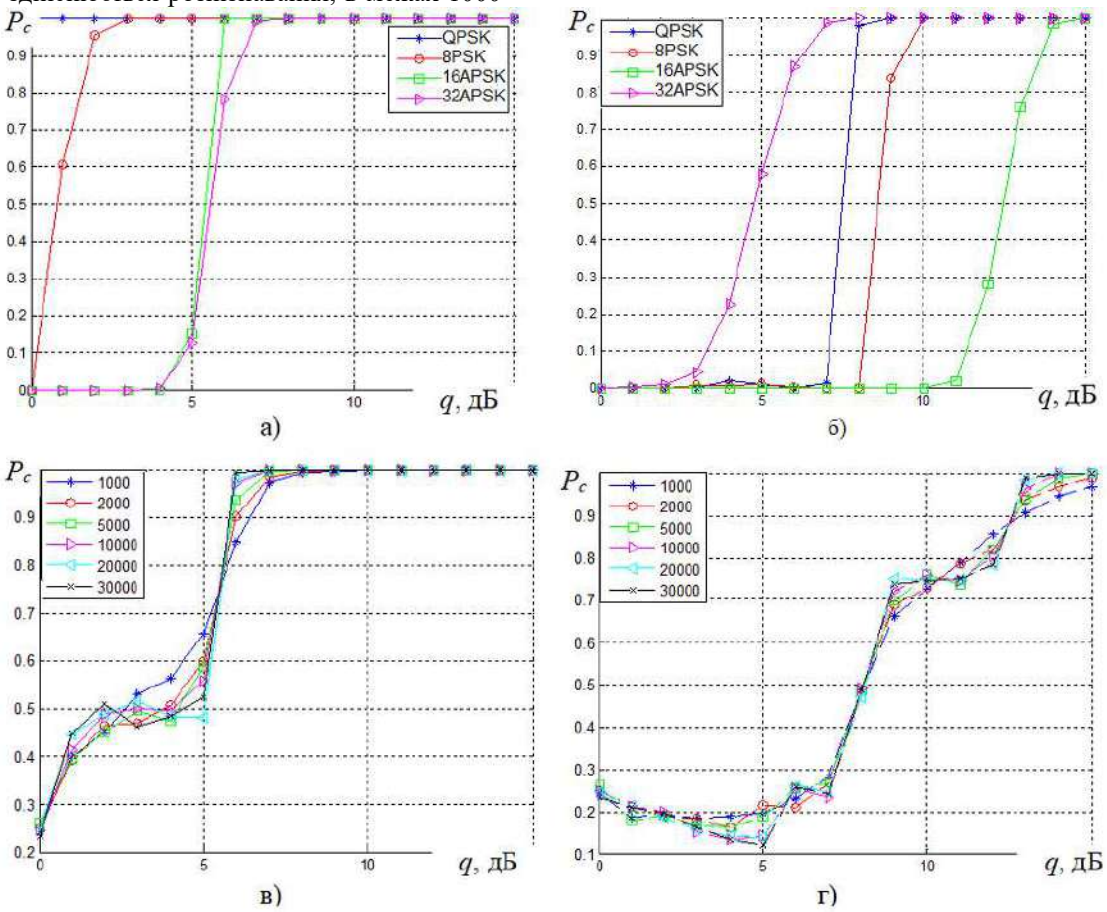


Рисунок 2 – Залежності ймовірності правильного розпізнавання виду модуляції сигналів стандарту ETSI EN 302 307 – 1:
а) для звичайних фазових сузір'їв залежно від виду модуляції за вибірки 5000 символів;
б) для модифікованих фазових сузір'їв залежно від виду модуляції за вибірки 5000 символів;
в) середня ймовірність для звичайних фазових сузір'їв залежно від кількості символів (1000 – 30000);
г) середня ймовірність для модифікованих фазових сузір'їв залежно від кількості символів (1000 – 30000)

Висновки й перспективи подальших досліджень

У статті вдосконалено метод розпізнавання виду модуляції радіосигналів, побудованих відповідно до стандарту ETSI EN 302 307 – 1, який ґрунтується на кумулянтному аналізі. Отримано теоретичні значення змішаних кумулянтів для чотирьох видів модуляцій, що передбачені стандартом.

Результати проведеного статистичного моделювання у програмному забезпеченні «MATLAB» свідчать, що вдосконалений метод дає змогу розпізнати вид модуляції з ймовірністю близькою до 1:

за відношення сигнал-шум від 7 дБ, за використання звичайних фазових сузір'їв;

за відношення сигнал-шум від 14 дБ, за використанні модифікованих фазових сузір'їв.

Слід відмітити, що для окремих видів модуляції розпізнавання здійснюється і за менших відношень сигнал-шум.

Враховуючи зазначене, метод розпізнавання виду модуляції радіосигналів, побудованих відповідно до стандарту ETSI EN 302 307 – 1, може бути використаний під час здійснення радіомоніторингу частотного ресурсу з використанням засобів цифрової обробки радіосигналів.

Список бібліографічних посилань

1. ДСТУ ETSI EN 302 307-1:2017 (ETSI EN 302 307-1:2014, IDT) Друге покоління структури кадрів, канального кодування та системи модуляції для супутникових систем мовлення, інтерактивних послуг, збору новин та інших широкосмугових застосувань. Частина 1. DVB-S2 – Вперше. [Чинний від 01.10.2017]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017, 81 с. **2. Muehlhau M., Oener M., Dobre O., Jaekel U., Jondral F.** A novel algorithm for MIMO signal classification using higher-order cumulants. Radio and wireless symposium. Austin, 2013. 3 p. **3. Report ITU-R SM.2152**. Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS). Geneva : ITU, 2009. 3 p. **4. Нагорнюк О. А., Писарчук О. О., Манойлов В. П.** Спосіб автоматизованого розпізнавання виду цифрової лінійної модуляції, заснований на кумулянтному аналізі сигналів. *Вісник Житомирського державного технологічного*

університету. Серія : Технічні науки, 2013. Т. 2. С.67-76. **5. Zhu Z., Nandi K.** Automatic modulation classification principles, algorithms and applications. London : John Wiley & Sons, 2015. 194 p. **6. Ahmed K. Ali, Erçelebi E.** Automatic modulation recognition of DVB-S2X standard-specific with an APSK-based neural network classifier. https://doi.org/10.1016/j.measurement.2019.107257 **7. Sapiano P., Martin J., Holbeche R.** Classification of PSK signals using the DFT of phase histogram. *In Proc. IEEE ICASSP*. 1995. Vol. 3. P. 1868–1871. **8. Smith A., Evans M., Downey J.** Modulation classification of satellite communication signals using cumulants and neural networks. Cleveland : Cognitive Communications for Aerospace Applications Workshop, 2017. 8 p. **9. Chen Z.** A blind classification method of adaptive coding and modulation signals based on cumulants. *Journal of Physics: Conference Series.* 2021. № 1738. doi:10.1088/1742-6596/1738/1/012015 **10. Sabbar M. B., Rasool A. H.** Automatic modulation classifier: review, Iraqi *Journal of Information and Communication Technology*. 2020. № 3(4). P. 11–32. doi: 10.31987/ijict.3.4.111 **11. Nezami M.** RF architecture and digital signal processing aspects of digital wireless transceivers. USA, 2003. 624 p. **12. Нагорнюк О**. Використання кумулянтного аналізу для розпізнавання радіосигналів цифрових телекомунікаційних систем. *Системи обробки інформації*. 2018. № 2(153). С. 136-143. https://doi.org/10.30748/soi.2018.153.17.

METHOD OF IDENTIFYING THE TYPE OF MODULATION OF RADIO SIGNALS OF SPACE COMMUNICATION SYSTEMS IN CONDITIONS OF PRIORI UNCERTAINTY

Nahorniuk Oleksandr (PhD)
Avsiievych Roman

Korolov Zhytomyr Military Institute, Zhytomyr, Ukraine

The purpose of the article is to develop a method for recognizing the type of modulation of radio signals built in accordance with the telecommunications standard ETSI EN 302 307 – 1 under conditions of a priori parametric uncertainty. The relevance of the research on the chosen topic is that the ETSI EN 302 307 – 1 standard is quite common in telecommunication systems. At the same time, this standard provides for the use of a significant variety of signal-code structures. The lack of data on the type of modulation makes it impossible to set up the demodulating equipment. In turn, the need to establish the type of modulation of radio signals in the absence of a priori data often arises during radio monitoring of a frequency resource, as well as within the framework of the functioning of cognitive radio systems. The method for recognizing the modulation type of radio signals of the ETSI EN 302 307 – 1 standard proposed in the article is based on cumulative analysis and the minimum metric method. The choice of mixed higher order cumulants as modulation features is due to their additivity property and the fact that the values of cumulants from the third and higher orders are equal to zero for values with a normal law of probability distribution. The application of the minimum metric method allows you to add other types of modulation that can be recognized by the developed method without significantly changing the method itself (it is only necessary to add new values of cumulants to the reference alphabet). The method has a relatively low computational complexity due to the use of only four values of cumulants (C40, C42, C61, C63). To increase the probability of correct recognition of the type of modulation in the conditions of existing synchronization errors by carrier frequency, it is proposed to use cumulants calculated for modified phase constellations. The advantage of modified constellations is their invariance to the residual values of the carrier frequency. The validation of the proposed methods took place in the «MATLAB» software environment according to the Monte Carlo statistical testing method. The modelling results showed that the proposed method allows to recognize the type of modulation with a probability close to 1 at SNR (signal noise reduancy) from 7 dB when using conventional phase constellations and at SNR from 14 dB when using modified phase constellations. Further research on the chosen topic is planned to be continued in the direction of increasing the number of modulation types provided by the new ETSI EN 302 307-2 telecommunications standard.

Key words: *radio signal, telecommunication system, automation, modulation, cumulant analysis, minimum metric method.*

References

1. DP «UkraNDNTs», (2017). *Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2*. DSTU ETSI EN 302 307-1:2017 (ETSI EN 302 307-1:2014, IDT) Kyiv. Vyd. ofits. **2. Muehlhau, M., Oener, M.,** (2013). *A novel algorithm for MIMO signal classification using higher-order cumulants.* Radio and wireless symposium. Austin, 3. **3. ITU** (2009). *Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)*. Report ITU-R SM.2152. Geneva, 3. **4. Nahorniuk, O. A., Pysarchuk, O. O., Manoilov, V. P.,** (2013). Method of digital linear modulation automatized recognition based on signals cumulant analysis. Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Seriia : Tekhnichni nauky. Zhytomyr, 2, 67-76. **5. Zhu Z. and Nandi K.,** (2015). Automatic modulation classification principles, algorithms and applications. London : John Wiley & Sons, 194. **6. Ali A. K., Erçelebi E.,** (2019). *Automatic modulation recognition of DVB-S2X standard-specific with an APSK-based neural network classifier*. doi: 10.1016/j.measurement.2019.107257 **7. Sapiano, P., Martin, J., Holbeche, R.,** (1995). Classification of PSK signals using the DFT of phase histogram. In Proc. *IEEE ICASSP*, 3, 1868–1871. **8. Smith, A., Evans, M., Downey, J.,** (2017). *Modulation classification of satellite communication signals using cumulants and neural networks*. Cognitive Communications for Aerospace Applications Workshop. Cleveland, 8. **9. Chen, Z.** (2021). A blind classification method of adaptive coding and modulation signals based on cumulants. *Journal of Physics: Conference Series*, 1738, doi:10.1088/1742-6596/1738/1/012015 **10. Sabbar, M. B. and Rasool, A. H.** (2020) «Automatic modulation classifier: review», *Iraqi Journal of Information and Communication Technology*, 3(4), 11–32. doi: 10.31987/ijict.3.4.111 **11. Nezami, M.,** (2003). RF architecture and digital signal processing aspects of digital wireless transceivers. USA, 2003. 624 p. **12. Nahorniuk, O.,** (2018). Use of cumulant analysis for recognition of radiosignals of digital telecommunication systems. *Systemy obrobky informatsii,* 2(153), 136-43. doi: 10.30748/soi.2018.153.17.

DOI: **10.33099/2311-7249/2023-47-2-25-30**

УДК 355.4

Штонда Роман Михайлович [1]
Зінченко Михайло Олександрович [1]
Чайка Євген Іванович [2]

[1] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2] ***Військова частина А0707, Гайсин, Україна***

ЗАСТОСУВАННЯ МАЛОГАБАРИТНИХ ЦИФРОВИХ ТРОПОСФЕРНИХ СТАНЦІЙ ЗВ'ЯЗКУ ПІД ЧАС ВЕДЕННЯ БОЙОВИХ ДІЙ (ОПЕРАЦІЙ)

На сьогоднішній день підходи щодо ведення операцій (бойових дій) змінили погляди із застосування Сил оборони під час відсічі збройного конфлікту. До 2000-х років XXI століття війни та військові конфлікти розвивалися за напрямом нарощування масовості живої сили та техніки з безпосереднім контактом військ (сил) на полі бою. Але сучасні збройні конфлікти і війни ведуться за принципом зменшення людського потенціалу й збільшення застосування високоточної та високо-інтегрованої зброї на великих відстанях. Сьогодні, використання високоточної зброї у поєднанні з розвідувальними засобами, диверсійними групами, незаконними збройними формуваннями, радіоелектронною розвідкою, засобами радіоелектронної боротьби значно впливає на організацію та функціонування системи зв'язку. Така тенденція буде лише нарощуватися та удосконалюватися, що призведе до виникнення проблем із роботою систем управління. Аналіз досвіду ведення операцій (бойових дій) свідчить, що використання великогабаритних станцій тропосферного зв'язку, призводить до моментального їх виявлення, внаслідок чого противник застосовує різні заходи щодо їх знищення. Тому, актуальним стало завдання щодо створення та впровадження до системи зв'язку держави малогабаритних цифрових тропосферних станцій зв'язку, які мають поєднувати в собі тропосферну та радіорелейну станції. Проаналізувавши попередні наукові видання стосовно тропосферного зв'язку, з'ясовано, що вони, переважно, зорієнтовані на висвітлення принципів застосування та впровадження великогабаритних тропосферних станцій зв'язку вітчизняних виробників. Водночас, підходи до застосування малогабаритних цифрових тропосферних станцій зв'язку розкриті недостатньо. Тому, в статті запропоновано підходи щодо застосування малогабаритних цифрових тропосферних станцій зв'язку іноземного виробництва як альтернатива вітчизняним розробкам в сучасних умовах ведення бойових дій (операцій), та надано рекомендації подальших напрямів наукової діяльності з розвитку тропосферного зв'язку.

***Ключові слова**: малогабаритна цифрова тропосферна станція зв'язку, тропосферний зв'язок, радіорелейний зв'язок, супутниковий зв'язок, комбінована тропосферна-радіорелейна станція зв'язку, кібератака.*

Вступ

Від самого початку повномасштабного вторгнення російської федерації на територію України стало відомо про численні кібератаки на українські ресурси. Напад російських зломників мереж і програм (хакерів) розпочався буквально за кілька годин до повномасштабного вторгнення російських військ. За даними агентства Reuters, США, Великобританія та Європейський Союз офіційно звинуватили росію у великомасштабному кібернападі, який порушив роботу супутникового інтернет-сервісу Viasat за годину до початку нового етапу війни 24 лютого 2022 року. Це спричинило знищення «десятків тисяч» супутникових терміналів [1].

Під час цієї кібератаки, 24 лютого 2022 року було запущено шкідливе програмне забезпечення AcidRain. Воно видалило усі дані на модемах та маршрутизаторах Viasat, які працювали на той час, через що всі термінали Viasat, перестали забезпечувати супутниковий зв'язок. І саме таким методом були виведені з ладу тисячі терміналів. Тому, після порушення роботи супутникового інтернет-сервісу Viasat велика частка передачі даних лягла на радіорелейні станції зв'язку [2]. Але на рівні з радіорелейними станціями зв'язку широко почали застосовуватися тропосферні станції зв'язку.

А отже, одним із найстійкіших і швидкісних способів передачі сигналу на сотні кілометрів, зокрема, у важкодоступні регіони, залишається тропосферний зв'язок.

Постановка проблеми. Протягом останніх років у науковому середовищі ведеться дискусія про місце та роль тропосферних станцій зв'язку в системі зв'язку. На сьогоднішній день актуальним

є завдання стосовно створення та впровадження малогабаритних цифрових тропосферних станцій зв'язку (далі – МЦТСЗ), які одночасно могли б працювати в двох режимах: загоризонтного зв'язку та прямої видимості. Поєднання цих двох режимів в одному виробі дозволить застосовувати тропосферні станції зв'язку під час ведення сучасних операцій (бойових дій) на полі бою з метою забезпечення надійного, стійкого, захищеного зв'язку між органами управління, зменшення ризиків щодо загибелі та травмування обслуговуючого персоналу та зниження можливості їх виявлення з метою ураження противником. Для досягнення даної мети буде необхідним впровадження МЦТСЗ до сучасної системи зв'язку.

Аналіз останніх досліджень і публікацій. У роботі [3] проаналізовано недоліки існуючих вітчизняних мобільних засобів тропосферного зв'язку та сформульовані шляхи їх вдосконалення. Крім того, підкреслено, що проблему розвитку військових систем цифрового тропосферного зв'язку потрібно вирішувати комплексно. А також визначено напрями вдосконалення мобільних засобів тропосферного зв'язку: створення станцій, що працюють за схемою «точка–багатоточка».

У статті [4] запропоновано нові технічні рішення, ключові технології і концепція побудови конкурентоздатних малогабаритних станцій тропосферного зв'язку нового покоління з високою пропускною спроможністю і захищеним радіодоступом до каналів зв'язку. Показано, що на їх основі в перспективі можна створити комбіновану станцію тропосферного і супутникового зв'язку.

У роботі [5] було досліджено стан, проблемні питання та напрями подальшого розвитку вітчизняних тропосферних систем зв'язку. Автори розглядають технічні аспекти роботи тропосферних станцій в сучасних умовах та пропонують шляхи їх модернізації.

Таким чином, проведений аналіз основних публікацій свідчить про наявність досліджень стану тропосферного зв'язку в Збройних Силах України. Проте узагальнені роботи, які б всебічно розглядали підходи до застосування МЦТСЗ, наразі відсутні.

Метою статті є пропонування підходів щодо застосування малогабаритних цифрових тропосферних станцій зв'язку в сучасних умовах проведення операцій (бойових дій) та надання рекомендацій стосовно подальших напрямів наукової діяльності з розвитку тропосферного зв'язку.

Виклад основного матеріалу дослідження

Станції тропосферного зв'язку за своїм функціональним призначенням відносяться до каналоутворюючих станцій і призначені для будівництва (розгортання) ліній (осей, рокад, ліній прямого зв'язку між пунктами управління, ліній доступу (прив'язки)) та організації каналів передачі ними інформації на різних рівнях управління [6].

Тропосферні станції зв'язку розроблені десятки років тому але після модернізації мають низку переваг не лише перед радіорелейними та супутниковими станціями зв'язку. Сьогодні в Україні модернізовано ряд станцій тропосферного зв'язку, серед них Р-417 до версії Р-417МУ та Р-423-1М до версії Р-423-1МУ. Ці сучасні модернізовані станції відносяться до великогабаритних станцій оскільки обладнання розміщується в кузові уніфікованого нульового габариту, який переміщується габаритними транспортними засобами з великою вантажопідйомністю, що не забезпечує скритість під час маршу, розгортання та експлуатації тропосферної станції зв'язку [7].

Отже, актуальним постає питання пошуку технічних рішень щодо зменшення великогабаритних тропосферних станцій зв'язку, а також уніфікації їх зовнішніх відмінних ознак, бо в умовах ведення операцій (бойових дій) будь-яка автомобільна техніка, що має нетипові ознаки, є об'єктом ураження. Тому для якісного виконання поставленого завдання щодо забезпечення надійного, стійкого, захищеного зв'язку між органами управління, зменшення ризиків стосовно загибелі й травмування обслуговуючого персоналу та зниження можливості їх виявлення з метою враження противником, буде перехід від великогабаритних тропосферних станцій зв'язку на МЦТСЗ.

Для вирішення даного питання пропонується розглянути можливість застосування вітчизняних МЦТСЗ або іноземного виробництва як альтернатива вітчизняним розробкам під час ведення операцій (бойових дій) [8].

МЦТСЗ повинні бути створені за блочно-модульним принципом на базі єдиних уніфікованих конструкцій, що розроблені з використанням сучасної мікроелектронної елементної бази та програмно-апаратних систем [9]. Основні складові конструктивної частини МЦТСЗ наведені на рисунку 1.

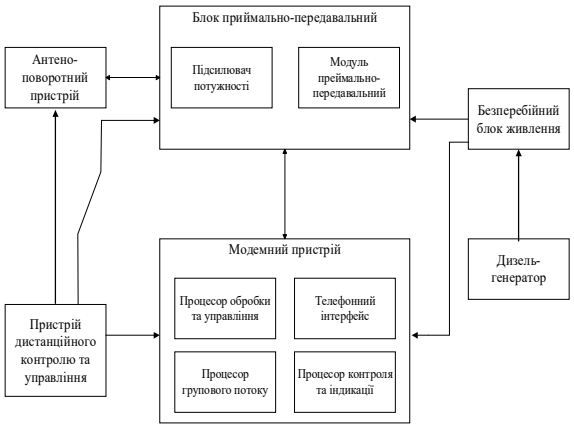


Рисунок 1 – Основні складові малогабаритної цифрової тропосферної станції зв'язку

Проєкт зовнішнього вигляду малогабаритних цифрових тропосферних станцій зв'язку наведено на рисунку 2.

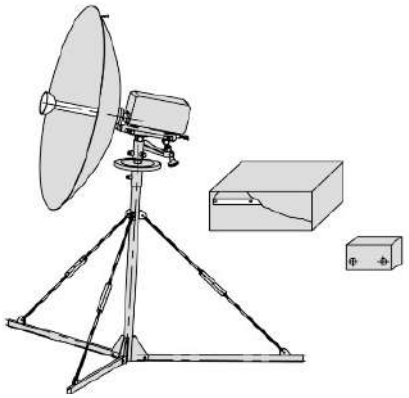


Рисунок 2 – Зовнішній вигляд малогабаритної цифрової тропосферної станції зв'язку

Антено-поворотний пристрій складається з:

триноги з можливістю встановлення обладнання вагою не менше 20 кілограм та механізмами закріплення на місцевості або на даху приміщень;

антени діаметром не більше 1 метру;

поворотного пристрою із забезпеченням повороту антени на 360 градусів.

До складу блоку приймально-передавального входять:

підвищувальний конвертер частоти;

підсилювач потужності з можливістю управління коефіцієнтом підсилення;

дуплексерні фільтри на передачу та прийом;

малошумливий понижуючий конвертер частоти;

пристрій вбудованого автоматичного контролю виробу;

елементи вторинного електроживлення вузлів виробу; перехід на антенний хвилевід круглого перерізу.

До складу модемного пристрою входять плати:

блоку обробки та управління;

процесора групового потоку і контролю та індикації;

інтерфейсу телефонного;

блоку вторинних джерел живлення;

віддаленого підключення.

До складу пристрою дистанційного контролю та управління входить:

ноутбук з програмно-апаратним комплексом для налаштування та управління МЦТСЗ;

також має бути доступна функція віддаленого доступу керування та налаштування за допомогою смартфона/планшета.

Крім того до складу МЦТСЗ входять:

телекомунікаційний комплект ТК-3 у разі потреби враховується можливість додавання ТК-4;

засоби захисту інформації та кібербезпеки;

джерело безперебійного живлення вихідною потужністю не менше 1500 Вт, діапазоном вхідної напруги живлення від 160–295 В, вихідною номінальною напругою 230 В., не менше 12 годин неперервної роботи;

дизель-генератор потужністю не менше 8 кВт;

кабелі живлення, довжиною не менше 30 метрів, і кабелі управління.

МЦТСЗ передбачає наявність таких технічних характеристик:

діапазон робочих частот від 4,4 до 5,0 ГГц;

максимальна швидкість приймання/передачі цифрового інформаційного потоку до 8 Мбіт/с;

інформаційний інтерфейс 10/100/1000 Base-T, наявні порти з можливістю інкапсуляції зовнішнього потоку конвертора E1 (G.703) в Ethernet;

протокол та інтерфейс передачі даних IP (TCP/IP), Ethernet;

вихідна потужність передавача на антенному фланці має становити приблизно 200 Вт;

забезпечувати швидкість передачі даних до 100 Мбіт/с – при тропосферному зв'язку та до 200 Мбіт/с – при радіорелейному зв'язку;

дальність тропосферної лінії зв'язку до 120 км;

дальність радіорелейної лінії зв'язку до 40 км;

час розгортання і входження в зв'язок має бути не більше 20 хв;

можливість віддаленого управління має здійснюватися дистанційно на відстані не більше100 метрів.

Таке обладнання має бути виготовлене в захищеному виконані за стандартом не нижче IP67, з урахуванням можливості живлення від декількох джерел. Одним із джерел живлення є стаціонарна (основна) мережа. Через те, що під час живлення від стаціонарної мережі є можливість відбору значних величин потужності, а струмове навантаження зовнішніх силових кабелів і внутрішніх приводів обмежене, необхідно суворо регламентувати споживану потужність, яка контролюється за показами споживаного струму. Так, номінальна величина споживаного струму для МЦТСЗ не повинна перевищувати величину 20-25 А. На нормальну роботу обладнання МЦТСЗ величина напруги живлення, що має становити величину 220 В ± 10 % і постійно контролюватися.

За допомогою дизель-генератора (резервна мережа) МЦТСЗ може працювати у випадку відсутності стаціонарної мережі. У зв'язку з тим, що дизель-генератори розраховані на видачу обмежених величин потужності, живлення сторонніх споживачів заборонено.

У разі відсутності стаціонарної та резервної мережі обладнання МЦТСЗ може працювати від джерела безперебійного живлення. Безперервна робота повинна бути не менше 12 годин. При під'єднаному джерелі безперебійного живлення категорично заборонено підключати сторонніх споживачів. Обслуговуючий персонал, становить не більше ніж 3 осіб і має знати:

власні функціональні обов'язки та, за необхідності, мають право замінити номер обслуги;

досконало знати експлуатаційні можливості обладнання МЦТСЗ;

уміти здійснювати розгортання обладнання МЦТСЗ у визначений термін;

бути підготовленим та досконало знати принципи застосування МЦТСЗ;

уміло проводити без порушень термінів технічне обслуговування МЦТСЗ.

Автомобільне шасі (пікап) формули 4 × 4 має забезпечувати надійну прохідність у різних кліматичних умовах на асфальтних та ґрунтових покриттях доріг, а також в важкодоступних складках місцевості. Залежно від умов проведення операцій (бойових дій) доцільно застосовувати броньоване автомобільне шасі, з метою забезпечення збереження життя особового складу. Також для перевезення майна екіпажу необхідне доукомплектування броньованого автомобільного шасі, одновісним чи двовісним напівпричепом з вантажопідйомністю не менше 3 тон.

Варіанти МЦТСЗ наведені на рис. 3, 4.

Рисунок 3 – Варіант 1. Розміщення малогабаритної цифрової тропосферної станції зв'язку на автомобільній базі

Рисунок 4 – Варіант 2. Переносна малогабаритна цифрова тропосферна станція зв'язку

Для розрахунку зон доступу МЦТСЗ має бути враховане максимальне значення дальності, на яку буде здійснюватися передача сигналу за заданою швидкістю і за необхідного значення якості передачі та заданою вірогідністю забезпечення зв'язку. Доступність каналу визначається за формулою [10]:

$$P_c = P\left(P_{прм} \geq P_{min}\right), \qquad (1)$$

де:

$P_{прм}$ – потужність сигналу на вході приймального пристрою;

P_{min} – реальна чутливість приймача;

P_c – доступність каналу.

Розрахунок доступності каналу в зоні доступу має будуватися на розрахунку енергетичного потенціалу тропосферних ліній зв'язку. Для розрахунку зон доступу на максимально допустимій відстані між МЦТСЗ в мережах необхідно враховувати:

потужності передавачів МЦТСЗ;

параметри антено-фідерного тракту приймально-передаючого обладнання (характеристики діаграм направленості антен, їх діючі висоти, втрати в антено-фідерному тракті і т.д.);

рівень зовнішніх та внутрішніх шумів на вході приймача та його чутливість;

електричні параметри обладнання, що застосовується (робоча частота, тип модуляції, ширина полоси пропускання приймача і т. д.).

Розглянуті параметри визначаються технічними умовами (технічними характеристиками) МЦТСЗ.

Максимальна зона доступу за високопіднятих антен в умовах рівнинної місцевості визначається виразом:

$$R_{max} \leq 0{,}8\left[4{,}12\left(\sqrt{h_1} + 2\sqrt{h_0} + \sqrt{h_2}\right)\right], \qquad (2)$$

де:

R_{max} – максимальна відстань до межі зони доступу;

h_1 – висота передавальної антени в метрах;

h_2 – висота прийомної антени в метрах;

h_0 – висота точки перехрещення між напрямками випромінювання дотичних до поверхні землі антен.

Додаткові втрати розраховуються як [11]:

$$W_{дтр} = W_{ст} + W_p + \Delta W_A + \Delta W_к + \Delta W_h + \Delta W_{hст} + \Delta W_з, \qquad (3)$$

де:

$W_{ст}$ – стандартне ослаблення, яке залежить лише від відстані R і довжини хвилі λ;

W_p – втрати, що обумовлені впливом нерівностей рельєфу місцевості й висот підйому антен;

ΔW_A – втрати підсилення антен;

$\Delta W_к$ – втрати, що обумовлені кліматичними умовами;

ΔW_h – втрати, що обумовлені впливом земної поверхні, за невеликих величин відношення h/λ;

$\Delta W_{hст}$ – втрати, що обумовлені відмінностями географічних висот;

$\Delta W_з$ – поправка, яка враховує швидкі та повільні завмирання.

Наприкінці зазначимо, що розрахунок зон

доступу МЦТСЗ, згідно наведених виразів, дасть змогу обслуговуючому персоналу якісно будувати тропосферні лінії зв'язку.

Отже, впровадження таких МЦТСЗ надасть можливість підвищити мобільність підрозділів зв'язку та якість виконання завдань і забезпечить:

стійкий та захищений зв'язок, який не залежить від погодних умов та фізичних завад, на відміну від супутникових і станцій зв'язку;

високу завадозахищеність, порівняно із супутниковими станціями зв'язку, тих же діапазонів частот;

високу живучість, порівняно із радіорелейними станціями зв'язку, до дій наземних станцій постановки завад та до засобів радіоелектронної боротьби повітряного базування;

кращу протидію до направлених та загороджувальних постановки завад;

можливість використання як тропосферної, так і радіорелейної станції зв'язку;

захищеність обслуговуючого персоналу.

Висновки й перспективи подальших досліджень

В статті авторським колективом розглянуто основні складові МЦТСЗ, описано характеристики станцій іноземного виробництва як альтернатива перспективним вітчизняним розробкам під час ведення операцій (бойових дій). Використання наведених в статті виразів/формул дасть можливість обслуговуючому персоналу здійснювати розрахунок зон доступу та розгортати тропосферні лінії зв'язку на належному рівні та в стислі терміни.

Водночас зазначимо, що МЦТСЗ доцільно застосовувати для забезпечення зв'язку зі старшим штабом/командиром, з підлеглими та взаємодіючими військами, а також між пунктами управління в оперативній та стратегічній ланках управління. В свою чергу, в тактичній ланці управління МЦТСЗ доцільно використовувати для забезпечення управління військами, починаючи з бригади і вище для побудови ліній прямого зв'язку та ліній прив'язки.

В свою чергу слід зауважити що МЦТСЗ також доцільно застосовувати в окремих випадках для організації зв'язку в інших підрозділах тактичного рівня (відділення, взвод, рота, батальйон та їм рівні) за неможливістю використання інших засобів зв'язку.

Таким чином, перспективність застосування малогабаритних цифрових тропосферних станцій зв'язку, що відповідають тенденціям розвитку тропосферних і радіорелейних засобів зв'язку, є актуальним напрямом для розроблення комбінованих цифрових комунікаційних систем вітчизняного виробництва.

Список бібліографічних посилань

1. Нечет Т. Війна росії проти України почалася з кібернападу на супутники. За годину до вторгнення були знищені «десятки тисяч» терміналів Viasat. ITC.ua. URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ (дата звернення: 01.03.2023). **2. Олексенко В. П., Штонда Р. М., Черниш Ю. О., Мальцева І. Р.** Сучасні підходи до забезпечення кібербезпеки в радіорелейних лініях зв'язку. *Кібербезпека: освіта, наука, техніка*. 2022. № 1(17). С. 57–64. **3. Почерняєв В. М., Повхліб В. С.** Стан і напрямки розвитку мобільних цифрових тропосферних систем зв'язку. Харків : *Системи озброєння і військова техніка*. 2018. № 2(54). С. 51–60. **4. Ільченко М. Є., Наритник Т. Н., Слюсар В. І.** Напрямки створення тропосферних станцій нового покоління. *Цифрові технології*. 2014. №16. С. 8–18. **5. Масесов М. О., Субач І. Ю., Руденко Д. М., Станович О. В.** Перспективи застосування цифрового діаграмоутворення у станціях тропосферного зв'язку спеціального призначення. *Збірник наукових праць ВІТІ ДУТ*. 2014. №1. С. 43–48. **6. Руденко В.І., Зінченко М. О., Бондаренко Л. О., Лазута Р. Р.** Вибір і обґрунтування структури системи тропосферного зв'язку спеціального призначення з урахуванням застосування інноваційних технологій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 3(45). С. 75–82. **7. Чайка Є. І., Штонда Р. М.** Сучасні підходи до розвитку малогабаритних цифрових тропосферних станцій зв'язку. *Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами* : матер. наук.-практ. конф. Харків : НАНГУ, 2023. С. 10. **8. Кравчук С. О.** Принципи створення портативних тропосферних радіорелейних станцій. *Проблеми телекомунікацій* : матер. Міжнар. наук.-техн. конф. Київ : НТУУ КПІ, 2015. С. 254–256. **9. Кравчук С. О.** Портативна тропосферна радіорелейна станція зв'язку. *Проблеми телекомунікацій* : матер. Міжнар. наук.-техн. конф. Київ : НТУУ КПІ, 2016. URL: http://conferenc.its.kpi.ua/proc/article/view/70959 (дата звернення: 01.03.2023) **10. Руденок В. І., Бондаренко О. Є., Сергієнко А. В., Остапук О. І.** Розрахунок зон доступу радіорелейними та тропосферними засобами зв'язку. *Збірник наукових праць ВІТІ ДУТ*. 2018. №3. С. 87–93.

MODERN APPROACHES TO THE APPLICATION OF SMALL DIGITAL TROPOSPHERIC COMMUNICATION STATIONS

Shtonda Roman [1]
Zinchenko Michael [1]
Chaika Yevhen [2]

[1] ***Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine,***
[2] ***Military unit A0707, Haisyn, Ukraine***

To date, approaches to conducting operations (combat operations) have changed views on the use of the Defense Forces during the repulsion of an armed conflict. Until the 2000s of the 21st century, wars and military conflicts developed in the direction of increasing the mass of manpower and equipment with direct contact of troops (forces) on the battlefield. But modern armed conflicts and wars are conducted according to the principle of reducing human potential and increasing the use of highly accurate and highly integrated weapons at long distances. Today, the use of high-precision weapons in combination with reconnaissance means, sabotage groups, illegal armed formations, radio-electronic intelligence, means of radio-electronic warfare significantly affects the organization and functioning of the communication system. This trend will only increase and improve, which will lead to problems with the operation of management systems. Analysis of the experience of conducting operations (combat operations) shows that the use of large-sized tropospheric communication stations leads to their immediate detection, as a result of which the enemy uses various measures to destroy them. Therefore, the task of creating and introducing small-sized digital tropospheric communication stations to the state communication system, which should combine tropospheric and radio relay stations, has become urgent. Having analyzed previous scientific publications related to tropospheric communication, it was found that they are mainly focused on highlighting the principles of application and implementation of large-sized tropospheric communication stations of domestic manufacturers. At the same time, approaches to the use of small-sized digital tropospheric communication stations are not sufficiently disclosed. Therefore, the article proposes approaches to the use of small-sized digital tropospheric communication stations in modern conditions of operations (combat operations) and provides recommendations for further directions of scientific activity in the development of tropospheric communication.

Keywords: *small-sized digital tropospheric communication station, tropospheric communication, radio relay communication, satellite communication, combined tropospheric-radio relay communication station, cyber attack.*

References

1. Nechet, T., (2022). *Russia's war against Ukraine began with a cyberattack on satellites. An hour before the invasion, "tens of thousands" of Viasat terminals were destroyed. ITC.ua.* [online]. Available at: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ [Accessed : 01 March 2023]. **2. Oleksenko, V. P.**, **Shtonda, R. M., Chernysh, Y. O., Maltseva, I. R.** (2022), Modern approaches to ensuring cyber security in radio relay communication lines. *Cyber security: education, science, technology*. 1(17), 57-64. **3. Pocherniaev. V. M.**, **Povhlib. V. S.,** (2018). Status and directions of development of mobile digital tropospheric communication systems. *Armament systems and military equipment*. 2(54), 51-60. **4. Ilchenko, M. E.**, **Narytnyk, T. N., Slyusar, V. I.** (2014), Directions for the creation of tropospheric stations of a new generation. *Digital technologies.* 16, 8-18. **5. Masesov, M. O.**. **Subach, I. Y, Rudenko, D. M., Stanovich, O. V.,** (2014). Prospects for the use of digital charting in special purpose tropospheric communication stations. *Collection of scientific papers VITI DUT,* 1, 43-48. **6. Rudenko, V. I., Zinchenko, M. O., Bondarenko, L. O., Lazuta, R. R.,** (2022). Selection and justification of the structure of the special purpose tropospheric communication system taking into account the application of innovative technologies. *Modern information technologies in the sphere of security and defense,* 3(45), 75-82. **7. Chaika, E. I.**, **Shtonda, R. M.,** (2023). Modern approaches to the development of small-sized digital tropospheric communication stations. In: *Prospects for the development and application of modern communication systems and means in the interests of troop management: materials of the scientific and practical conference*: NANGU, 10. **8. Kravchuk, S. O.,** (2015). Principles of creation of portable tropospheric radio relay stations. In: *Problems of telecommunications: materials of the International Scientific and Technical Conference*. Kyiv : NTUU KPI, 254-256. **9. Kravchuk, S. O.,** (2016). Portable tropospheric radio relay communication station. In: *Problems of telecommunications: materials of the International Scientific and Technical Conference.* Kyiv: NTUU KPI, [online]. Available at: http://conferenc.its.kpi.ua/proc/article/view/709 [Accessed : 15 March 2023]. **10. Rudenok, V. I.**, **Bondarenko, O. E., Sergienko, A. V, Ostapuk, O. I.,** (2018). Calculation of access zones by radio relay and tropospheric means of communication. *Collection of scientific papers VITI.* 3, 87-93.

DOI:**10.33099/2311-7249/2023-47-2-31-40**

УДК: 351.354: 354: 355.359

Машталір Вадим Віталійович *(доктор історичних наук, професор)*
Гудима Олег Петрович *(кандидат технічних наук, старший науковий співробітник)*

Національний університет оборони України, Київ, Україна

КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ФОРМУВАННЯ МОДЕЛІ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ СИТУАЦІЙНОГО ЦЕНТРУ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Початок агресії російської федерації проти України та хід збройного протистояння формує потребу в якісному інформаційно-аналітичному забезпеченні управлінської діяльності. Аналіз останніх наукових публікацій свідчить, що питання системного (комплексного) підходу до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України, як органу інформаційно-аналітичного забезпечення, не розглядалися. Метою статті є формування концептуального підходу до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України для забезпечення реагування на кризові ситуації. Під час опрацювання статті було застосовано методи аналізу, синтезу, аналогії, декомпозиції, структурного синтезу, моделювання, експертні методи. Опрацьований концептуальний підхід дозволив виокремити та опрацювати орієнтовні завдання і функції Ситуаційного центру Міністерства оборони України. Крім того, запропоновано його організаційну структурну модель, враховуючи категорії «загроза», «кризова ситуація», «ризик» та вимоги чинного законодавства держави. Означене дає підстави для уточнення завдань, функцій і структури Ситуаційного центру Міністерства оборони України. Крім того, запропонований підхід може бути використаний для вироблення завдань, формування функцій та побудови організаційних структур ситуаційних центрів складових сил оборони України й інших центральних органів виконавчої влади. В подальшому дослідження будуть спрямовані на удосконалення алгоритмів роботи та взаємодії Ситуаційного центру Міністерства оборони України з ситуаційними центрами центральних органів виконавчої влади держави.

Ключові слова*: кризова ситуація, ситуаційний центр, реагування, концептуальний підхід.*

Вступ

Широкомасштабне вторгнення російської федерації в Україну ще раз підтвердило тезу, що характер сучасних конфліктів має гібридний характер, ознаками якого є [1]: «використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на досягнення раптовості, захоплення ініціативи та отримання психологічних переваг для використання в дипломатичних діях; масштабні і стрімкі інформаційні, електронні і кібернетичні операції; прикриття воєнних і розвідувальних дій у поєднанні з економічним тиском». Означене актуалізує підвищення якості інформаційно-аналітичного забезпечення управлінської діяльності з метою завчасного прогнозування (виявлення) «гібридних» дій.

Для підвищення спроможностей сектору безпеки і оборони України (далі – СБіО) та сил оборони (далі – СО) в зазначеному напрямі видано Указ Президента України від 18 червня 2021 року № 260/2021 «Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року "Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони"» [2]. Цим нормативним документом унормовано розширення та подальший розвиток єдиної мережі ситуаційних центрів (далі – СЦ), до складу якої мають входити Головний СЦ України, Урядовий СЦ, СЦ органів СБіО, СЦ центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі СЦ. Крім того, Указом визначено відповідні завдання для досягнення необхідного результату.

Реалізація заходів, що передбачені зазначеним Указом, потребує наукового супроводу питань створення (розвитку) СЦ Міністерства оборони України (далі – МО України) та, відповідно, формування моделі його організаційної структури та межі відповідальності (перелік завдань, функцій та готовність реагувати на відповідні кризові ситуації (далі – КС).

Аналіз останніх досліджень і публікацій. *Щодо побудови механізмів протидії «гібридним» загрозам*: в [3] авторами розглянуто різні підходи щодо визначення змісту «гібридної» агресії й проаналізовані військові та невійськові

інструменти в збройному протистоянні; в [4] авторами розглянуто питання розробки нового інструментарію щодо комплексного використання військових та невійськових сил в умовах протидії сучасним загрозам; в [5] опрацьовано варіант побудови державної системи управління (координації) заходів протидії гібридним загрозам на базі системи СЦ.

Щодо теоретичних і практичних підходів до нового формату стратегічного керівництва СБіО та військового управління СО: в [6], авторами на підставі аналізу зарубіжного досвіду стратегічного керівництва обороною країн-членів НАТО та системи забезпечення воєнної безпеки і оборони України, сформовано потребу в удосконаленні системи державного управління й міжвідомчої координації зусиль під час КС воєнного характеру; в [7] авторами на основі аналізу вітчизняного законодавства сформовано варіант побудови моделі системи оборони України та здійснено її опис; в [8] автором на основі аналізу досвіду країн світу сформовані пропозиції, що стосуються удосконалення системи забезпечення національної безпеки України та системи державного управління СО в КС.

Щодо визначення місця і ролі СЦ в загальній системі аналізу воєнно-політичної обстановки та реагування на КС: в [1] авторами розглянуті питання аналізу воєнно-політичної обстановки та висвітлено питання щодо використання СЦ для її аналізу; в [9] авторами розроблено методику оцінювання впливу загострення воєнно-політичної обстановки на виникнення КС; в [10] автором зроблено аналіз понятійного апарату в сфері кризового реагування, що використовується в багатьох країнах; в [11] автором запропоновано використовувати єдину методику обробки інформаційних потоків для забезпечення процесів ухвалення рішень на державному рівні; в [12] авторами розглянуто СЦ, як елемент механізму стратегічних комунікацій та проаналізовано СЦ ЗС України; в [13] автором проведено комплексний аналіз досвіду створення СЦ (кризових центрів, інформаційно-аналітичних центрів) в Україні; в [14] розглянуто питання, що стосується необхідності створення в межах СЦ МО України спеціалізованої організаційної структури для реагування на кіберзагрози.

Проведений аналіз останніх досліджень і публікацій свідчить, що питання системного (комплексного) підходу до формування організаційної структури СЦ МО України для забезпечення реагування на КС наразі не розглядалося. Отже, можна констатувати наявну потребу в усуненні невизначеностей, що виникають під час формування СЦ МО України для реагування на КС.

Метою статті є формування концептуального підходу до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України для забезпечення реагування на кризові ситуації.

Виклад основного матеріалу дослідження

Загальний перелік нормативно-правових актів держави [2; 15–18], які формують вимоги щодо інформаційно-аналітичного забезпечення управлінської діяльності представлено на рис. 1.

Рисунок 1 – Перелік національних нормативних документів, які формують вимоги щодо інформаційно-аналітичного забезпечення управлінської діяльності Міністерства оборони України

Розширений перелік завдань в зазначених нормативно-правових актах подано в таблиці 1, де передбачено створення (розширення, розвиток):

мережі СЦ у державних органах (в межах системи національних стратегічних комунікацій);

мережі СЦ моніторингу та аналізу ризиків з метою запобігання загрозам для об'єктів критичної інфраструктури;

системи СЦ СБіО для оперативного прийняття рішень у сфері оборони;

мережі галузевих СЦ кібербезпеки;

єдиної мережі СЦ.

З огляду на означене, з метою інформаційно-аналітичного забезпечення виконання функції управління державою, передбачено створення низки мереж (систем) СЦ в різних сферах діяльності держави, робота яких потребує синхронізації та забезпечення надійного обміну інформацією. Зважаючи на означене, виникає потреба опрацювати підхід до інтеграції відповідних елементів всіх зазначених мереж (систем) СЦ для конкретного СЦ органу державної влади, відповідно до його завдань і функцій.

Таблиця 1

Завдання щодо створення (розвитку) ситуаційних центрів у нормативно-правових актах України

Назва нормативно-правового документу	Окремі завдання щодо створення (розвитку) ситуаційних центрів
Указ Президента України від 14 вересня 2020 року № 392/2020 «Про Стратегію національної безпеки України»	Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме: оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей; ефективне стратегічне планування і кризовий менеджмент, зокрема впровадження універсальних протоколів реагування на КС та відновлення з урахуванням рекомендацій НАТО. З метою системного захисту України від загроз національній безпеці необхідним є розвиток СБіО. Для цього Україна: «…створить систему ефективного управління та координації діяльності органів СБіО, удосконалить її архітектуру; …завершить створення національної системи кібербезпеки, сформує сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнить систему їх координації;…» та інше.
Указ Президента України від 25 березня 2021 року № 121/2021 «Про Стратегію воєнної безпеки»	Визначено пріоритет досягнення цілей державної політики у воєнній сфері, сфері оборони і військового будівництва – запровадження об'єднаного керівництва з підготовки та ведення всеохоплюючої оборони України, який буде реалізований шляхом виконання таких основних завдань: «створення системи комплексного стратегічного аналізу воєнних загроз національній безпеці України; координація діяльності розвідувальних органів; розвиток об'єднаних розвідувальних спроможностей СО з метою отримання повної та достовірної упереджувальної інформації для своєчасного ухвалення рішень щодо забезпечення воєнної безпеки держави; упровадження сучасних інформаційних та космічних технологій; автоматизація управлінських процесів і цифровізація діяльності в СО України з відповідним рівнем захищеності інформації, що обробляється; розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохоплюючої оборони України» та інші.
Укази Президента України від 26 травня 2020 року № 203/2020 «Про Річну національну програму під егідою Комісії Україна – НАТО на 2020 рік» та від 11 травня 2021 року № 189/2021 «Про Річну національну програму під егідою Комісії Україна – НАТО на 2021 рік»	Визначено завдання (на 2021 рік) стосовно створення: системи національних стратегічних комунікацій: «…створення мережі СЦ державних органів…» та інше; Національної системи стійкості: «…формування єдиної нормативно-правової бази у сфері планування та реагування на КС та загрози з метою забезпечення координації дій державних органів у таких ситуаціях…»; державної системи захисту критичної інфраструктури: «…створення мережі СЦ моніторингу та аналізу ризиків для запобігання загрозам для об'єктів критичної інфраструктури, що досягається виконанням таких пріоритетних завдань: формування нормативно-правової бази для функціонування СЦ; створення ефективної системи обміну інформацією між суб'єктами та об'єктами державної системи захисту критичної інфраструктури для прогнозування можливих загроз та запобігання їм…»; системи управління СО: «…розбудова спільної структури командування, контролю та координації СО на стратегічному, оперативному та тактичному рівнях, сумісну із системами військового керівництва держав – членів НАТО; нарощення можливостей СЦ складових СБіО, що досягається виконанням пріоритетного завдання зі створення системи СЦ СБіО для оперативного прийняття рішень у сфері оборони…»; умови для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави: «…створення єдиної мережі галузевих СЦ кібербезпеки, що здатна забезпечити оперативне реагування на кіберзагрози на рівні, який відповідає стандартам НАТО…» та інше.
Указ Президента України від 18 червня 2021 року № 260/2021 «Щодо удосконалення мережі СЦ та цифрової трансформації сфери національної безпеки і оборони»	1. Визнати за необхідне розширення та подальший розвиток єдиної мережі СЦ, до складу якої мають входити Головний СЦ України, Урядовий СЦ, СЦ органів СБіО, СЦ центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі СЦ. 2. Забезпечити: подальший розвиток мережі СЦ, використовуючи інформаційно-аналітичну систему Головного СЦ України; можливість розгортання резервних СЦ у запасних резервних (міських, позаміських) пунктах управління, а також рухомих СЦ для забезпечення стійкості та живучості системи управління державою в особливий період, зокрема в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення КС, що загрожують національній безпеці України та інше.

Спираючись на положення теорії організації, загальна схема взаємодії елементів управління має вигляд наведений на рис. 2 [19]:

Рисунок 2 – Загальна схема взаємодії елементів управління

На основі розглянутої схеми пропонується концептуальний підхід до формування моделі організаційної структури СЦ МО України для реагування на КС, а саме: визначення мети СЦ, його завдань і функцій та формування моделі організаційної структури СЦ.

Мета (цілі) СЦ органу державного управління) – визначаються відповідно до положення про орган державного управління в інтересах якого буде функціонувати СЦ.

Під час формування завдань і функцій організації СЦ відповідного органу державного управління доцільно врахувати:

вимоги нормативно-правових документів держави та відомчих документів;

перелік загроз (реагування на які є сферою відповідальності органу державного управління);

перелік КС (згідно до сфери відповідальності органу державного управління);

ризики негативних наслідків від настання КС (сформовані у відповідному органі державного управління).

Варто зазначити, що під час формування завдань і функцій СЦ додатково залучено такі категорії, як «загроза», «кризова ситуація», «ризик», зміст яких наведено в таблиці 2.

Таблиця 2

Зміст категорій «загроза», «кризова ситуація», «ризик»

Визначення категорії «загроза»	Визначення категорії «кризова ситуація»	Визначення категорії «ризик»
Загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [20]. *Загрози гібридного типу* – різновид загроз національній безпеці, реалізація яких спричиняє синергетичний ефект від одночасного застосування комбінованих методів впливу, які часто мають прихований характер або маскуються під інші процеси у рамках правового поля [21]. *Загроза* – можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь [32].	*Кризова ситуація* – крайнє загострення суперечностей, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні [22]. *Кризова ситуація* – порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів [23]. *Кризова ситуація* – стан, що характеризується крайнім загостренням суперечностей, значною дестабілізацією становища в будь-якій сфері діяльності, регіоні, державі, у тому числі значним порушенням умов функціонування основних сфер життєдіяльності суспільства і держави, й потребує вжиття комплексу заходів для стабілізації ситуації та відновлення якості життя населення, умов функціонування суспільства і держави на рівні, не нижчому за докризовий. Однією з передумов розвитку КС може бути виникнення надзвичайної ситуації [21].	*Ризик* – це ймовірність виникнення збитків або недоотримання прибутків порівняно з варіантом, що прогнозується [24, 25]. *Ризик* – небезпека несприятливого кінця на одну очікувану подію [24, 26]. *Ризик* – це потенційна можливість того, що під час реалізації функцій, процесів та операцій, спрямованих на досягнення встановленої мети (місії), цілей і виконання завдань, можуть виникнути обставини, що призведуть до втрат ресурсу, небезпеки або небажаного результату у майбутньому [27].

Наведені у таблиці 2 категорії дають змогу висвітлити питання реагування на КС, включно з періодом, який передує настанню кризової ситуації та період усунення її наслідків (розмір можливої шкоди від них). Співзв'язок (співвідношення) вищезазначених категорій подано на рис. 3.

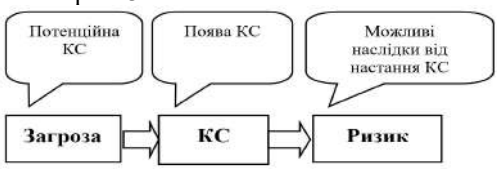


Рисунок 3 – Орієнтовна модель співзв'язку (співвідношення) категорій, як «загроза», «кризова ситуація», «ризик»

Особливої уваги заслуговує розгляд питання щодо класифікації КС. Відповідно до Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо» [20].

Водночас, якщо розглянути термін «кризова ситуація», що зазначено в [21] через призму сфер діяльності, які визначені в [20] та враховуючи зміст понять «інформація» та «інформаційний простір» можна припустити, що КС кіберхарактеру є складовою частиною КС

інформаційного характеру. Зважаючи на означене, констатуємо наявність типів кризових ситуацій:

невоєнного характеру: зовнішньополітичні; державні; економічні; інформаційні (в тому числі і КС кіберхарактеру); екологічні (надзвичайні ситуації (далі – НС));

воєнного характеру. Розглядаючи систему понять «кризова ситуація» і «надзвичайна ситуація» з погляду послідовності їх настання, то можна припустити, що КС воєнного характеру є кінцевою складовою і їй передують (можуть передувати) КС в усіх вищезазначених напрямах. Варто констатувати, що поява одночасно всіх вищезазначених КС не є обов'язковою умовою настання КС воєнного характеру.

Отже, визначимо призначення СЦ МО України і запропонуємо орієнтовну модель з формування завдань і функцій цього центру. З урахуванням [28] СЦ МО України призначений для здійснення інформаційно-аналітичної підтримки діяльності під час формування та реалізації державної політики з питань національної безпеки у воєнній сфері. Орієнтовну модель з формування завдань і функцій СЦ МО України подано на рис. 4.

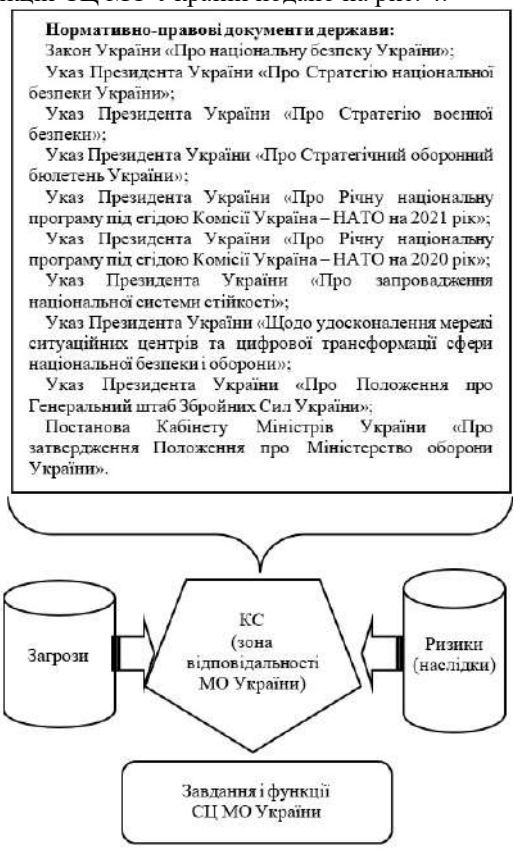


Рисунок 4 – Орієнтовна модель з формування завдань і функцій Ситуаційного центру Міністерства оборони України

Охарактеризуємо елементи орієнтовної моделі з формування завдань і функцій Ситуаційного центру Міністерства оборони України.

Загрози. Відповідно до [16], основними загрозами, на які має реагувати МО України є:

стрімке зростання ролі інформаційних технологій у всіх сферах суспільного життя. Розробляються системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері штучного інтелекту, створення нових матеріалів, робототехніки та автономних безпілотних апаратів;

зовнішня і внутрішня деструктивна пропаганда з використанням суперечностей у суспільстві, розпалом ворожнечі, провокуванням конфліктів, підривом суспільної єдності. Крім того, спостерігається відсутність цілісної інформаційної політики держави, а слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози;

недостатня ефективність державних органів, що ускладнює вироблення і реалізацію ефективної політики;

загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України;

загострюються змагання між Сполученими Штатами Америки і Китайською Народною республікою за світове лідерство. Посилюється міжнародна конкуренція із застосуванням усіх інструментів національної сили – політико-дипломатичних, воєнних, економічних, інформаційно-психологічних, кіберзасобів. Її наслідки проявляються у Східній Європі, на Близькому Сході і у Північній Африці, Південно-Східній Азії, Арктиці, в інших регіонах;

зростають виклики трансатлантичній та європейській єдності, що може спричинити ескалацію наявних і виникнення нових конфліктів. Ситуацією намагається скористатися російська федерація, яка продовжує збройну агресію проти України;

російська федерація використовує Чорноморсько-Каспійський регіон, окупований Крим як «міст» на Балкани, у Середземномор'я, на Близький Схід і у Північну Африку. Для зміцнення позицій у Європі російська федерація застосовує енергетичну та інформаційну «зброю», намагається впливати на внутрішньополітичну ситуацію у європейських державах, підживлює тривалі конфлікти, збільшує військову присутність у Східній Європі тощо.

Кризові ситуації. До КС, реагування на які є сферою відповідальності МО України можна віднести тільки КС воєнного характеру.

Ризики. Зважаючи на нормативно-правові документи, управління ризиками у сфері воєнної безпеки передбачає прийняття відповідних рішень та здійснення заходів, спрямованих на їх зменшення. Основними ризиками у цій сфері можуть бути [15]:

ухвалення стратегічно помилкових рішень у воєнній сфері на підставі неякісного аналізу

реальних і потенційних воєнних загроз національній безпеці;

недостатні інвестиції в розвиток сил оборони, неефективний розподіл видатків на оборону України і витрачання державних ресурсів на утримання безперспективного озброєння, військової та спеціальної техніки;

недостатній рівень взаємодії і неузгодженість заходів, що здійснюються СО, іншими складовими СБіО, відсутність належної координації їх дій з іноземними партнерами та міжнародними організаціями в ході підготовки до збройного захисту України у разі збройної агресії або збройного конфлікту, а також відбудовного періоду після закінчення воєнних дій;

неспроможність забезпечити відсіч і стримування збройної агресії проти України з боку російської федерації традиційними формами та способами збройної боротьби, зважаючи на незрівнянну різницю у воєнних потенціалах;

недостатні спроможності Збройних сил України (далі – ЗС України) та інших складових СО з охорони повітряного простору та протиповітряного прикриття важливих державних і військових об'єктів, недостатні військово-морські спроможності, у тому числі щодо охорони підводного простору в межах територіального моря України, берегової оборони, а також захисту національних інтересів України в Азовському і Чорному морях.

За результатами проведеного дослідження [2, 15–18, 20, 21, 28–31], можна виокремити такі орієнтовні завдання СЦ МО України:

організація і здійснення моніторингу інформаційного простору, обробка інформації та її узагальнення з метою забезпечення діяльності керівництва МО України, здійснення прогнозування розвитку ситуації у визначених сферах відповідальності МО України;

здійснення (в межах компетенції) аналізу воєнно-політичної обстановки, прогнозуванні, виявленні та визначенні рівня воєнної загрози національній безпеці України;

участь у створенні та функціонуванні системи комплексного стратегічного аналізу воєнних загроз національній безпеці України;

оцінювання наявних (можливих) ризиків у сфері оборони, налагодження взаємодії та обміну інформацією між суб'єктами оцінювання ризиків національної безпеки і стану відповідних спроможностей;

участь у плануванні та здійсненні заходів (у межах компетенції) щодо протидії і нейтралізації воєнно-політичних ризиків, викликів, загроз застосування воєнної сили проти України;

завчасне виявлення та аналіз (в межах компетенції) КС, підготовка проєктів відповідних рішень щодо підготовки держави до оборони, реагування на КС;

підтримка достатнього рівня забезпечення готовності до реагування МО України в умовах виникнення загроз і настання КС, підтримання функціонування базових елементів національної системи стійкості;

забезпечення здатності (в межах компетенції) МО України швидко адаптуватися до змін безпекового середовища, протистояти воєнним загрозам, безперебійно функціонувати до і під час воєнного конфлікту, а також відновлюватися після його завершення;

оперативне інформаційно-аналітичне забезпечення керівництва МО України з прийняття управлінських рішень в НС та КС;

проведення керівництвом МО України службових нарад та інших відповідних заходів з використанням інформаційно-телекомунікаційних систем в режимі реального часу;

організація і підтримання постійної взаємодії з обміну інформацією між Головним СЦ при Апараті Ради національної безпеки і оборони України (далі – РНБО), Національним координаційним центром кібербезпеки РНБО, Урядовим СЦ, СЦ центральних органів виконавчої влади, органів військового управління (стратегічного рівня) та органів місцевої влади, інформаційно-аналітичними групами (центрами);

підтримка інформаційного і програмно-технічного середовища та забезпечення доступу до загальнодержавної системи оперативної, архівної інформації підтримки прийняття рішень органами виконавчої влади всіх рівнів;

забезпечення розвитку спроможностей МО України в сфері стратегічних комунікацій;

забезпечення розвитку спроможностей МО України в сфері кібербезпеки, кіберзахисту і кібероборони під час підготовки та ведення всеохоплюючої оборони України.

Крім того, слід зазначити такі орієнтовні функції СЦ МО України:

забезпечення моніторингу стану МО України;

здійснення збору, обробки інформації про стан різних сфер національної безпеки України (складових СО);

здійснення оповіщення керівництва МО України, координація та контроль за виконанням заходів з ліквідації НС і КС;

введення в дію та контролювання механізму реагування на НС і КС, визначеного керівництвом;

здійснення оцінювання ситуації, прогнозування її розвитку та можливих негативних наслідків з допомогою застосування сучасних інформаційних технологій;

здійснення інформаційно-аналітичної підтримки керівництва МО України під час формування рішення та прогнозування наслідків проєктів управлінських рішень за результатами проведеного моделювання їх реалізації;

здійснення експертної оцінки проєктів управлінських рішень та підготовка пропозицій щодо їх оптимізації;

забезпечення проведення керівництвом МО України нарад та інших відповідних заходів з використанням інформаційно-телекомунікаційних систем МО України в режимі реального часу;

підтримання та контролювання, в межах компетенції, захищеного інформаційного і

програмно-технічного середовища та загальнодержавної системи доступу до оперативної й архівної інформації;

організація впровадження до СЦ сучасних інформаційних технологій для прийняття обґрунтованих управлінських рішень;

забезпечення удосконалення методичних підходів до діяльності СЦ, а саме, організування розробки засад оцінювання ризиків національній безпеці й науково-математичного апарату щодо прогнозування, запобігання та реагування на ризики та КС на різних етапах їх розвитку; удосконалення системи забезпечення кібербезпеки для забезпечення гарантованої кіберстійкості інформаційних ресурсів МО України;

забезпечують організацію обміну досвідом з Європейським Центром передового досвіду з протидії гібридним загрозам;

організовують впровадження адаптивних алгоритмів узгоджених дій щодо запобігання та реагування на загрози та КС на різних етапах їх розвитку;

забезпечують ефективне стратегічне планування і кризовий менеджмент, зокрема, впровадження універсальних протоколів реагування на КС з урахуванням досвіду НАТО;

здійснюють накопичення інформації про стан та діяльність МО України;

беруть участь в опрацюванні інформаційно-аналітичних матеріалів про стан ЗС України для їх подання керівництву держави;

беруть участь у впровадженні сучасних інформаційних та космічних технологій, автоматизації управлінських процесів і цифровізації діяльності в МО України з відповідним рівнем захищеності інформації, що обробляється;

беруть участь у розгортанні захищеної мережі обміну інформацією між органами управління СО, що відповідає вимогам до захисту інформації;

беруть участь у впровадженні інформаційних технологій (інформаційних систем) в управління військами і зброєю, захисту інформації, розвідки та логістики у воєнній сфері;

беруть участь у впровадженні програмно-проєктного управління оборонними ресурсами, планів утримання і розвитку відповідних складових СО, забезпечення виконання державних цільових програм;

беруть участь, в межах повноважень передбачених законом, у міжнародному співробітництві за воєнно-політичним, військово-технічним та іншими напрямами з відповідними органами іноземних держав і міжнародними організаціями.

Означені вище завдання та функції СЦ МО України дають змогу візуалізувати модель організаційної структури СЦ МО України (враховуючи категорії «загроза», «кризові ситуації», «ризик» (наслідки від настання КС) (рис. 5).

Слід зазначити, що загрози, КС і ризики групуються за напрямами з використанням експертних методів, які в організаційній структурі відображаються відповідними модулями (загрози – модулі 1…L, КС – модулі 2…M, ризики – модулі 3…N).

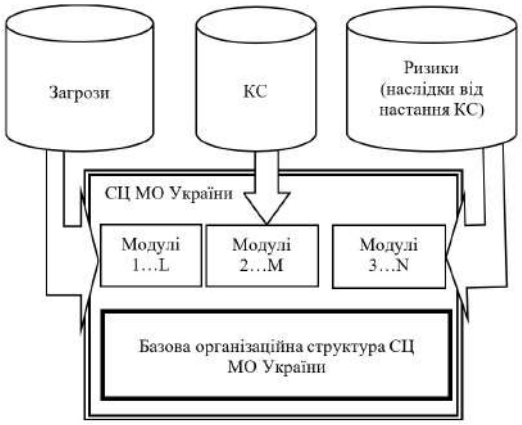


Рисунок 5 – Модель організаційної структури Ситуаційного центру МО України

Під базовою організаційною структурою розуміємо перелік елементів (підрозділів), які забезпечують цілодобове функціонування та попередній аналіз (обробку) інформації, що надходить; штаб реагування на КС, який здійснює формування рішень на реагування; технічний підрозділ.

Представлена на рис. 5 модель з урахуванням вимог нормативно-правових документів [2; 15–18], аналіз яких був проведений вище, прийме вигляд зображений на рис. 6, де додатково введені елементи (модулі) вищезазначених мереж СЦ, а саме: моніторингу об’єктів критичної інфраструктури (модуль P); стратегічних комунікацій (модуль R); кібербезпеки (модуль S)), які будуть забезпечувати обмін інформацією та координацію з вищезазначеними мережами.

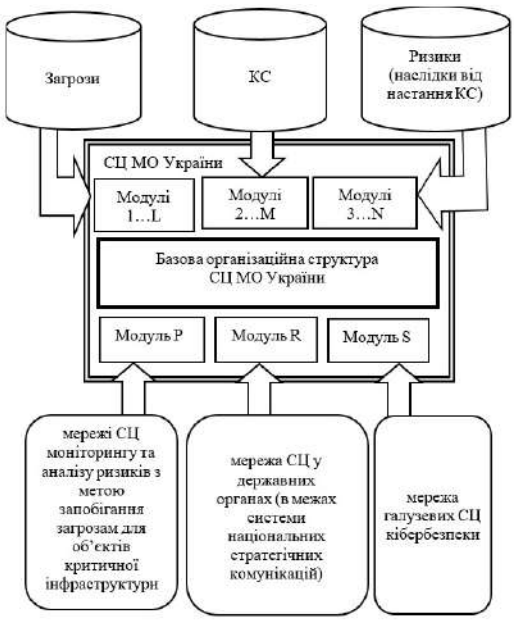


Рисунок 6 – Модель організаційної структури СЦ МО України (враховуючи категорії «загроза», «кризові ситуації», «ризик»(наслідки) та вимоги чинного законодавства держави)

Висновки й перспективи подальших досліджень

В статті опрацьовано концептуальний підхід до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України для забезпечення реагування на кризові ситуації. Такий підхід дав змогу виокремити та опрацювати орієнтовні завдання і функції Ситуаційного центру Міністерства оборони України. А також – запропонувати організаційну структурну модель, враховуючи категорії «загроза», «кризова ситуація», «ризик» та вимоги чинного законодавства держави.

Практичною значущістю отриманих результатів дослідження є можливість уточнення завдань, функцій і структури Ситуаційного центру Міністерства оборони України, а також вироблення завдань, формування функцій та побудови організаційних структур ситуаційних центрів складових сил оборони України й інших центральних органів виконавчої влади.

У подальшому, дослідження будуть спрямовані на удосконалення алгоритмів роботи та взаємодії Ситуаційного центру Міністерства оборони України з ситуаційними центрами центральних органів виконавчої влади держави.

Список бібліографічних посилань

1. Бочарніков В.П., Свєшніков С.В., Тимошенко Р.І., Павленко В.І. Технологія аналізу воєнно-політичної обстановки: монографія. Київ : НУОУ ім. Івана Черняховського, 2019. 384 с. **2. Щодо** удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони: Указ Президента України від 18.06.2021 № 260/2021. URL: https://www.president.gov.ua/ documents/ 2602021-39225 (дата звернення: 02.02.2023). **3. Воєнні** аспекти протидії «гібридній» агресії: досвід України: монографія / колектив авторів; за заг. ред. А. М. Сиротенка. Київ: НУОУ ім. Івана Черняховського, 2020. 176 с. **4. Богданович В. Ю.** та ін. Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: монографія. 2 видання, розш. і доп. Київ : НУОУ ім. Івана Черняховського, 2021. 364 с. **5. Hudyma O.** Situational Center as an element of the state management system in counteracting hybrid threats. *Current issues of military specialists training in the Security and Defence Sector under conditions of hybrid threats*: monograph / Scientific editors Boguslaw Pacek, Hennadii Pievtsov, Anatolii Syrotenko. Warsaw: Wydawnictwo Instytutu Bezpieczeństwa i Rozwoju Międzynarodowego. 2021. P. 58–65. URL: https://instytutbirm.pl/wp-content/uploads/2021/03/ Monografia_mm1.pdf. (Accessed : 02.02.2023). **6. Саганюк Ф. В**. та ін. Сектор безпеки і оборони України: стратегічне керівництво та військове управління: монографія / за ред. д. військ. н., проф. І. С. Руснака. Київ, ЦЗ МО та ГШ ЗС України, 2018. 230 с. **7. Тимошенко Р. І., Павліковський А. К., Лобко М. М.** Модель системи оборони України. *Наука і оборона*. 2021. № 1. С. 21–30. DOI: 10.33099/2618-1614-2021-14-1-21-30. **8. Гудима О. П.** Міжнародний досвід побудови систем забезпечення національної безпеки. Висновки для України. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2021. № 3(69). С. 16–25. DOI: 10.30748/ zhups.2021.69.02. **9. Загорка О. М., Поліщук С. В., Коваль В. В., Загорка І. О.** Оцінка впливу загострення воєнно-політичної обстановки на виникнення кризової ситуації: методичний аспект. *Наука і оборона.* 2021. № 2. С. 61–65. DOI: 10.33099/2618-1614-2021-15-2-61-65. **10. Гудима О. П.** Методологічні основи побудови підсистеми антикризового реагування в системі державного управління. *Наукові перспективи.* 2022. Вип. №2(20). С. 54–67. DOI: 10.52058/2708-7530-2022-2(20)-54-67. **11. Домарєв В. В.** Система ситуаційного управління: Теорія, методологія, рекомендації. Київ: Знання України, 2017. 347 с. **12. Сальнікова О. Ф., Посмітюх О. І., Петренко М. І.** Ситуаційний центр як ефективний механізм стратегічних комунікацій. *Інвестиції: практика та досвід*. 2021. № 17. С. 62–66. DOI:10.32702/2306_ 6814.2021.17.62. **13. Гудима О. П.** Національний досвід створення ситуаційних центрів в органах державної влади. *Публічне адміністрування та національна безпека*. 2020. № 8(16). С. 104–111. https://doi.org/10.25313/2617-572X-2020-8-6446. **14. Живило Є. О.** Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави. *Актуальні проблеми державного управління*. 2022. № 1(60). С. 27-41. DOI: https://doi.org/10.26565/1684-8489-2022-1-02. **15. Про Стратегію** воєнної безпеки: Указ Президента України від 25.03.2021 № 121/2021. **16. Про Стратегію** національної безпеки України: Указ Президента України від 14 вересня 2020 р. № 392/2020. **17. Про Річну** національну програму під егідою Комісії Україна – НАТО на 2021 рік: Указ Президента України від 11.05.2021 № 189/2021. URL: https://www.president.gov.ua/documents/1892021-38845 (дата звернення: 02.02.2023). **18. Про Річну** національну програму під егідою Комісії Україна – НАТО на 2020 рік: Указ Президента України від 26 травня 2020 р. № 203/2020. URL: https://www.president.gov.ua/documents/2032020-33861 (дата звернення: 02.02.2023). **19. Городнов В. П., Фык О. В.** Математическое моделирование, оценка эффективности и синтез организационных структур предприятий. Харьков.: изд-во НУА, 2005. 192 с. **20. Про національну** безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 02.02.2023). **21. Про запровадження** національної системи стійкості: Указ Президента України від 27.09.2021 N 479/2021. URL: https://www.president.gov.ua /documents/4792021-40181 (дата звернення: 02.02.2023). **22. Про Раду** національної безпеки і оборони України: Закон України від 5.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80/conv#Text (дата звернення: 02.02.2023). **23. Про критичну** інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL:

https://zakon.rada.gov.ua/laws /show/1882-20#Text (дата звернення: 02.02.2023). **24. Куташенко М. В.** Сутність ризику і причини його виникнення. *Інвестиції: практика та досвід*. 2009. Вип. № 6. С. 45–48. **25. Шарапов О. Д.** Ризикологія в економіці та підприємництві: *Зб. наук. пр. за матеріалами міжнародної науково-практичної конф*. 27–28 березня 2001 року. Київ: Київський національний економічний ун-т; Академія державної податкової служби України, 2001. С. 452. **26. Фере В. А., Романченко О. В.** Методи оцінки фінансового ризику. *Фінанси України*. 1997. № 2. С. 48–53. **27. Методичний** посібник щодо аспектів управління ризиками, як складової системи внутрішнього контролю у розпорядника бюджетних коштів. Київ : Міністерство фінансів України, 2022. 22 с. **28. Про затвердження** Положення про Міністерство оборони України: Постанова Кабінету Міністрів України від 26.11.2014 № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF #Text (дата звернення: 02.02.2023). **29. Про Положення** про Генеральний штаб Збройних Сил України: Указ Президента України від 30.01.2019 № 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (дата звернення: 02.02.2023). **30. Про Стратегічний** оборонний бюлетень України: Указ Президента України від 17.09.2021 № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 02.02.2023). **31. Гудима О. П.** Концептуальний підхід до формування змісту типового положення про ситуаційний центр органу сектору безпеки і оборони. *Наукові перспективи*. 2022. випуск № 4(22). С. 11–23. DOI: https://doi.org/10.52058/2708-7530-2022-4(22)-11-23. **32. Академічний** тлумачний словник. Словник української мови. URL: https://sum.in.ua/s/zaghroza (дата звернення: 02.02.2023).

CONCEPTUAL APPROACH TO THE FORMATION OF A MODEL OF THE ORGANIZATIONAL STRUCTURE OF THE SITUATION CENTER OF THE MINISTRY OF DEFENSE OF UKRAINE

Mashtalir Vadym ***(Doctor of Historical Sciences, Professor)***
Hudyma Oleh ***(Candidate of technical sciences, Senior Research Fellow)***

National Defence University of Ukraine, Kyiv, Ukraine

The beginning of the russian federation's aggression against Ukraine and the course of the armed conflict creates a need for high-quality information and analytical support for management activities. The analysis of recent scientific publications shows that the issues of a systematic (integrated) approach to the formation of a structural model of the organizational structure of the Situation Center of the Ministry of Defense of Ukraine as an information and analytical support body have not been considered. The purpose of the article is to formulate a conceptual approach to creating a structural model of the organizational structure of the Situation Center of the Ministry of Defense of Ukraine to ensure crisis response. The methods of analysis, synthesis, analogy, decomposition, structural synthesis, modeling, and expert methods were used in the course of elaboration of the article. The developed conceptual approach made it possible to identify and elaborate on the approximate tasks and functions of the Situation Center of the Ministry of Defense of Ukraine. In addition, the author proposes its organizational structural model, taking into account the categories of "threat", "crisis situation", "risk" and the requirements of the current legislation of the State. This gives grounds to clarify the tasks, functions and structure of the Situation Center of the Ministry of Defense of Ukraine. In addition, the proposed approach can be used to develop tasks, formulate functions and build organizational structures of situational centers of the components of the defense forces of Ukraine and other central executive bodies. Further research will be aimed at improving the algorithms of work and interaction of the Situation Center of the Ministry of Defense of Ukraine with the situation centers of the central executive authorities of the state.

Key words: *crisis situation, situation center, response, conceptual approach.*

References

1. Bocharnikov, V. P., Sveshnikov, S.V., Tymoshenko, R. I., Pavlenko, V. I., (2019). *The technology of analysis of the military and political situation*: a monograph. Kyiv: NUOU named after Ivan Chernyakhovsky. **2. Regarding** the improvement of the network of situation centers and the digital transformation of the sphere of national security and defense [online], (2021). Decree of the President of Ukraine № 260/2021, June 18. Available at: https://www.president.gov.ua/ documents/ 2602021-39225 [Accessed 02 February 2023]. **3. Military aspects** of countering «hybrid» aggression: experience of Ukraine: monograph (2020). Collective of authors; in general ed. A. M. Syrotenko. Kyiv: NUOU named after Ivan Chernyakhovsky. **4. Bohdanovych, V.Yu. et al.,** (2021). Methodology of integrated use of military and non-military forces and means of the security and defense sector to counteract modern threats to the military security of Ukraine: monograph; 2nd edition, expanded and supplemented. Kyiv : NUOU named after Ivan Chernyakhovsky. **5. Hudyma, O.,** (2021). Situational Center as an element of the state management system in counteracting hybrid threats. Current issues of military specialists training in the Security and Defense Sector under conditions of hybrid threats: Monograph / Scientific editors Boguslaw Pacek, Hennadii Pievtsov, Anatolii Syrotenko. Warsaw: Wydawnictwo Instytutu Bezpieczeństwa i Rozwoju Międzynarodowego. [online]. Available at: https://instytutbirm.pl/wp-content/uploads/2021/03/ Monografia_mm1.pdf. [Accessed 02 February 2023]. **6. Saganyuk F.V. and others,** (2018). The security and

defense sector of Ukraine: strategic leadership and military management: monograph / under the editorship Doctor of Military Sciences, Prof. I.S. Russian Kyiv, Center of the Ministry of Defense and General Staff of the Armed Forces of Ukraine. **7. Tymoshenko, R. I., Pavlikovskyi, A. K., Lobko, M. M.,** (2021). Model of the defense system of Ukraine. *Science and defense*, 1, 21-30. DOI: 10.33099/2618-1614-2021-14-1-21-30. **8. Hudyma, O. P**., (2021). International experience of building national security systems. Conclusions for Ukraine. *Collection of scientific works of the Kharkiv National University of the Air Force,* 3(69), 16-25. DOI: 10.30748/zhups.2021.69.02. **9. Zagorka, O. M., Polishchuk, S. V., Koval, V. V., Zagorka, I. O.,** (2021). Assessment of the influence of the aggravation of the military and political situation on the emergence of a crisis situation: methodological aspect. *Science and defense*, 2, 61-65. DOI: 10.33099/2618-1614-2021-15-2-61-65. **10. Hudyma, O. P.,** (2022). Methodological foundations of the construction of the anti-crisis response subsystem in the state administration system. *Scientific perspectives*, 2(20), 54-67. DOI: 10.52058/2708-7530-2022-2(20)-54-67. **11. Domarev, V. V.,** (2017). System of situational management: Theory, methodology, recommendations. Kyiv: Knowledge of Ukraine. **12. Salnikova, O. F., Posmityukh, O. I., Petrenko, M. I.,** (2021). The situational center as an effective mechanism of strategic communications. *Investments: practice and experience,* 17, 62-66. DOI:10.32702/2306_6814. 2021.17.62. **13. Hudyma, O. P.,** (2020). National experience of creating situational centers in state authorities. *Public administration and national security,* 8(16), 104-111. https://doi.org/10.25313/2617-572X-2020-8-6446.

14. Jivilo, E. O., (2022). The Situation Center of the Ministry of Defense of Ukraine is a model for early detection and analysis of crisis situations in the state security sector. *Actual problems of public administration*, 1(60), 27-41. DOI: https://doi.org/10.26565/1684-8489-2022-1-02. **15. On the Military** Security Strategy: Decree of the President of Ukraine №. 121/2021, March 25, 2021. **16. On the National Security** Strategy of Ukraine: Decree of the President of Ukraine №. 392/2020, September 14, 2020. **17. About** the Annual National Program under the auspices of the Ukraine-NATO Commission for 2021: Decree of the President of Ukraine № 189/2021, May 11, 2021. **18. About** the Annual National Program under the auspices of the Ukraine-NATO Commission for 2020: Decree of the President of Ukraine №. 203/2020, May 26, 2020. **19. Horodnov, V. P., Fyk, O. V.,** (2005). Mathematical modeling, efficiency assessment and synthesis of organizational structures of enterprises. Kharkiv: NUA publishing house. **20. On the national security** of Ukraine: Law of Ukraine № 2469-VIII, June 21, 2018. **21. On the introduction** of the national sustainability system: Decree of the President of Ukraine № 479/2021, September 27, 2021. **22. About the** National Security and Defense Council of Ukraine: Law of Ukraine № 183/98-VR, March 5, 1998. **23. On critical** infrastructure: Law of Ukraine № 1882-IX, November 16, 2021. **24. Kutashenko, M. V.,** (2009). The essence of the risk and its causes. *Investments: practice and experience,* 6, 45-48. **25. Sharapov, O. D.,** (2001). Riskology in economics and entrepreneurship: *Collection. of science pr. based on the materials of the international scientific and practical conference.* March 27-28, Kyiv: Kyiv National University of Economics; Academy of the State Tax Service of Ukraine. **26. Fere, V. A., Romanchenko, O. V.,** (1997). Methods of financial risk assessment. *Finances of Ukraine*, 2, 48-53. **27. Methodical** manual on aspects of risk management as a component of the internal control system of the manager of budget funds, (2022). Kyiv: Ministry of Finance of Ukraine, 22. **28. On the approval** of the Regulation on the Ministry of Defense of Ukraine: Resolution of the Cabinet of Ministers of Ukraine №. 671, November 26, 2014. **29. On the Regulations** on the General Staff of the Armed Forces of Ukraine: Decree of the President of Ukraine № 23/2019, January 30, 2019. **30. About the Strategic** Defense Bulletin of Ukraine: Decree of the President of Ukraine № 473/2021, September 17, 2021. **31. Hudyma, O. P.,** (2022). A conceptual approach to the formation of the content of the standard provision on the situational center of the body of the security and defense sector. *Scientific perspectives*, 4(22), 11-23. DOI: https://doi.org/10.52058/2708-7530-2022-4(22)-11-23. **32. Academic** explanatory dictionary. Dictionary of the Ukrainian language [online]. Available at: https://sum.in.ua/s/zaghroza [Accessed : 02 February 2023].

DOI:**10.33099/2311-7249/2023-47-2-41-47**

УДК: 004.056

Сидоркін Павло Григорович [1]
Горліченко Сергій Олександрович [1]
Некоз Василь Сергійович [1]
Шилан Микола Володимирович [2]

[1] ***Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна***
[2] ***Національний університет оборони України, Київ, Україна***

МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ CRAMM ТА COBIT 5 FOR RISK

Метою статті є проведення детального аналізу відомих методів управління ризиками CRAMM та COBIT 5 for Risk для їх використання стосовно мінімізації впливу ризиків на інформаційну безпеку підприємства (організації, установи). Під час написання статті застосовано теоретичні методи, а саме аналіз досліджень і публікацій за тематикою управління ризиками. Зазначений методологічний підхід дає змогу порівняти основні методи управління ризиками. У роботі зазначено, що найбільш поширеними у світі методами та методиками управління ризиками інформаційної безпеки є CRAMM, COBIT for Risk, FRAP, Octave і Microsoft. Проведено ретельний аналіз методів CRAMM і COBIT 5 for Risk. Зазначено що метод CRAMM має етапи ініціювання, ідентифікації й оцінювання IT-активів, оцінювання загроз і вразливостей, визначення ризику. Наведено структуру методології COBIT 5 for Risk, розглянуто компоненти установи стосовно опису функцій і процесів управління ризиками за цією методологією та запропоновано рекомендації щодо впровадження заходів зниження ризиків. Наведено основні переваги та недоліки розглянутих методів управління ризиками. Значимість ризиків інформаційної безпеки зростає через збільшення кількості реалізованих нападів, і з урахуванням їх руйнівного потенціалу. Поряд із визначеними перевагами вони мають і свої обмеження. Зокрема, розглянуті методи ефективно використовуються комерційними компаніями і державними установами, а також можуть бути застосовані під час оцінювання й управління ризиками інформаційної безпеки об'єктів критичної інфраструктури.

Ключові слова: *управління ризиками, потенційна шкода, ранжування ризиків, оцінювання ризиків безпеці інформації, реагування на ризик.*

Вступ

Постановка проблеми. У сучасних умовах агресії російської федерації проти України спостерігається тенденція до зростання кількості нападів на об'єкти критичної інфраструктури і стратегічні промислові об'єкти нашої держави. Це призводить до виведення з ладу систем життєзабезпечення промисловості, що вже спричинило глобальну техногенну катастрофу (знищення греблі *Каховської гідроелектростанції)*. Водночас, ризики інформаційної безпеки (далі – ІБ) входять до категорії найбільш ймовірних ризиків, поряд із природніми катаклізмами, екстремальними погодними умовами та іншими.), Також вони містяться у переліку з шести найбільш критичних ризиків за можливою шкодою. Цей список включає ризики пов'язані із застосуванням зброї масового ураження, природними катаклізмами, погодними аномаліями та нестачею питної води. Рівень захисту об'єктів інформаційної діяльності залежить від ризиків ІБ, що зростають через збільшення кількості реалізованих нападів і з урахуванням їх руйнівного потенціалу. Управління ризиками ІБ та їх підтримка на прийнятному рівні є важливою функцією підприємства (організації, установи) (далі – установа), що реалізується за допомогою комплексних систем захисту інформації. Створення таких систем потребує вибору засобів захисту, що забезпечують зниження впливу потенційних ризиків та виявлених під час аналізу ризиків ІБ без суттєвих витрат на впровадження цих засобів та їх підтримку в робочому стані. Результатом проведеного аналізу ризиків ІБ може бути визначення потрібної та достатньої сукупності засобів захисту інформації, рекомендований перелік організаційних заходів, спрямованих на зниження ризиків ІБ та розроблена (удосконалена) архітектура системи ІБ установи. Це дає змогу створити ефективну систему захисту, яка враховує специфіку діяльності конкретної установи та спрямована на зниження саме її ризиків ІБ. За таких умов процес

управління ризиками складається з двох етапів.

Першим етапом управління ризиками є прийняття рішення відносно ризиків ІБ, що мають бути ідентифіковані та оцінені з погляду шкоди для ІБ установи та ймовірності реалізації ризиків.

Другим етапом управління ризиками є ранжування ризиків щодо визначення пріоритетності під час реагування на ризики для подальшого розроблення плану реагування.

Склад і наповнення наведених етапів залежить від методів управління ризиками та їх оцінювання. Тому питання вибору оптимальних і ефективних методів для управління ризиками ІБ установи та їх оцінювання є важливим науковим завданням. Для вирішення цього завдання потрібно провести аналіз відомих методів управління ризиками.

Аналіз останніх досліджень і публікацій. В Україні розроблено і затверджено низку нормативних документів, що регулюють основні засади інформаційної безпеки, зокрема кібербезпеки стосовно необхідності оцінювання ефективності систем захисту установ та об'єктів критичної інфраструктури, проте єдиного розуміння щодо використання методів оцінювання ризиків ІБ для них не наведено [1; 2]. Водночас, у світі розроблено низку міжнародних стандартів для систем управління інформаційною безпекою, що визначають вимоги до системи управління ІБ управління ризиками, метрики і вимірювання, а також керівництво з їх впровадження. Аналіз цих стандартів проведено у декількох наукових публікаціях. Так, у статті [3] зазначені принципи системного підходу, що мають використовуватися під час оцінювання ризиків безпеки інформації. Докладно описуються лише методи аналізу Magerit та Mehari. В роботі [4] розглянуто загальні положення щодо оцінювання і управління ризиками кібер- і інформаційної безпеки, наведені критерії вибору методів оцінки і управління ризиками та проведено короткий аналіз відомих методів відповідно до критеріїв вибору.

У роботі [5] наведено переваги та недоліки програмного забезпечення для визначення і оцінювання ризиків інформаційної безпеки (CRAMM, CORAS, Risk Watch, OCTAVE, Oracle Crystal Ball) і сформовано ряд рекомендацій щодо доцільності застосування розглянутих програмних засобів. Також у статті [6] проведено аналіз процедур оцінювання інформаційних ризиків з допомогою таких видів програмного забезпечення, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE, що розроблені та функціонують згідно міжнародних стандартів. Слід зазначити, що у роботах [3–6] методологія COBIT for Risk не розглядалась.

Метою статті є проведення детального аналізу методів управління ризиками CRAMM та COBIT 5 for Risk для їх використання стосовно мінімізації впливу ризиків на інформаційну безпеку підприємства (організації, установи).

Виклад основного матеріалу дослідження

Метод аналізу та управління ризиками *CRAMM* (CCTA Risk Analysis and Management Method), розроблений 1985 року у Великобританії і базується на стандартах управління інформаційної безпеки серії BS7799 (переопрацьований в ISO 27000) та описує підхід до якісного оцінювання ризиків [7]. Водночас перехід до шкали значень якісних показників відбувається за допомогою спеціальних таблиць, що визначають відповідність між якісними і кількісними показниками. Оцінювання ризику проводиться на основі аналізу функціонування інформаційних технологій (далі – ІТ), що використовуються в установі з урахуванням цінності ІТ-активу, вразливостей, загроз і ймовірностей їх реалізації відповідно до алгоритму (рис. 1) [3].

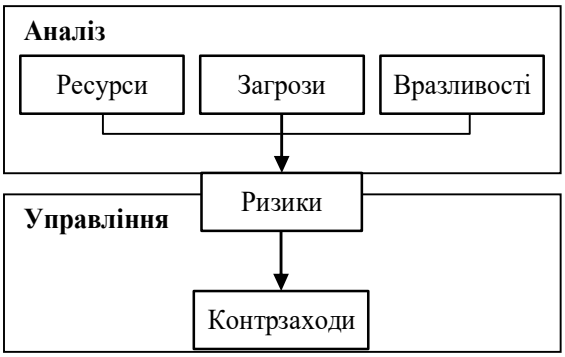


Рисунок 1 – Алгоритм реалізації методу CRAMM

Процес управління ризиками за методом CRAMM складається з таких етапів:

Ініціювання (Initiation). Проводиться серія інтерв'ю із зацікавленими у процесі аналізу ризиків інформаційної безпеки особами, в тому числі з відповідальними за експлуатацію, адміністрування, забезпечення безпеки і використання ІТ-активів, для яких проводиться аналіз ризиків. За підсумками надається формалізований опис області для подальшого дослідження, її меж і визначається склад залучених до аналізу ризиків осіб.

Ідентифікація й оцінювання ІТ-активів (Identification and Valuation of Assets). Визначається перелік ІТ-активів, що використовує організація у визначеній області дослідження. ІТ-активи можуть мати такий вид: дані; програмне забезпечення; фізичні носії.

Для кожного активу визначається його критичність для діяльності організації і спільно з представниками підрозділів, що використовують ІТ-актив для виконання завдань, оцінюються наслідки для діяльності організації від порушення його конфіденційності, цілісності та доступності.

Оцінювання загроз і вразливостей (Threat and Vulnerability Assessment). На доповнення до оцінювання критичності ІТ-активів, важливою є оцінювання ймовірності загроз і вразливостей

ІТ-активів. Метод CRAMM містить таблиці, що описують відповідність між вразливостями ІТ-активів і загрозами, які можуть впливати на них завдяки цим вразливостям. Також маються таблиці, що описують шкоду для ІТ-активів у випадку реалізації цих загроз. Цей етап виконується тільки для найбільш критичних ІТ-активів, для яких недостатньо впровадження базового набору заходів забезпечення ІБ. Визначення актуальних вразливостей і загроз проводиться шляхом інтерв'ювання осіб, що є відповідальними за адміністрування й експлуатацію ІТ-активів. Для решти ІТ-активів метод CRAMM містить набір потрібних базових заходів забезпечення інформаційної безпеки.

Визначення ризику (Risk Calculation) проводиться за виразом:

$$R = P_{\text{реаліз}} \times S_{\text{шк}}, \quad (1)$$

де $P_{\text{реаліз}} = P_{\text{загрози}} \times P_{\text{уразливості}}$ – ймовірність реалізації ризику;

$S_{\text{шк}}$ – шкода ІТ-активам за реалізації загроз.

На етапі визначення ризиків для кожного ІТ-активу визначаються вимоги до набору заходів із забезпечення його інформаційної безпеки за шкалою від «1» до «7», де значенню «1» відповідає мінімальний необхідний набір заходів із забезпечення інформаційної безпеки, а значенню «7» – максимальний.

Визначення ризику (Risk Management). На основі визначеного ризику за виразом (1) розробляється перелік заходів із забезпечення інформаційної безпеки. Для цього використовується спеціальний каталог, що містить до 4 тис. заходів. Рекомендований перелік заходів порівнюється із заходами, які вже застосовані. В підсумку ідентифікуються області, що вимагають додаткової уваги в частині застосування заходів захисту, і області з надлишковими заходами захисту. Ця інформація використовується для формування плану дій зі зміни переліку заходів захисту, що застосовуються в організації з метою приведення рівня ризиків до потрібного стану.

З погляду практичного застосування слід виділити такі переваги методу CRAMM:

апробований метод, за яким накопичено значний досвід і професійні компетенції;

наявність зрозумілого формалізованого опису зводить до мінімуму можливість виникнення помилок за реалізації процесів аналізу та управління ризиками;

наявність засобів автоматизації аналізу ризиків дає змогу мінімізувати трудові витрати і час виконання заходів з аналізу та управління ризиками;

каталоги загроз, вразливостей, наслідків, заходів забезпечення інформаційної безпеки спрощують вимоги до спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками.

Основними недоліками методу CRAMM є:

складність і трудомісткість збору початкових даних, що потребує залучення значних ресурсів усередині організації або ззовні;

великі витрати ресурсів і часу на реалізацію процесів аналізу та управління ризиками інформаційної безпеки;

залучення великої кількості зацікавлених осіб потребує значних витрат на організацію спільної роботи, комунікацій всередині проєктної команди та узгодження підсумків;

неможливість оцінити ризики у грошовому еквіваленті ускладнює використання підсумків оцінювання ризиків інформаційній безпеці за техніко-економічного обґрунтування інвестицій, потрібних для впровадження засобів і методів захисту інформації.

Метод CRAMM застосовується як в урядових, так і в комерційних установах, і є фактично стандартом управління ризиками інформаційної безпеки у Великобританії. Метод може бути використаний в установах, що орієнтовані на міжнародну взаємодію та відповідають міжнародним стандартам управління, які здійснюють первісне впровадження процесів управління ризиками ІБ. Водночас така установа має виділяти значні ресурси і час на впровадження методу CRAMM та використання у своїй діяльності.

Відомим методом управління ризиками є *COBIT 5 for Risk* (Control Objectives for Information and Related Technologies – завдання управління за інформаційними та суміжними технологіями) (далі – COBIT), що є методологію управління інформаційними технологіями. Зазначена методологія розроблена асоціацією ISACA (Information Systems Audit and Control Association) базується на найкращих практиках управління ризиками (COSO ERM, ISO 31000, ISO\IEC 27000) [8]. Методологія COBIT розглядає ризики ІБ стосовно основної діяльності установи, описує підходи до реалізації функції управління ризиками ІБ в установі до процесів якісного аналізу ризиків інформаційної безпеки і управління ними. Структура методології наведена на рис. 2.

Компоненти установи стосовно опису функцій та процесів управління ризиками за методологією COBIT наведені на рис 3. Компонентами функції управління ризиками є: процеси, організаційна структура, культура та поведінка, принципи політики, процедури, інформація, пропозиції та ІТ-сервіси, персонал і компетенції. До процесу управління ризиками слід віднести: процес, що містить ризик, ризикові сценарії – віднесення сценаріїв і паролів, інші документи з бібліотеки COBIT. Під час реалізації функції управління ризиками в установі методологія COBIT виділяє компоненти, що впливають як на ризики інформаційної безпеки, так і на процес управління ними, а саме: принципи політики, процедури організації; процеси; організаційна структура; корпоративна культура, етика і правила поведінки; інформація; ІТ-сервіси, ІТ-інфраструктура і

додатки; персонал, його досвід і компетенції.

Основним елементом аналізу та управління ризиками ІБ згідно з COBIT є ризикові сценарії. Кожний сценарій є «описом події, яка у випадку виникнення, може призвести до невизначеного (позитивного чи негативного) впливу на досягнення цілей організації».

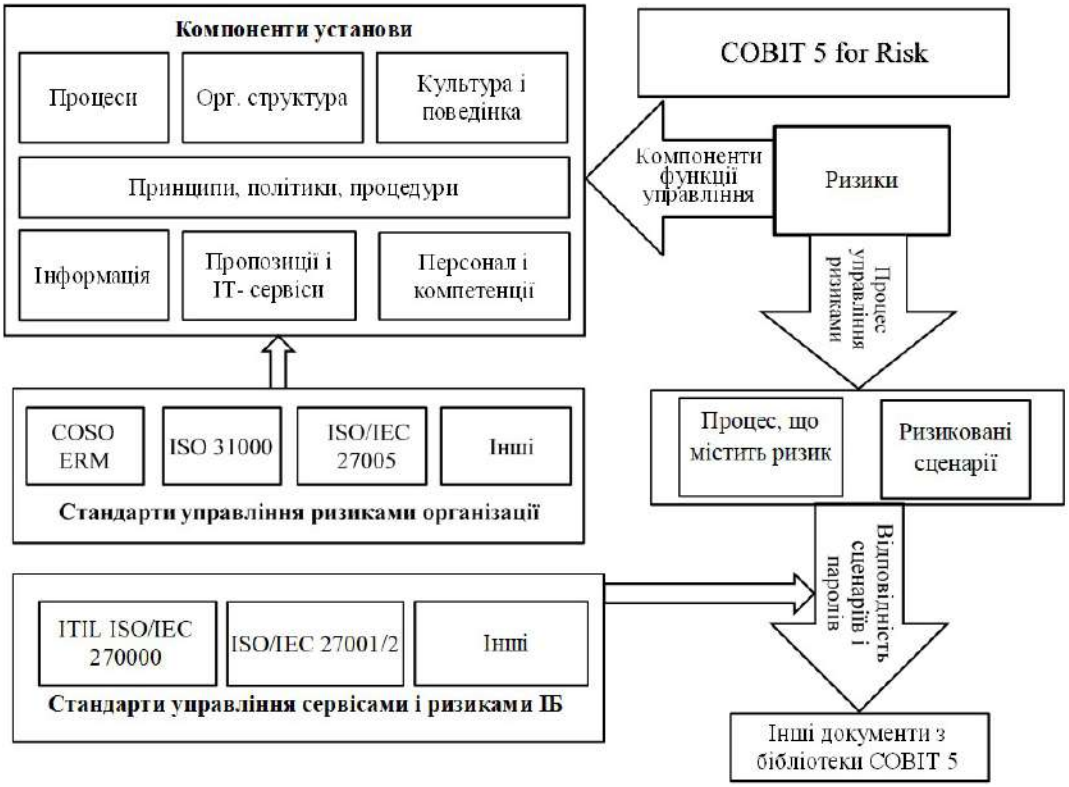


Рисунок 2 – Структура методології COBIT 5 for Risk

Рисунок 3 – Компоненти установи стосовно опису функцій та процесів управління ризиками за методологією COBIT

Методологія містить більш, ніж 100 ризикових сценаріїв, що охоплюють категорії впливу: створення та обслуговування портфелів IT-проєктів; управління життєвим циклом програми / проєкту; інвестиції в IT; експертиза і навички персоналу IT; операції з персоналом; інформація; архітектура; IT-інфраструктура; програмне забезпечення; неефективне використання IT; вибір та управління постачальниками IT; відповідність нормативним вимогам; геополітика; викрадання елементів інфраструктури; шкідливе програмне забезпечення; логічні напади; техногенний вплив; навколишнє середовище; природні явища; інновації.

Для кожного сценарію визначений ступінь його належності до конкретного типу ризиків:

стратегічні ризики, що пов'язані з втраченими можливостями використання IT для розвитку та підвищення ефективності основної діяльності організації;

проєктні ризики, що пов'язані з впливом IT на створення чи розвиток існуючих процесів організації;

ризики управління IT і надання IT-сервісів, що пов'язанні із забезпеченням доступності, стабільності та надання користувачам IT-сервісів з потрібним рівнем якості, проблеми, що можуть призвести до втрат у основної діяльності організації.

Кожен ризиковий сценарій містить таку інформацію:

тип джерела загрози – внутрішній або зовнішній;

тип загрози – зловмисна дія, природне явище, помилка;

опис події – доступ до інформації, знищення, внесення змін, розкриття інформації, крадіжка;

типи активів (компонентів) організації, на які впливає подія – люди, процеси, IT-інфраструктура;

час події.

У випадку реалізації ризикового сценарію діяльності організації заподіюється шкода. Таким чином, під час аналізу ризиків інформаційної безпеки у відповідності з методологією COBIT виявляються актуальні для організації ризикові сценарії і заходи щодо зниження ризиків, спрямованих на зменшення ймовірності реалізації цих сценаріїв. Для кожного з виявлених ризиків проводиться аналіз його відповідності ризик-апетиту установи з подальшим прийняттям одного з таких рішень: уникання ризику; прийняття ризику; передача ризику; зниження ризику.

Подальше управління ризиками ІБ здійснюється шляхом аналізу залишкового рівня ризиків і прийняття рішення про необхідність реалізації додаткових заходів зниження ризиків. Методологія містить рекомендації щодо впровадження заходів зниження ризиків стосовно кожного з типів компонентів організації (рис. 4).

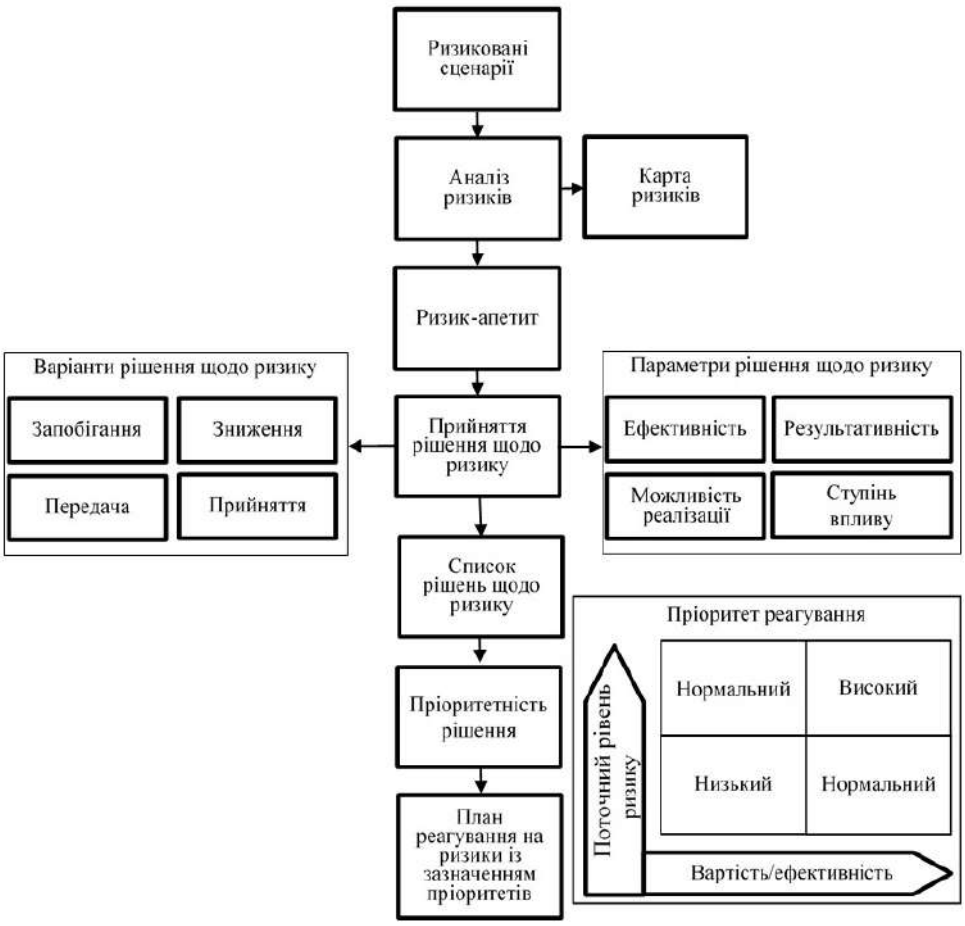


Рисунок 4 – Рекомендації щодо впровадження заходів зниження ризиків

З погляду практичного застосування методології COBIT можна виділити такі переваги:

зв'язок із загальною бібліотекою COBIT і можливість використовувати підходи та «IT-контролі» (заходів зі зниження ризиків) із суміжних областей, які дають змогу розглядати ризики ІБ і заходи щодо їх зниження відносно впливу ризиків на процеси установи;

багаторазово апробований метод, за яким накопичений значний досвід і професійні компетенції, а підсумки якого визнаються міжнародними інститутами;

наявність зрозумілого формалізованого опису методології дає змогу звести до мінімуму помилки під час реалізації процесів аналізу та управління ризиками;

каталоги ризикових сценаріїв та «IT-контролів» дають змогу спростити вимоги щодо спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками;

можливість використання методології під час проведення аудитів дає змогу знизити трудовитрати і потрібний час для інтерпретації підсумків зовнішніх і внутрішніх аудитів.

За таких умов методиці COBIT властиві такі недоліки та обмеження:

складність і трудомісткість збору початкових даних потребує залучення значних ресурсів всередині установи або ззовні;

залучення великої кількості зацікавлених осіб потребує значних витрат на організування їх спільної роботи, виділення часу на комунікації всередині проєктної команди та узгодження підсумків з усіма зацікавленими особами;

відсутність можливості оцінювання ризиків у грошовому еквіваленті ускладнює використання підсумків оцінювання ризиків ІБ під час обґрунтування інвестицій, потрібних для впровадження засобів і методів захисту інформації [28].

Методологія COBIT використовується в установах різних форм власності та є найбільш придатною для великих технологічних підприємств із високим ступенем залежності основної діяльності від інформаційних технологій і мають потрібні ресурси і компетенції для використання цієї методології. В цьому випадку можлива ефективна інтеграція процесів управління ризиками інформаційної безпеки та процесів загального управління IT і досягнення синергетичного ефекту, який дасть змогу оптимізувати витрати на реалізацію процесів аналізу й управління ризиками інформаційної безпеки.

Таким чином, проведений аналіз методу CRAMM та методології COBIT 5 for Risk стосовно процесу управління ризиками інформаційної безпеки установи дав змогу визначити переваги та недоліки зазначених методів. Використання ризиково-орієнтованих підходів, реалізованих у розглянутих методах дає змогу побудувати більш ефективну систему безпеки для установ, захищати в першу чергу найбільш критичні для забезпечення функціонування об'єкти, враховуючи актуальні загрози безпеки і технології, що застосовуються. Також слід відзначити важливість обміну інформацією про ризики, інциденти та загрози для спільної протидії новим викликам і загрозам.

Висновки й перспективи подальших досліджень

Розглянуті методи CRAMM та COBIT 5 for Risk зарекомендували себе як дієві та ефективні стосовно мінімізації впливу ризиків на інформаційну безпеку установ різних форм власності. Зазначені методи можна рекомендувати для застосування в управлінні критичною інфраструктурою з метою забезпечення їх безпеки [9], проте це вимагає належного нормативно-правового регулювання, оскільки від функціонування критичних об'єктів, значною мірою, залежить національна безпека держави. Крім того, потрібно розробляти (удосконалювати) конкретні вимоги, виконання яких дасть змогу забезпечити належний рівень захищеності. Водночас заходи забезпечення безпеки мають обиратися під конкретний об'єкт захисту з урахуванням його характеристик та особливостей функціонування.

Подальші дослідження слід спрямувати на розгляд та порівняльний аналіз інших методів і методик, де реалізовані ризиково-орієнтовані підходи (стандарти NIST SP 800-30 і ISO/IES 27005;2008).

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення: 30.08.2023). **2. Про** рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 14 вересня 2020 року: Указ Президента України від 14 вересня 2020 року № 392/2020. URL:https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 30.08.2023). **3. Потій О. В., Горбенко Ю. І., Замула О. А., Ісірова К. В.** Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки Радіотехніка. 2021. Вип. 206. С. 5–23. **4. Потій О. В., Лєншин А. В.** Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу. Зб. наук. праць Харків. ХУПС. 2010. Вип. 2(24). С. 85–91. **5. Савельєва Т. В., Панаско О. М., Пригодюк О. М.** Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. Вісник Черкаського державного технологічного університету. Сер: Технічні науки. 2018. № 1. С. 81–89. **6. Бучик С. С., Шалаєв В. О.** Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. Наукоємні

технології № 3(35). 2017. С. 215–226. **7. CRAMM** user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001. **8. COBIT 5:** A Business Framework for the Governance and Management of Enterprise ISACA, 2012. **9. Мельничук О.** Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. Державне управління та місцеве самоврядування. 2019. № 3(42). С. 13–27.

METHODS OF MANAGEMENT OF INFORMATION SECURITY RISKS CRAMM AND COBIT 5 for Risk

Sydorkin Pavlo [1]
Horlichenko Serhii [1]
Nekoz Vasyl [1]
Shylan Mykola [2]

[1] ***Institute of Special Communications and Information Protection National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine***
[2] ***National Defence University of Ukraine, Kyiv, Ukraine***

The purpose of the article is to conduct a detailed analysis of known risk management methods CRAMM and COBIT 5 for Risk for their use in minimizing the impact of risks on the information security of the enterprise (organizations, institutions). During the writing of the article, theoretical methods were applied, namely the analysis of research and publications on the topic of risk management. The specified methodological approach makes it possible to compare the main methods of risk management. The work states that the most common methods and techniques of information security risk management in the world are CRAMM, COBIT for Risk, FRAP, Octave and Microsoft. A thorough analysis of CRAMM and COBIT 5 for Risk methods was carried out. It is noted that the CRAMM method has stages of initiation, identification and assessment of IT assets, assessment of threats and vulnerabilities, and risk determination. The structure of the COBIT 5 for Risk methodology is presented, the components of the institution are considered in relation to the description of risk management functions and processes according to this methodology, and recommendations are offered for the implementation of risk reduction measures. The main advantages and disadvantages of the considered risk management methods are given. The importance of information security risks is growing due to the increase in the number of implemented attacks, and taking into account their destructive potential. Along with certain advantages, they also have their limitations. In particular, the considered methods are effectively used by commercial companies and state institutions, and can also be applied during the assessment and management of information security risks of critical infrastructure objects.

Keywords: *risk management, potential harm, risk ranking, information security risk assessment, risk response.*

References

1. On the Fundamental Principles of Ensuring Cybersecurity in Ukraine [online], (2017). Zakon Ukrainy № 2163-VIII. 5 October/ Available at: https://zakon.rada.gov.ua/laws/show/392/2020#Text [Accessed 30 August 2023]. **2. On the Decision** of the National Security and Defense Council of Ukraine 'On the Strategy of National Security of Ukraine [online], (2020). Presidential Decree of Ukraine № 392/2020 of September 14, Available at: https://zakon.rada.gov.ua/laws/show/392/2020#Text [Accessed 30 August 2023]. **3. Potii, O. V., Horbenko, Yu. I., Zamula, O. A., Isirova, K. V.,** (2021). Analysis of Methods for Assessing and Managing Risks in Cyber and Information Security. *Radiotekhnika*, Issue 206, 5-23. **4. Potii, O. V., Lenshin, A. V.** (2010). Research on Methods of Assessing Information Security Risks and Proposals for their Improvement Based on a Systemic Approach. *Collection of Scientific Works*, Kharkiv. KhUPS, Issue 2(24), 85-91. **5. Savelieva, T. V., Panasko, O. M., Pryhodiuk, O. M.** (2018). Analysis of Methods and Tools for Implementing a Risk-Oriented Approach in the Context of Enterprise Information Security. *Bulletin of Cherkasy State Technological University. Series: Technical Sciences*, 1, 81-89. **6. Buchyk, S. S., Shalaiev, V. O.** (2017). Analysis of Instrumental Methods for Determining Information Security Risks in Information and Telecommunication Systems. *Technology-Intensive Technologies*, 3 (35), 215-226. **7. United** Kingdom Central Computer and Telecommunication Agency (CCTA) (2001). CRAMM User Guide, Risk Analysis and Management Method, UK. **8. ISACA** (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise. **9. Melnychuk, O.** (2019). Management of the State's Critical Infrastructure: Basic Methods and Criteria for Object Identification. *Public Administration and Local Government*, 3(42), 13-27.

DOI:**10.33099/2311-7249/2023-47-2-48-54**

УДК: 355:358.4

Ярошенко Ярослав Віталійович

Національний університет оборони України, Київ, Україна

УДОСКОНАЛЕНА ЧАСТКОВА МЕТОДИКА ОЦІНЮВАННЯ РІВНЯ ПІДГОТОВКИ ПОСАДОВИХ ОСІБ, ЯКІ ЗАЛУЧАЮТЬСЯ ДО УПРАВЛІННЯ БОЙОВИМ ПОЛЬОТОМ СПІЛЬНОЇ АВІАЦІЙНОЇ ГРУПИ ПІЛОТОВАНОЇ ТА БЕЗПІЛОТНОЇ АВІАЦІЇ

Під час бойового польоту, управління авіаційним угрупованням пілотованої та безпілотної авіації здійснюється командиром угруповання та офіцерами з бойового управління наземних (повітряних) пунктів управління авіації, а також у повітрі командирами (старшими) груп тактичного призначення. Кожна посадова особа, яка залучається до управління таким угрупованням повинна мати відповідний фактичний рівень підготовки, що впливає на загальний рівень підготовки цих посадових осіб, як команди, яка управляє протягом всього бойового польоту. Оцінювання рівня підготовки посадових осіб, які мають різнорідну спрямованість за існуючими методиками оцінювання рівня підготовки особового складу не дає змогу визначити їх фактичний рівень підготовки та може призвести до зриву виконання бойового завдання авіаційним угрупованням. Тому виникає актуальне наукове завдання стосовно удосконалення існуючого науково-методичного апарату з метою оцінювання загального рівня підготовки посадових осіб різнорідного призначення, які залучаються до управління бойовим польотом авіаційного угруповання пілотованої та безпілотної авіації. Це дозволить під час планування бойового польоту визначати прогнозовану ефективність виконання бойового завдання авіаційним угрупованням та залучати до управління ним посадових осіб, які мають високий рівень підготовки. Дослідження проводилось із застосуванням системного підходу та теорії нечіткої логіки. У статті проведено аналіз існуючих методик оцінювання рівня підготовки особового складу та запропоновано удосконалену часткову методику оцінювання рівня підготовки посадових осіб, що залучаються до управління бойовим польотом спільної авіаційної групи пілотованої та безпілотної авіації. Удосконалена часткова методика, за допомогою математичного апарату нечіткої логіки, дозволяє, на відміну від існуючих, визначати індивідуальний фактичний рівень підготовки посадових осіб, які мають різне призначення та оцінювати загальний фактичний рівень підготовки посадових осіб, які залучені до управління бойовим польотом авіаційного угруповання. Під час дослідження, для імітаційного моделювання визначення рівня підготовки посадових осіб, використовувався пакет прикладних програм Matlab: Simulink та Fuzzy Logic Designer. Запропонована удосконалена часткова методика має важливе практичне значення для військових частин авіації, оскільки може стати дієвим інструментом під час вибору посадових осіб, що будуть здійснювати управління бойовим польотом авіаційного угруповання, підрозділів та військових частин авіації, а також складовою системи підтримки прийняття рішень керівного складу органів військового управління для планування операцій.

Ключові слова: *рівень підготовки, авіація, методика оцінювання, спільна авіаційна група пілотованої та безпілотної авіації, бойовий політ, офіцер з бойового управління, нечітка логіка, управління.*

Вступ

Постановка проблеми. Сучасні військові операції, в тому числі й російсько-українська війна (далі – РУВ), демонструють вплив якості управління на ефективність виконання бойових завдань [1]. Якість управління військовою операцією залежить від рівня підготовки командувача (командира) та особового складу пунктів управління. Існуючі концепції проведення військових операцій передбачають створення угруповань об'єднаних сил, до яких залучаються підрозділи та військові частини різних видів і родів військ, в тому числі й авіації [2].

З метою ефективного управління об'єднаними операціями та забезпечення координації авіаційного угруповання створюється відповідна система управління, що містить наземні та повітряні пункти управління авіацією. Згідно з підходами Командування Повітряних Сил Збройних сил України безпілотну авіацію планується застосовувати спільно з пілотованою [3]. Для ефективного досягнення цієї мети доцільно створювати спільні авіаційні групи (далі – САГ), що об'єднують пілотовану та безпілотну авіацію, зокрема винищувальну, штурмову (бомбардувальну) та безпілотну. Ці формування можуть бути розподілені по групах тактичного призначення: група винищувально-авіаційного прикриття, ударна група та група дорозвідки і позначення цілей. Важливо встановити спільну систему управління, яку має очолювати командир САГ [4]. Система управління авіацією, залежно від роду авіації Повітряних Сил Збройних сил України,

має свої особливості. Так, система управління винищувальної авіації (далі – ВА) для збільшення поля управління та наведення нарощується пунктами наведення авіації (далі – ПНА), а в перспективі й літаками дальнього радіолокаційного виявлення і управління (далі – AWACS). Система управління штурмової авіації (далі – ША) має штатні групи бойового управління (далі – ГБУ) та передових авіаційних навідників (далі – ПАН). Система управління безпілотною авіацією (далі – БпА) може нарощуватися за рахунок допоміжних станцій управління безпілотними літальними апаратами (далі – БпЛА). Крім того, особливістю управління бойовим польотом САГ є автономність та стійкість системи управління через те, що командири груп тактичного призначення (далі – ГТП) у разі виходу з ладу наземних пунктів управління авіації (далі – ПУА) здійснюють управління бойовими порядками у повітрі. Управління бойовим польотом САГ є командною роботою визначених посадових осіб, яку здійснюють командир САГ, офіцери з бойового управління ПУА та командири груп тактичного призначення у повітрі [5; 6].

Успіх виконання бойового завдання САГ залежить як від високого рівня підготовки кожної окремої посадової особи, що приймає участь в управлінні САГ, так і високого рівня командної роботи всіх зазначених вище посадових осіб, проте порядок визначення їхнього рівня підготовки та призначення до бойового розрахунку нормативними документами не визначений. Тому виникає актуальне наукове завдання стосовно удосконалення існуючого науково-методичного апарату з метою оцінювання загального рівня підготовки посадових осіб різнорідного призначення, які залучаються до управління бойовим польотом САГ. Це дозволить під час планування бойового польоту визначати прогнозовану ефективність виконання бойового завдання САГ та залучати до управління нею посадових осіб, які мають високий рівень підготовки.

Аналіз останніх досліджень і публікацій. Питання оцінювання рівня підготовки льотного складу та персоналу державної авіації України розглядалися у роботах [7–9]. Так, перевагою роботи [7] є те, що автори запропонували оцінювати готовність льотного складу винищувальної авіації до бойових дій не за його класною кваліфікацією [9], а за фактичним рівнем підготовки. Недоліком даної методики є те, що вона розглядає оцінювання рівня готовності лише льотного складу винищувальної авіації за визначеними показниками, що не дає змогу оцінювати льотний склад інших родів авіації або особовий склад, який має різнорідні функції та оцінюється за різними показниками. У [8] автори описали погляди, щодо оцінювання рівня підготовленості авіаційного персоналу з погляду безпеки польотів, проте методика оцінювання його підготовленості представлена не була. У [9] автор розглядає методичний підхід щодо оцінювання впливу рівня підготовленості екіпажів на бойову могутність бойового складу тактичної авіації, де пропонує оцінювати рівень підготовленості екіпажів тактичної авіації відповідно до їх класної кваліфікації та загального нальоту на типі повітряного судна. Перевагою цієї роботи є, те що автор розглядає рівні підготовленості екіпажів різних родів авіації, а недоліком – не враховується наявність досвіду участі екіпажу в бойових діях, що має значний вплив на його готовність до бойових дій. Підхід щодо оцінювання рівня навченості органів військового управління тактичного рівня за показником сукупного рівня індивідуальних спроможностей військовослужбовців органу військового управління тактичного рівня та показником їх злагодженості описано в [10]. Перевагою даного підходу є можливість оцінювати рівень індивідуальної підготовленості різних військовослужбовців органу управління тактичного рівня за його теоретичними, практичними навичками та психологічним станом. Недоліком підходу є те, що він оцінює рівень підготовленості військовослужбовців за однаковими показниками і не враховує досвід бойових дій та управлінський досвід військовослужбовців, що не дозволяє в повній мірі визначити їх фактичний рівень підготовки. Методика оцінювання рівня підготовленості військовослужбовців до виконання бойових завдань розглянута в [11]. Перевагою розглянутої методики є можливість оцінити рівень підготовки, як окремого військовослужбовця, так і підрозділу в цілому. Недоліками визначено те, що вона базується на імовірнісних показниках, які важко визначити достовірно. Всі військовослужбовці оцінюються за однаковими показниками, і не враховується бойовий та управлінський досвід. В цілому, означені підходи та методики не розглядають оцінювання посадових осіб, які виконують командну роботу з різнорідними функціями та оцінювання яких здійснюється за різними показниками рівня підготовки. Тому залишається невирішеним наукове завдання щодо оцінювання загального фактичного рівня підготовки різнорідних посадових осіб, які залучаються до управління бойовим польотом САГ, як команди.

Мета статті – вирішення наукового завдання щодо оцінювання загального фактичного рівня підготовки різнорідних посадових осіб, які залучаються до управління бойовим польотом спільної авіаційної групи та удосконалення часткової методики оцінювання їх рівня підготовки за допомогою математичного апарату нечіткої логіки.

Виклад основного матеріалу дослідження.

Якість управління бойовим польотом залежить від рівня підготовки наступних посадових осіб:

командира САГ, який здійснює управління з наземного (повітряного) пункту управління;

офіцера з бойового управління, оператор цільового спорядження БпЛА (далі – ОБУ) ПУА, який здійснює управління САГ за маршрутом, забезпечує пошук наземних цілей в районі ведення повітряної розвідки; здійснює наведення ВА на повітряні цілі та штурмової авіації на наземні цілі.

командири ГТП, які здійснюють управління в групі та взаємодіють з іншими ГТП та наземними (повітряними) ПУА. На основі інформації, що надходить до них від ПУА та БпЛА приймають остаточне рішення щодо застосування авіаційних засобів ураження. У разі загрози втрати льотного складу та літаків від впливу противника приймає рішення на відмову від виконання завдання та повернення на аеродром базування.

Через те, що нормативними документами не визначено порядок призначення посадових осіб, які здійснюють управління бойовим польотом САГ вони зазвичай призначаються відповідно їх класної кваліфікації або загального нальоту (загальної кількості наведень для ОБУ), що не завжди відповідає їх фактичному рівню підготовки або наявному в них бойовому досвіду. Це створює невизначеність у системі управління авіацією, що може створити ризик зриву виконання бойового завдання. Для визначення ризику невиконання бойового завдання, в частині, що стосується системи управління, необхідно детально дослідити ризики, які в собі несе рівень підготовки посадових осіб, які залучаються до управління бойовим польотом САГ. Підходи, які можуть бути використані для вирішення даного питання частково описані в роботах [7; 8], але вони не враховували рівень підготовки посадових осіб, які здійснюють управління на різних ПУА на землі та в повітрі.

З метою вирішення описаних вище проблемних питань автором запропоновано удосконалену методику оцінювання рівня підготовки посадових осіб, які залучаються до управління бойовим польотом САГ (рис.1), яка включає в себе 12 кроків та визначити фактичний рівень підготовки не тільки командира САГ, ОБУ ПУА та командира ГТП, як окремих посадових осіб, а й загальний рівень підготовки цих посадових осіб як команди, яка управляє бойовим польотом САГ [12].

Крок 1: Визначення факторів, що під час управління бойовим польотом САГ створюють ризики для зриву виконання бойового завдання. Оскільки одним з показників якості управління є рівень підготовки особового складу, тому визначимо фактори, що впливають на якість управління командиром САГ, офіцером з бойового управління наземного ПУА, командиром групи тактичного призначення. Наприклад, на рівень підготовки командира САГ, найбільше впливає: рівень освіти, досвід бойових польотів у складі САГ та досвід управління САГ.

Крок 2: Здійснюється формалізація оцінки вхідних факторів ризику як кортеж $< \varepsilon_j, T, K, G >$, де ε_j– назва лінгвістичної змінної, Т – терми лінгвістичної змінної, К – межі визначення лінгвістичної змінної, $G = \{\mu_\varepsilon (X)|X\}$ – функції приналежності лінгвістичної змінної ризику [8].

Наприклад, ε_j – рівень освіти командира САГ; Т = {“тактичний рівень (низький)”, “закінчив курс тактичного рівня L-2 (середній)”, “оперативний рівень або курс оперативного рівня L-3 (достатній)”, “стратегічний рівень або курс стратегічного рівня L-4 (високий)”}; К = [0, 1];

Крок 3: Здійснюється побудова функцій належності на основі нормативних вимог державної авіації України, статистичних показників досвіду управління бойовими діями авіації, або експертних оцінювань.

Наприклад, терм лінгвістичної змінної – рівень освіти ≤ 0,5 – низький, 0,51–0,7 – середній, 0,71-0,9 – достатній, ≥ 0,91 – високий.

Крок 4: Створюється база правил для лінгвістичних змінних: “рівень підготовки командира САГ”, рівень підготовки офіцера з бойового управління наземного ПУ САГ”, рівень підготовки командира групи тактичного призначення САГ” “ЯКЩО-ТО”.

Наприклад, *ЯКЩО* рівень освіти низький, *І* досвід управління САГ високий, *ТО* рівень підготовки середній.

Крок 5: Здійснюється формалізація оцінки вихідного ризику. Визначаються його значення $< \varepsilon_j, T, K, G >$, а також вибір необхідного алгоритму нечіткого висновку (Мамдані або Сугено).

Крок 6: Розрахунок рівня підготовки *і*-ї посадової особи (“рівень підготовки командира САГ”, рівень підготовки офіцера з бойового управління САГ”, рівень підготовки командира групи тактичного призначення САГ”).

Крок 7: Перевірка рівня відповідності рівня підготовки *і*-ї посадової особи необхідному значенню, яке не буде критичним для виконання бойового завдання САГ. У разі невідповідності значення рівня підготовки *і*-ї посадової особи необхідному виконується крок 1 та вносяться зміни вхідних даних.

Крок 8: Створюється база правил для лінгвістичної змінної “загальний рівень підготовки посадових осіб, що залучені до управління САГ” “ЯКЩО-ТО”.

Крок 9: Побудова системи нечіткої логіки (рис. 2). Система нечіткої логіки для *і*-ї посадової особи та всіх, хто здійснює управління в цілому будуються за допомогою графічного набору інструментів Fuzzy Logic Disigner, з комплекту програм MATLAB. Особливістю побудови системи в запропонованій методиці, те що спочатку на першому етапі формуються правила та оцінюються різнорідні посадові особи окремо, а потім формуються правила та оцінюється їх загальний рівень підготовки, як команди. Визначення функцій належності повинно здійснюватися за допомогою статистики та консультацій з авіаційними експертами [13; 14].

Крок 10: Розрахунок загального рівня підготовки посадових осіб, які залучені до управління САГ.

Крок 11: Перевірка відповідності загального рівня підготовки посадових осіб, які залучені до управління САГ необхідному значенню, що дозволить виконати бойове завдання САГ на заданому рівні. У разі неприйнятного значення, вносяться відповідні зміни вхідних даних. У разі прийнятного значення – допуск визначених посадових осіб до управління бойовим польотом САГ.

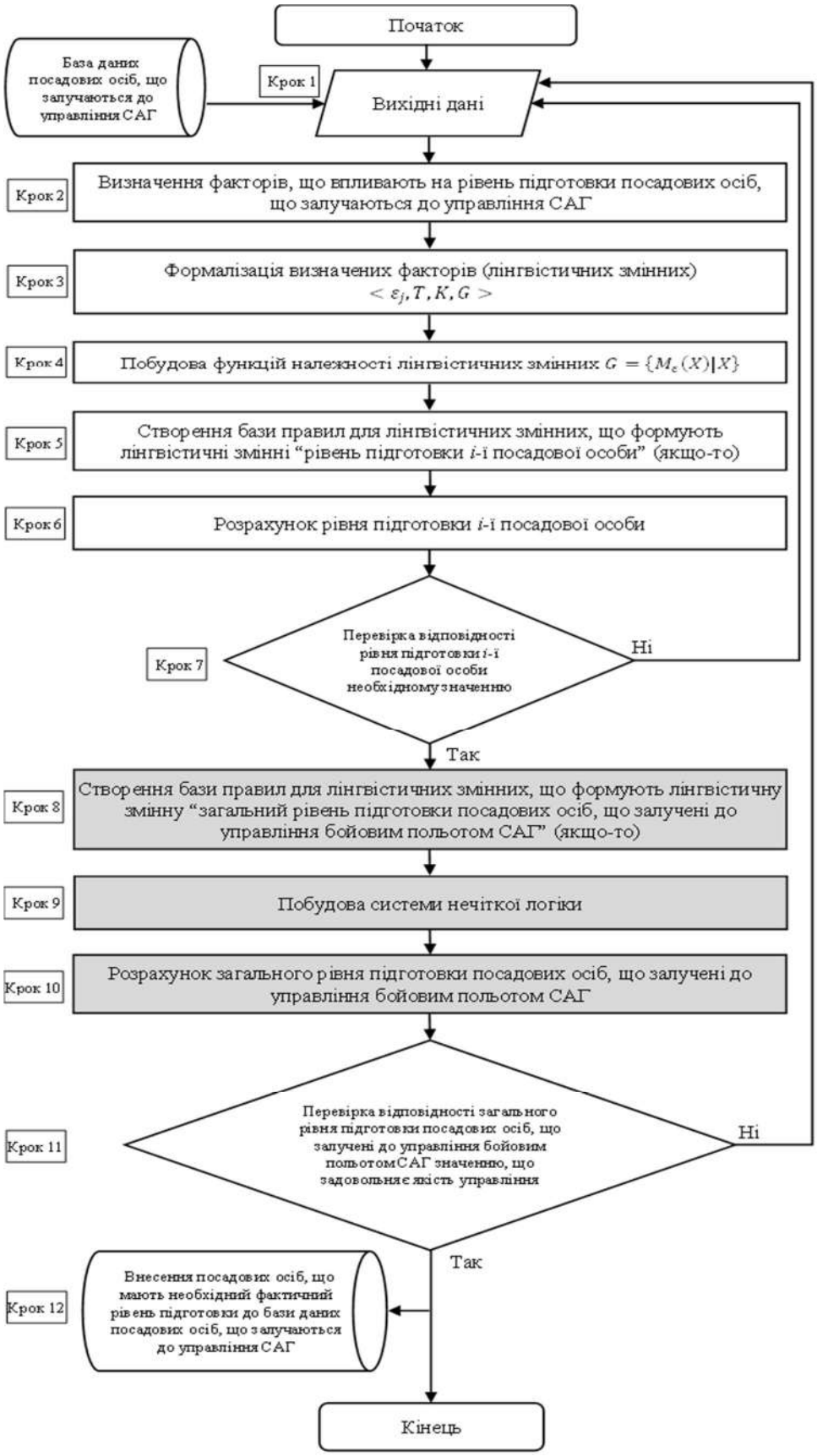


Рисунок 1 – Блок-схема удосконаленої часткової методики оцінювання рівня підготовки посадових осіб, що залучаються до управління бойовим польотом спільної авіаційної групи пілотованої та безпілотної авіації

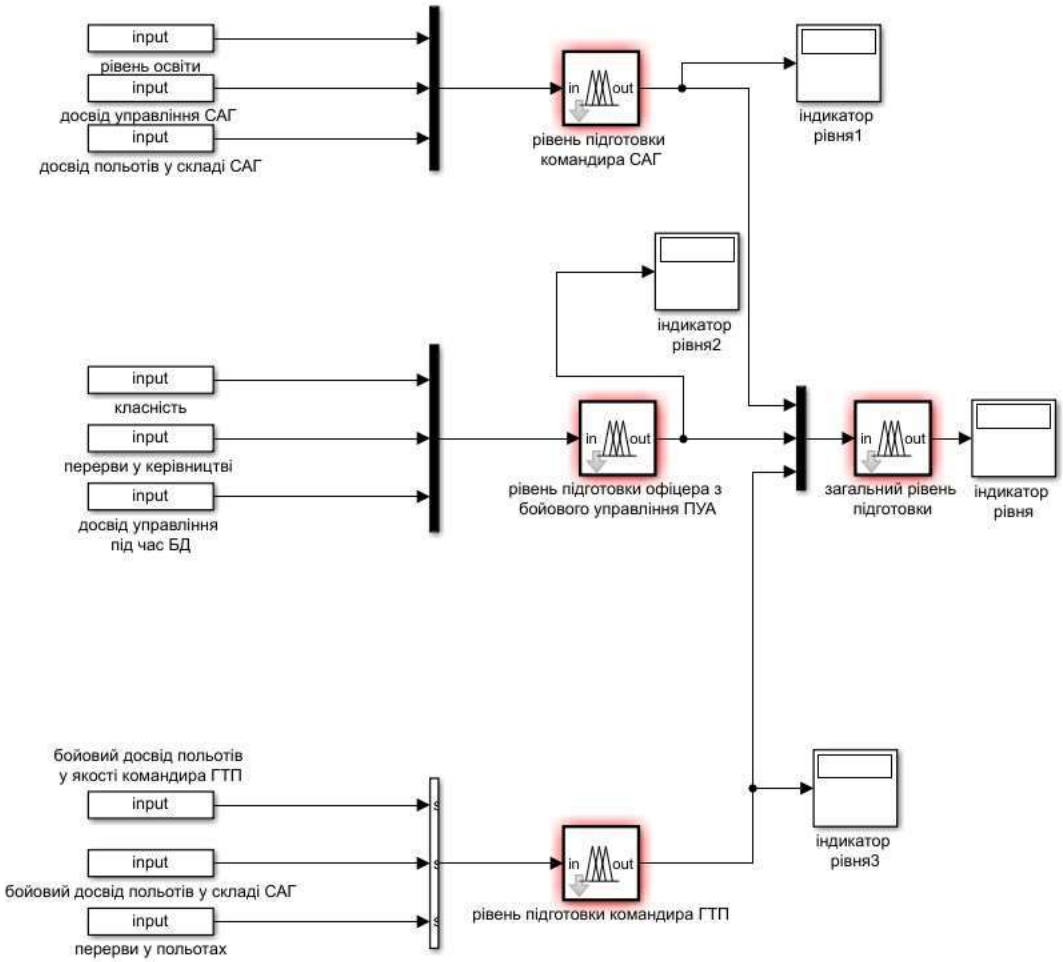


Рисунок 2 – Система нечіткої логіки для визначення рівня підготовки посадових осіб, що залучаються до управління бойовим польотом САГ

Крок 12: Дані про посадових осіб, що мають необхідний рівень підготовки заносяться до бази даних посадових осіб, що залучаються до управління САГ, яка повинна після кожного бойового польоту САГ уточнятися.

Математичний апарат нечіткої логіки дозволяє створювати системи підтримки прийняття рішень, які допомагають зменшити ризики прийняття неефективних рішень та негативні наслідки, які ці рішення за собою тягнуть [15].

Висновки і перспективи подальших досліджень

У статті проведено аналіз існуючих методик оцінювання рівня підготовки особового складу, визначено їх переваги та недоліки. Основними *недоліками* в яких є:

оцінювання індивідуального рівня підготовки особового складу за однаковими (типовими) показниками; не врахування бойового та управлінського досвіду посадових осіб;

неможливість оцінити загальний рівень підготовки різнорідних посадових осіб, як команди, яка виконує спільне завдання.

Запропоновано удосконалену часткову методику оцінювання рівня підготовки посадових осіб, що залучаються до управління бойовим польотом спільної авіаційної групи пілотованої та безпілотної авіації, яка, на відміну від існуючих, за допомогою математичного апарату нечіткої логіки дає змогу оцінювати окремо фактичний рівень підготовки різнорідних посадових осіб, таких як: командир спільної авіаційної групи пілотованої та безпілотної авіації; офіцер з бойового управління пункту управління авіації; командир групи тактичного призначення, а також оцінювати їх загальний фактичний рівень підготовки, як команди.

Перевагою запропонованої удосконаленої часткової методики є те, що рівень підготовки кожної посадової особи, яка виконує різнорідні функції під час управління бойовим польотом спільної авіаційної групи, оцінюється за різними показниками, які відображають їх фактичну готовність до виконання завдань, в тому числі враховується їх особистий досвід (бойових дій, управління, польотів та інше). Це дасть змогу прогнозувати ефективність бойового застосування спільної авіаційної групи, інших авіаційних угруповань та підрозділів авіації під час планування військових операцій.

Запропонована методика може стати складовою системи підтримки прийняття рішень для органів

військового управління, що дасть змогу обирати для управління бойовим польотом підготовлений особовий склад з необхідним фактичним рівнем підготовки.

В подальшому доцільно провести дослідження щодо визначення рівня підготовки посадових осіб авіаційного угруповання (спільної авіаційної групи) до бойового застосування в операціях сил оборони, де буде врахований рівень підготовки посадових осіб, які забезпечують підготовку та планування бойових польотів авіаційного угруповання, підготовку повітряних суден, авіаційних засобів ураження, аеродрому, засобів зв'язку та радіотехнічного забезпечення польотів та логістики до виконання бойових завдань.

Список бібліографічних посилань

1. Жирохов М. О. Війна в повітрі. Україна, лютий-травень 2022. Чернігів : Княжий вал, 2022. 94 с. **2. Allied Joint** Doctrine For The Conduct Of Operations. AJP-3 (B). Washington: NATO Standartization Office, 2019. 164 p. URL: https://assets.publishing.service.gov.uk/government/publications/allied-joint-doctrine-for-the-conduct-of-operations-ajp-3b (Accessed : 16.06.2023). **3. Візія** Повітряних Сил 2035. Київ : Міністерство оборони України ; Командування ПС ЗСУ, 2020. 39 с. **4. Ярошенко Я. В., Герасименко В. В., Коротін С. М., Мартинюк О. Р., Блискун О. Є.** Алгоритм процесу управління спільною авіаційною групою за етапами бойового польоту. *Повітряна міць України,* 2022. № 2. С. 29-34. URL: https://doi.org/10.33099/2786-7714-2022-1-2(3)-29-34 (дата звернення : 16.06.2023). **5. Правила** виконання польотів в державній авіації України : наказ Міністерства оборони України від 05.01.2015 р. № 2. Офіц. вид. 2015. 107 с. **6. Правила** виконання польотів безпілотними авіаційними комплексами державної авіації України : наказ Міністерства оборони України від 08.12.2016 р. № 661. Офіц. вид. 2016. 32 с. **7. Blyskun O., Herasymenko V., Kolomiiets Y., Honcharenko Y., Yaroshenko Y.** Alghorthm of determining the readiness level of the flight crew based on fuzzy logic approaches. *Sciences of Europe*. 2021. Vol. 2. №80. P. 46-49. **8. Гончаренко Є. В. Блискун О. Є., Ткаченко А. В., Ковба О. П., Титаренко О. І.** Застосування підходів теорії нечіткої логіки для оцінювання підготовленості авіаційного персоналу *Повітряна міць України.* 2021. №1. С. 8–11. URL: https://doi.org/10.33099/2786-7714-2021-1-1-8-11 (дата звернення : 16.06.2023). **9. Дроздов С. С.** Методичний підхід до кількісного оцінювання впливу рівня підготовленості екіпажів на бойову могутність бойового складу тактичної авіації. *Наука і техніка Повітряних Сил Збройних Сил України.* 2016. № 3. С. 49-53. URL: http://nbuv.gov.ua/UJRN/Nitps_2016_3_10 (дата звернення : 16.06.2023). **10. Макаліш О. В., Георгадзе О. А.** Методичний підхід до оцінювання рівня навченості органів військового управління тактичного рівня. *Збірник наукових праць Центру воєнно-наукових досліджень Національного університету оборони України імені Івана Черняховського.* 2016. № 3. С. 104–108. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2016_3_20 (дата звернення : 16.06.2023). **11. Овчаренко В. В.** Методика оцінювання існуючого рівня підготовленості військовослужбовців підрозділу спеціального призначення внутрішніх військ до виконання бойових завдань по знешкодженню озброєних злочинців. *Честь і закон*. 2011. № 2. С. 51–59. URL: https://doi.org/10.33405/2078-7840/2011/0/2/143960 (дата звернення : 16.06.2023). **12. Лендюк Т. В., Васильків Н. М.** Нечітка модель формування індивідуальної траєкторії навчання та побудова онтології на її основі. *Інформатика та математичні методи в моделюванні.* 2017. Т. 7. № 1-2. С. 103–112. URL: http://nbuv.gov.ua/UJRN/Itmm_2017_7_1-2_14 (дата звернення : 16.06.2023). **13 Goncharenko Y., Blyskun O., Martyniuk O., Radko O., Kolomiiets Y., Bilokur M.** Flight safety fuzzy risk assessment for combat aviation system. *IEEE 2nd International Conference on Advanced Trent in Information Theory*, 2020. P. 132-137. **14. Martin McNeill F., Thro E.** Fuzzy logic: a practical approach. Boston, USA: AP PROFESSIONAL, 1994. P. 309. **15. Кравець П., Киркало Р.** Системи прийняття рішень з нечіткою логікою. *Вісник Національного університету «Львівська політехніка* . 2009. № 650: Комп'ютерні науки та інформаційні технології. С. 115–123. URL: https://ena.lpnu.ua/handle/ntb/2806 (дата звернення : 16.06.2023).

AN IMPROVED PARTIAL METHODOLOGY FOR ASSESSING THE OFFICIAL'S READINESS LEVEL INVOLVED IN THE MANNED AND UNMANNED JOINT AVIATION GROUP COMBAT FLIGHT COMMAND AND CONTROL

Yaroshenko Yaroslav

The National Defence University of Ukraine, Kyiv, Ukraine

During a combat flight, the manned and unmanned aircraft aviation group command and control is carried out by the group commander and combat command and control officers from ground (air) aviation control points, as well as in the air by commanders (seniors) of tactical assignment groups. Each official who is involved in the aviation grouping command and control must have the corresponding actual readiness level, which effects on these official's general readiness level as a team that manages during the entire combat flight. Evaluating the official's readiness level who have different using orientations the existing methods of evaluating the personal readiness level does not allow determining the actual readiness level and may lead to disruption of the aviation groups combat mission. Therefore, there is a scientific task to improve the existing scientific and methodical apparatus for assessing the official's readiness level, which allow to evaluate the overall actual various official's readiness level involved in aviation group combat flight command and control. This will allow, during the planning of a combat flight, to determine the predicted aviation group combat mission effectiveness and to involve officials with a high training level in its management. The research was conducted using a system approach and the fuzzy

logic theory. The article analyzed the existing methods the personnel readiness level assessing and proposed an improved partial method of the official's level readiness assessing involved in manned and unmanned aviation joint air group combat flight command and control. The improved partial methodology, which using the fuzzy logic mathematical apparatus allows, unlike the existing ones, to determine the individual actual official's readiness level who have different assignments and to evaluate the overall actual official's readiness level involved in the aviation group combat flight command and control. During the research, the Matlab application program package Simulink and Fuzzy Logic Designer were used for simulation modeling of determining the level of training of officials. The proposed improved partial methodology has important practical significance for military aviation units, as it can become an effective tool during the official's selection who will aviation group combat flight command and control, units, and military aviation units, as well as a component of the military administration bodies decision-making support system for planning operations.

Keywords: *readiness level, fighter aircraft, attack aircraft, unmanned aerial vehicle, assessment methodology, joint manned and unmanned aviation group, combat flight, combat command and control officer, fuzzy logic, combat application, management, control system.*

References

1. Zhyrohov, M.O., (2022). Airwar in Ukraine, February-May 2022. Chernihiv: Kniazhyi val, 94. **2. NATO** Standartization Office, (2019). Allied Joint Doctrine for The Conduct Of Operations. AJP-3 (B). [online]. Available at: https://assets.publishing.service.gov.uk/government/publications/allied-joint-doctrine-for-the-conduct-of-operations-ajp-3b [Accessed : 16 June 2023]. **3. Air** Force Vision 2035, (2020). 39. [online]. Available at: https://mil.in.ua/uk/articles/viziya-povitryanyh-syl-zsu-zamina-radyanskogo-ta-unifikatsiya/ [Accessed : 16 June 2023]. **4. Yaroshenko, Y. V., Herasymenko, V. V., Korotin, S. M., Martyniuk, O. R., and Blyskun, O. Ye.,** (2022). The Joint Aviation Group Management Process Algorithm by Stages of Combat Flight. *Ukrainian Air Power,* 2, 29-34. [online]. Available at: https://doi.org/10.33099/2786-7714-2022-1-2(3)-29-34 [Accessed : 16 June 2023]. **5. Ukrainian** State Aviation Flight Rules, (2015). Nakaz Ministerstva oborony Ukrainy vid 05.01.2015 r. № 2. Ofits. vyd.. 107. **6. Ukrainian** State Aviation Unmanned Aircraft Systems Flight Rules, (2016). Nakaz Ministerstva oborony Ukrainy vid 08.12.2016 r. № 661. Ofits. vyd. 32. **7. Blyskun, O., Herasymenko, V., Kolomiiets, Y., Honcharenko, Y. and Yaroshenko, Y.,** (2021). Alghorythm of determining the readiness level of the flight crew based on fuzzy logic approaches. *Sciences of Europe,* 2, 80, 46-49. **8. Honcharenko, Ye.,V. Blyskun, O. Ye., Tkachenko, A. V., Kovba, O. P. and Tytarenko, O. I.,** (2021). The Fuzzy Logic Theory Approaches Application For Aviation Personnel Training Assessment *Ukrainian Air Power*, 1, 8-11. DOI: ttps://doi.org/10.33099/2786-7714-2021-1-1-8-11.

9. Drozdov, S. S., (2016). Methodological Approach to Influence Level Scoring of Readiness of Crew to Field Personnel Combat Might in Tactical Aviation. *Science and Technology of the Air Force of Ukraine,* 3, 49-53 [online]. Available at: http://nbuv.gov.ua/UJRN/Nitps_2016_3_10 [Accessed : 16 June 2023]. **10. Makalish, O. V. and Heorhadze, O. A.,** (2016). Methodical Going Near the Evaluation of Level of Preparation of Organs of Military Management of Tactical Level. *Collection of Scientific Papers of the Center for Military and Strategic Research of the National Defense University of Ukraine,* 3, 104-108 [online]. Available at: http://nbuv.gov.ua/UJRN/Znpcvsd_2016_3_20 [Accessed : 16 June 2023]. **11. Ovcharenko, V. V.,** (2011). Methods of Estimating the Current Level of Proficiency of the Interior Troops Special-Purpose Units Personnel to Carry Out the Combat Mission in Neutralizing the Armed Criminals *Honor and Law*, 2, 51-59. DOI: https://doi.org/10.33405/2078-7840/2011/0/2/143960. **12. Lendiuk, T. V. and Vasylkiv, N. M.,** (2017). Fuzzy Model of Individual Learning Path Forming and Ontology Design on its Basis. *Informatics and Mathematical Methods in Simulation,* 7, 1-2, 103-112, 108 [online]. Available at: http://nbuv.gov.ua/UJRN/Itmm_2017_7_1-2_14 [Accessed : 16 June 2023]. **13 Goncharenko, Y., Blyskun, O., Martyniuk, O., Radko, O., Kolomiiets, Y. and Bilokur, M.,** (2020). Flight safety fuzzy risk assessment for combat aviation system. *IEEE 2nd International Conference on Advanced Trent in Information Theory*, pp. 132-137. **14. McNeill F. Martin,** (1994). Fuzzy logic: a practical approach / F. Martin McNeill, Ellen Thro. Boston: AP PROFESSIONAL. 309. **15. Kravets, P. and Kyrkalo, R.,** (2009). Decision-Making Systems with Fuzzy Logic. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika». № 650: Kompiuterni nauky ta informatsiini tekhnolohii.* pp. 115-123 [online]. Available at:: https://ena.lpnu.ua/handle/ntb/2806 [Accessed : 16 June 2023].

DOI:**10.33099/2311-7249/2023-47-2-55-66**

УДК: 358.1

Репіло Юрій Євгенович *(доктор військових наук, професор)*
Головченко Олег Володимирович *(доктор філософії)*
Ріман Олексій Олександрович *(кандидат військових наук, доцент)*

Національний університет оборони України, Київ, Україна

МЕТОДИКА ВИЗНАЧЕННЯ ПРІОРИТЕТНОСТІ РАКЕТНИХ ТА АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ ДЛЯ ЇХ ОСНАЩЕННЯ БЕЗПІЛОТНИМИ СИСТЕМАМИ

Результати аналізу здобутих уроків застосування військ (сил) у ході ведення воєнних дій впродовж останніх років показують, що успіх ведення операцій (дій) значною мірою залежатиме від результативної вогневої підтримки. У свою чергу, досягнення її потрібної результативності неможливо без своєчасних та достовірних розвідувальних даних про об'єкти (цілі) противника із застосуванням безпілотних систем. Водночас, у теорії і практиці управління ракетними та артилерійськими підрозділами виникла неприпустима невідповідність між потребою оснащення ракетних та артилерійських підрозділів безпілотними системами й обмеженим складом таких систем за ознакою їх пріоритетності. Отже, з одного боку, існує потреба максимізувати оснащення ракетних та артилерійських підрозділів залежно від специфіки завдань вогневої підтримки, а з іншого – обмежена кількість наявних безпілотних систем, які можуть забезпечити ракетні та артилерійські підрозділи актуальними розвідувальними даними про об'єкти (цілі) противника для виконання завдань вогневої підтримки в операціях (діях). Виходячи з цього, мета статті полягає в розробленні методики визначення пріоритетності ракетних та артилерійських підрозділів для оснащення безпілотними системами. У статті набула подальшого розвитку методика розв'язування задачі багатокритеріального вибору оптимального рішення з-поміж альтернатив за ознакою пріоритетності методом експертного опитування. За таких умов, для визначення пріоритетності багатовимірної системи під час розв'язування задачі багатокритеріального вибору запропоновано застосовувати дві групи показників: важливості й пріоритетності застосування ракетних і артилерійських підрозділів. Експертне опитування узгоджують за допомогою коефіцієнта конкордації Кендала. Бальні оцінки показників, отриманих експертами, приводять до єдиної безрозмірної шкали переваг, для чого використовують узагальнену функцію переваг Харрінгтона. Запропоновану методику пропонується застосовувати в органах військового управління під час визначення пріоритетності ракетних та артилерійських підрозділів для їх оснащення безпілотними системами.

Ключові слова: *управління, пріоритетність, важливість, вогнева підтримка, ракетні та артилерійські підрозділи, безпілотні системи, експертне опитування, коефіцієнт конкордації Кендала, функція переваг Харрінгтона.*

Вступ

Результати аналізу здобутих уроків застосування військ (сил) під час ведення воєнних дій впродовж останніх років свідчать, що в сучасних умовах та на перспективу до 2030 року, успіх ведення бойових операцій (дій) залежатиме від результативної вогневої підтримки (далі – ВгП) [1; 2]. ВгП являє собою скоординоване й інтегроване застосування вогневих засобів для ведення непрямого вогню з метою досягнення необхідних ефектів по наземних (надводних) цілях для підтримки дій військ (сил) [3; 4]. Зміст доктринальних положень та наукові результати досліджень, проведених у країнах – членах Організації Північноатлантичного договору, практика ведення воєнних дій під час відсічі широкомасштабної збройної агресії російської федерації проти України свідчать про те, що ракетні та артилерійські підрозділи (далі – РАП) залишаються основними військовими формуваннями, здатними забезпечити результативну ВгП в операціях (діях) [5–18].

Водночас, досягнення потрібної результативності ВгП неможливе без своєчасних і достовірних розвідувальних даних про об'єкти (цілі) противника із застосуванням безпілотних систем (далі – БС). За таких умов, в ході нинішніх бойових операцій (дій) виявлено, що саме БС дають змогу забезпечити РАП актуальними розвідувальними даними про об'єкти (цілі) противника під час виконання завдань ВгП [19–21]. Отже, в сучасних умовах існує актуальна потреба в забезпеченні РАП безпілотними системами, що сприятимуть результативній ВгП завдяки наданню актуальних даних про об'єкти (цілі) противника.

Відповіддю на цей виклик стало збільшення обсягів постачання БС різних видів і модифікацій. Проте існують певні обмеження за їхньою кількістю. Тому для оснащення РАП безпілотними системами потрібно їх раціонально розподілити, тобто визначити пріоритетність РАП.

Постановка проблеми. Таким чином у практиці військового управління для досягнення результативності ВгП в операціях (діях) виникла неприпустима невідповідність між потребою в оснащенні РАП безпілотними системами та обмеженістю складу таких систем за ознакою їх пріоритетності. Отже, з одного боку, існує потреба в максимізації оснащення РАП залежно від специфіки завдань ВгП, а з іншого – обмежена кількість наявних БС, які можуть забезпечити РАП актуальними розвідувальними даними про об'єкти (цілі) противника для виконання завдань ВгП в операціях (діях). Однак усунення такої невідповідності можливе лише за результатами дослідження з використанням відповідного науково-методичного апарату з оцінювання системи показників та визначення критерію пріоритетності РАП для їх оснащення безпілотними системами.

Аналіз останніх досліджень і публікацій. Визначення пріоритетності РАП для їх оснащення безпілотними системами є задачею багатокритеріального вибору оптимального рішення з-поміж кількох альтернатив. Щоб розв'язати цю задачу, необхідно створити систему показників і критеріїв для визначення пріоритетності РАП з метою їх оснащення безпілотними системами, встановити порядок оцінювання окремих показників та інтегрального показника пріоритетності.

Враховуючи значну кількість РАП у Збройних силах України (далі – ЗС України), якісну зміну їхнього озброєння та різноплановість завдань ВгП, для визначення пріоритетності таких підрозділів з метою оснащення БС, досвідчені військові командири додатково потребують відповідного математичного обґрунтування.

Питанням розв'язування задач багатокритеріального вибору оптимального рішення з-поміж кількох альтернатив та системи показників і критеріїв їх оцінювання під час визначення пріоритетності присвячено низку досліджень [22–29]. У цих роботах, для розв'язування багатокритеріальної задачі та розрахунку інтегрального показника пріоритетності багатовимірної системи, широко застосовувався метод експертного опитування. Водночас, у практиці військового управління, за різними напрямами службової діяльності, визначення експертних оцінок за окремими показниками та розрахунок інтегрального показника пріоритетності на основі поєднання експертних оцінок за окремими показниками у вигляді середньоарифметичного або середньозваженого значень забезпечує прийняття обґрунтованих рішень. Зокрема, в розробленій методиці визначення пріоритетності багатовимірної системи [23] запропоновано підхід до визначення пріоритетності науково-дослідних та дослідно-конструкторських робіт, пов'язаних зі створенням (модернізацією) зразків озброєння та військової техніки. Для цього використовується експертне опитування. Так, підсумкові оцінки пріоритетності [23] пропонується визначати з використанням узагальненої функції переваг Харрінгтона та відповідної вербально-числової шкали. Однак для оцінювання пріоритетності РАП для їх оснащення безпілотними системами система показників, запропонована в зазначеній праці, потребує певних перетворень.

Отже, наявний науково-методичний апарат оцінювання пріоритетності системи показників і критерію під час розв'язування задач багатокритеріального вибору оптимального рішення з-поміж кількох альтернатив не може бути використаний в інтересах визначення пріоритетності РАП для їх оснащення безпілотними системами, але може стати базовим для подальшого розвитку.

Мета статті полягає в розробленні методики визначення пріоритетності ракетних та артилерійських підрозділів для їх оснащення безпілотними системами.

Виклад основного матеріалу дослідження.

Відомо, що властивості будь-якого об'єкта повною мірою можуть проявлятися лише у процесі його застосування за призначенням. Однак результати досліджень [22–26] показують, що визначити лише за одним показником пріоритетність багатовимірної системи, до якої відносяться РАП, під час розв'язування задач багатокритеріального вимірювання, практично неможливо. Саме тому запропоновано для оцінювання пріоритетності РАП для їх оснащення безпілотними системами використовувати таку систему показників: основний (інтегральний); узагальнені (найбільш репрезентативні), що характеризують кінцевий результат функціонування РАП; кілька додаткових, що характеризують важливість оснащення безпілотними системами. Отже, для визначення пріоритетності РАП, для їх оснащення безпілотними системами, запропоновано використовувати дві групи показників: важливості і пріоритетності застосування РАП. Такий підхід даватиме змогу проводити експертне опитування у два етапи та виключати з розгляду на другому етапі РАП, які не мають особливого значення. Для визначення важливості РАП запропоновано застосовувати показники, наведені в табл. 1.

Для визначення значень показників $A_1 \ldots A_4$ (див. табл. 1) запропоновано обрати критерії, що відповідають бальним оцінкам від 1 до 9. Результати аналізу теорії та практики ведення воєнних дій за ознакою змісту застосування РАП показують, що головним їхнім змістом є цілеспрямована участь у ВгП під час операцій (дій). Така участь РАП буде реалізована через їхні бойові можливості, максимальне досягнення яких буде спрямовано на виконання завдань ВгП в операціях (діях). На цій підставі можна зробити висновок, що група показників пріоритетності буде пов'язана з виконанням РАП завдань з ВгП в операціях (діях), табл. 2.

Таблиця 1

Показники та критерії важливості ракетних та артилерійських підрозділів для їх оснащення безпілотними системами

Найменування показника	Критерії важливості	Бальна оцінка
A_1 – ступінь впливу функціонування РАП на результативність виконання оперативних (тактичних) завдань в операціях (діях)	Надзвичайно високий	9
	Високий	7
	Середній	5
	Низький	3
	Відсутність впливу	1
A_2 – ступінь відповідності вогневих можливостей РАП встановленим вимогам під час їх застосування в операціях (діях)	Повний	9
	Майже повний	7
	Високий	5
	Середній	3
	Низький	1
A_3 – ступінь відповідності маневрених можливостей РАП встановленим вимогам під час їх застосування в операціях (діях)	Повний	9
	Майже повний	7
	Високий	5
	Середній	3
	Низький	1
A_4 – ступінь відповідності спроможностей РАП встановленим вимогам щодо виконання основних завдань за призначенням	Повний	9
	Майже повний	7
	Високий	5
	Середній	3
	Низький	1
Для всіх показників	Проміжна бальна оцінка між сусідніми значеннями	2, 4, 6, 8

Джерело: розроблено авторами за даними [30, 11–16].

Таблиця 2

Показники та критерії пріоритетності застосування ракетних та артилерійських підрозділів для їх оснащення безпілотними системами

Найменування показника	Критерії пріоритетності	Бальна оцінка
B_1 – ступінь участі РАП у дезорганізації системи управління військами і зброєю, розвідки та радіоелектронної боротьби противника	Надзвичайно високий	9
	Високий	7
	Середній	5
	Низький	3
	Відсутність участі	1
B_2 – ступінь участі РАП у протидії засобам ураження повітряного базування та протиповітряної оборони противника	Надзвичайно високий	9
	Високий	7
	Середній	5
	Низький рівень	3
	Відсутність участі	1
B_3 – ступінь участі РАП у вогневій протидії засобам вогневої підтримки противника	Надзвичайно високий	9
	Високий	7
	Середній	5
	Низький	3
	Відсутність участі	1
B_4 – ступінь участі РАП у зниженні спроможностей частин (підрозділів) угруповання військ (сил) противника	Надзвичайно високий	9
	Високий	7
	Середній	5
	Низький	3
	Відсутність участі	1
B_5 – ступінь участі РАП у порушенні логістичного забезпечення	Надзвичайно високий	9
	Високий	7
	Середній	5
	Низький	3
	Відсутність участі	1
Для всіх показників	Проміжна бальна оцінка між сусідніми значеннями	2, 4, 6, 8

Джерело: розроблено авторами за даними [30, 11–16].

Для визначення значень показників $B_1 ... B_5$ (див. табл. 2) запропоновано обрати критерії, що відповідають бальним оцінкам від 1 до 9.

Важливість РАП за визначення пріоритетності їх оснащення БС пропонується визначати згідно з алгоритмом (рис. 1) за такими етапами.

Етап 1 – введення вхідних даних. Тут і далі позначено: n – поточний номер РАП ($n = \overline{1, N}$, де N – кількість оцінюваних РАП) і – поточний номер показника важливості РАП ($i = \overline{1, I}$, де I – кількість показників важливості ($I = 4$), m – умовний номер експерта ($m = \overline{1, M}$, де M – кількість експертів у групі).

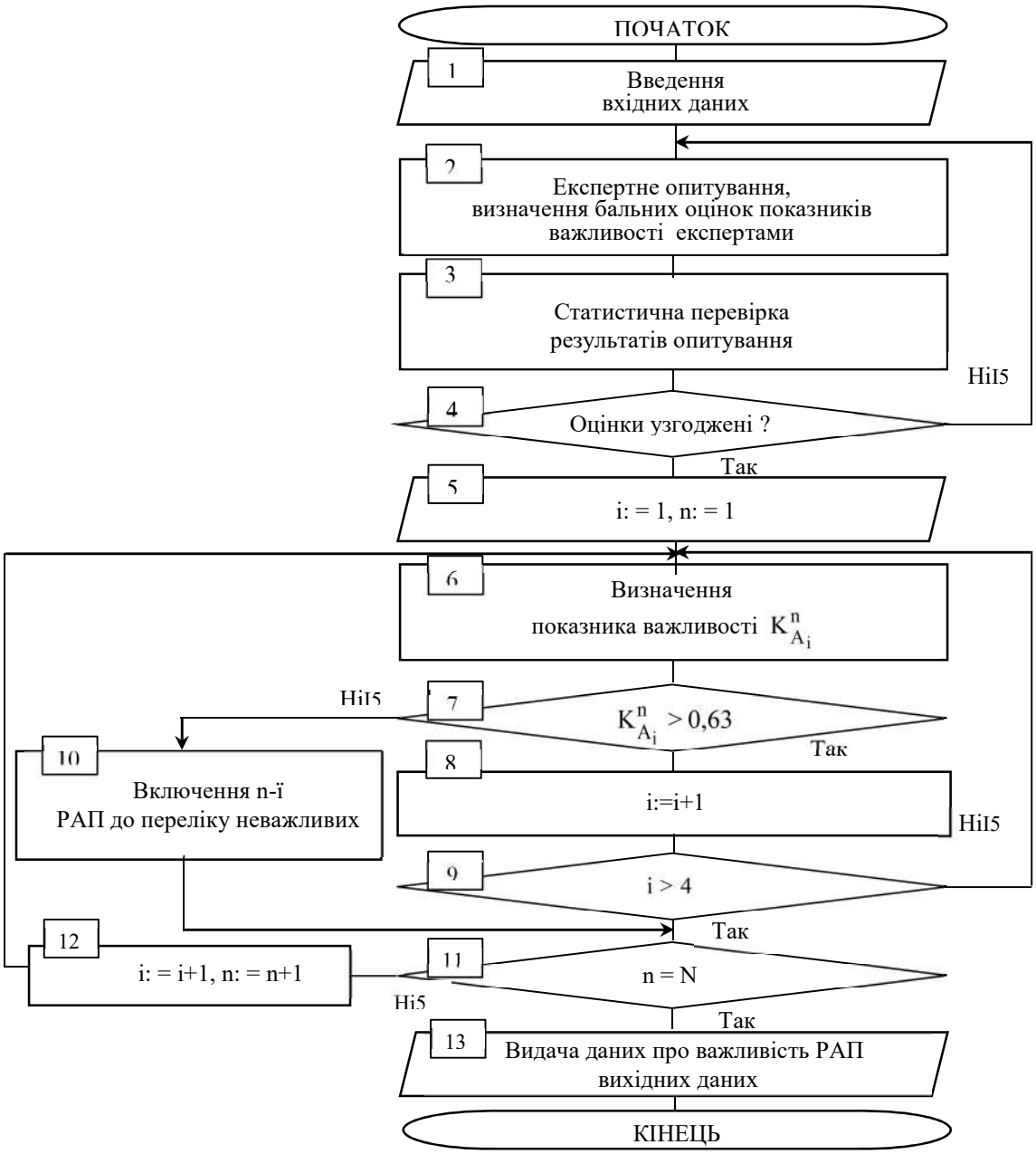


Рисунок 1 – Блок-схема алгоритму визначення важливості ракетних та артилерійських підрозділів для їх оснащення безпілотними системами

Етап 2 – проведення експертного опитування. Кожен m -й експерт для кожної n -ї РАП визначає бальні оцінки $k^n_{A_i}$ для кожного i -го показника важливості РАП при визначені пріоритетності для їх оснащення БС.

Етап 3 – статистична перевірка результатів опитування експертів. У ході етапу пропонується виявляти узгодженість в оцінках. Гіпотезу про наявність узгодженості в оцінках експертів під час визначення бальної оцінки показника для розглянутих РАП перевіряють за допомогою коефіцієнта конкордації Кендала W , який обчислюють за такою залежністю [23]:

$$W = \frac{D}{D_{max}}, \qquad (1)$$

де D – дисперсія рангів оцінок експертів;

D_{max} – максимальна дисперсія рангів оцінок експертів.

Коефіцієнт конкордації може мати значення від 0 (відсутність будь-якої згоди в оцінках експертів) до 1 (повна згода). Дисперсію рангів в оцінках експертів D пропонується обчислювати так:

$$D = \sum_{n=1}^{N} (\Delta_n)^2 . \qquad (2)$$

В аналітичній залежності (2) введено позначення Δ_n , яке пропонується визначати за таким співвідношенням:

$$\Delta_n = \sum_{m=1}^{M} r_{nm} - \frac{1}{N} \sum_{n=1}^{N} \sum_{m=1}^{M} r_{nm} , \qquad (3)$$

де r_{nm} – ранг n -ї РАП, визначений з бальної

оцінки відповідного показника, виставленої m -м експертом;

N – кількість оцінюваних РАП.

Ранги РАП за визначеним показником отримують із відповідних бальних оцінок. При цьому бальним оцінкам показника, виставленим експертом для різних РАП, присвоюються ранги $1,2,3,...,N$ таким чином, щоб менше значення рангу відповідало вищій оцінці експерта. Наприклад, якщо бальні оцінки показника для чотирьох РАП, виставлені експертом, мають вигляд 7, 3, 5, 9, то відповідна послідовність рангів набуває вигляду 2, 4, 3, 1.

Якщо бальні оцінки експерта повторюються, необхідно відповідним РАП приписати стандартизовані ранги – частки від ділення суми місць, зайнятих цілими з однаковими рангами, на загальну кількість таких альтернатив. Наприклад, якщо бальні оцінки показника для чотирьох РАП, виставлені експертом, мають вигляд 9, 5, 7, 9, то відповідна послідовність рангів набуває вигляду 1,5; 4; 3; 1,5.

Максимальну дисперсію оцінок експертів обчислюють за таким співвідношенням:

$$D_{max} = \frac{1}{12} M^2 (N^3 - N) - \frac{1}{12} M \cdot \sum_{m=1}^{M} T_m , \quad (4)$$

де M – кількість експертів у групі;

N – кількість РАП, що підлягають оцінюванню.

В аналітичній залежності (4) введено позначення T_m , яке пропонується обчислювати за таким співвідношенням:

$$T_m = \sum_{k_m} (t_m^3 - t_m), \quad (5)$$

де t_m – кількість повторень кожного рангу в оцінках m -го експерта;

k_m – кількість повторюваних рангів в оцінках m -го експерта.

Етап 4 – перевірка виконання умов узгодженості оцінок експертів за коефіцієнтом конкордації Кендала, який пропонується визначати за виразом (1). Високого рівня узгодженості оцінок експертів досягають за $W \geq 0,7$. За $0,5 < W$ результати експертизи слід визнати незадовільними, а етапи 2 і 3 експертизи повторити.

Етап 5 – встановлення поточних номерів РАП $n := 1$ і показника важливості $i := 1$.

Етап 6 – опрацювання результатів експертного опитування, а саме визначення показника важливості $K_{A_i}^n$, розрахунок усереднених значень бальних оцінок i -го показника важливості РАП за співвідношенням [23]:

$$k_{A_i}^n = \frac{1}{M} \sum_{m=1}^{M} k_{A_{im}}^n , \quad (6)$$

де $k_{A_{im}}^n$ – бальні оцінки i -го показника важливості n -ї РАП, отримані m -м експертом;

M – кількість експертів у групі.

З використанням узагальненої функції переваг Харрінгтона пропонується обчислювати значення i -го показника важливості РАП за таким співвідношенням:

$$K_{A_i}^n = exp(-exp(-y_{A_i}^n)) . \quad (7)$$

В аналітичній залежності (7) введено допоміжну величину $y_{A_i}^n$, яку пропонується визначати так:

$$y_{A_i}^n = -2 + \frac{7}{8}(k_{A_i}^n - 1) . \quad (8)$$

Розрахунки, що проводять на етапі 6, є перетворенням визначених експертами бальних оцінок показника важливості в узагальнену функцію переваг Харрінгтона для відповідних показників.

Таке перетворення проводять, по-перше, щоб компенсувати помилки у визначенні бальних оцінок показників експертами, спричиненні впливом закону Вебера – Фехнера, згідно з яким психологічна оцінка будь-якого показника експертом нелінійно залежить від його величини; по-друге для приведення бальних оцінок експертів до єдиної безрозмірної шкали переваг Харрінгтона.

Етап 7 – порівняння отриманого значення з граничним значенням показників (0,63). Якщо значення i -го показника важливості більше, ніж граничне, переходять до етапу 8, в іншому разі – до етапу 10.

Етап 8 – збільшення поточного номера показника важливості, який розглядають, на одиницю $i := i + 1$.

Етап 9 – перевірка виконання умови розгляду всіх показників важливості. Якщо умови виконано, переходять до етапу 11, в іншому разі – повертаються до етапу 6.

Етап 10 – включення n -ої РАП до переліку неважливих для оснащення БС.

Етап 11 – перевірка виконання умови розгляду всіх РАП. Якщо умови виконано, переходять до етапу 12; в іншому разі – до етапу 13.

Етап 12 – збільшення поточного номера РАП на одиницю $n := n + 1$, встановлення поточного номера показника важливості $i := 1$, і повернення до етапу 6.

Етап 13 – за результатами визначення важливості формування переліку важливих РАП у кількості S .

Визначений перелік РАП у кількості S військових формувань надалі розглядає експертна група, щоб визначити підсумкові оцінки і визначити пріоритетність їх застосування та оснащення безпілотними системами. Алгоритм розгляду складається з 12 етапів (рис. 2).

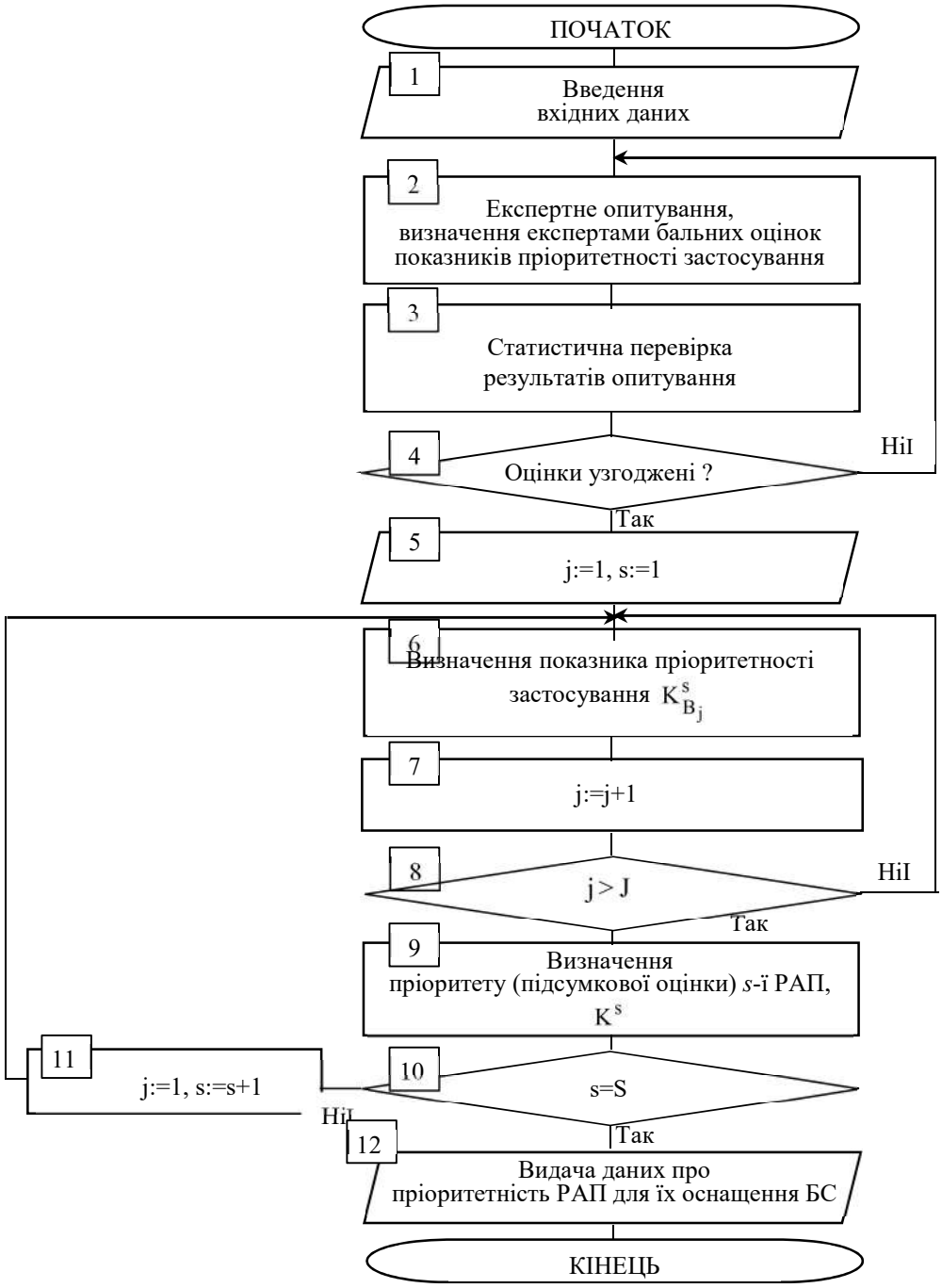


Рисунок 2 – Блок-схема алгоритму визначення пріоритетності ракетних та артилерійських підрозділів для їх оснащення безпілотними системами

Етап 1 – визначення вхідних даних. Тут і далі позначено: s – поточний номер важливої РАП ($s = \overline{1,S}$, де S – кількість важливих РАП), j – порядковий номер показника пріоритетності застосування РАП ($j = \overline{1,J}$, де J – кількість показників пріоритетності ($J = 5$)).

Етап 2 – проведення експертного опитування. У ході опитування пропонується, що кожен m -й експерт для кожної s -ї РАП визначає бальні оцінки $k^s_{B_{jm}}$ для кожного j -го показника пріоритетності застосування РАП.

Етап 3 – статистична перевірка результатів опитування експертів. У ході етапу пропонується виявляти узгодженість в оцінках. Гіпотезу про наявність узгодженості в оцінках експертів під час визначення бальної оцінки показника для розглянутих РАП перевіряють за допомогою коефіцієнта конкордації Кендала W , обчисленого за виразами (1) – (5).

Етап 4 – перевірка виконання умов узгодженості оцінок експертів за коефіцієнтом конкордації Кендала, визначеним за виразом (1). Високого рівня узгодженості оцінок експертів досягають при $W \geq 0{,}7$. При $0{,}5 < W$ результати експертизи слід визнати незадовільними, а етапи 2 і 3 експертизи повторити.

Етап 5 – встановлення поточних номерів РАП $s := 1$ і показника пріоритетності застосування $j := 1$.

Етап 6 – опрацювання результатів експертного опитування, а саме обчислення показника пріоритетності застосування $K^s_{B_{jm}}$, розрахунок усереднених значень бальних оцінок j -го показника пріоритетності застосування за співвідношенням [23]:

$$k^s_{B_j} = \frac{1}{M}\sum_{m=1}^{M} k^s_{B_{jm}}, \qquad (9)$$

де $k^s_{B_{jm}}$ – бальні оцінки j -го показника пріоритетності застосування n -ї РАП, отримані m -м експертом;

M – кількість експертів у групі.

З використанням узагальненої функції переваг Харрінгтона пропонується обчислювати j -й показник пріоритетності застосування за таким співвідношенням:

$$K^s_{B_i} = exp(-exp(-y^s_{Bj})). \qquad (10)$$

В аналітичній залежності (10) введено допоміжну величину $y^s_{B_j}$, яку пропонується визначати за таким співвідношенням:

$$y^s_{B_j} = -2 + \frac{7}{8}(k^s_{B_j} - 1). \qquad (11)$$

Етап 7 – збільшення поточного номера показника пріоритетності застосування, який розглядають, на одиницю $j := j + 1$;

Етап 8 – перевірка виконання умови розгляду всіх показників пріоритетності застосування. Якщо умову виконано, переходять до етапу 9 в іншому разі – повертаються до етапу 6.

Етап 9 – визначення підсумкового пріоритету (бальної оцінки) s -ї РАП, який пропонується визначати за таким співвідношенням:

$$K^s = \sum_{i=1}^{4} K^n_{A_i} \cdot V_{A_i} + \sum_{j=1}^{5} K^s_{B_j} \cdot V_{B_j}, \qquad (12)$$

де $K^n_{A_i}$ – значення показника важливості s -ї РАП;

V_{A_i} – ваговий коефіцієнт показника важливості;

$K^s_{B_j}$ – значення показника пріоритетності застосування s -ї РАП;

V_{B_j} – ваговий коефіцієнт показника пріоритетності застосування.

Вагові коефіцієнти V_{A_i} і V_{B_j} експертна група визначає так, щоб їхня сума дорівнювала 1.

Етап 10 – перевірка виконання умови розгляду всіх важливих РАП. Якщо умови виконано переходять до етапу 11, в іншому разі – до етапу 12.

Етап 11 – збільшення поточного номера важливої РАП на одиницю $s := s + 1$, встановлення поточного номера показника пріоритетності $j := 1$, та повернення до етапу 6.

Етап 12 – за результатами визначення бальних оцінок формування переліку пріоритетності серед важливих РАП. Кожну РАП зараховують до однієї з груп пріоритетів. Вважають, що s -та РАП під час її оснащення БС має такі пріоритети:

«дуже високий» – при $0{,}8 < K^s \le 1{,}0$;

«високий» – при $0{,}63 < K^s \le 0{,}8$;

«задовільний» – при $0{,}37 < K^s \le 0{,}63$;

«низький» – при $K^s \le 0{,}37$.

Числові межі груп пріоритетів обрано відповідно до вербально-числової шкали Харрінгтона. В межах груп пріоритетів «дуже високий», «високий», «задовільний», «низький» РАП упорядковують відповідно до отриманих значень пріоритетів (підсумкових бальних оцінок) у порядку від вищого до нижчого пріоритету.

Результати попередніх досліджень [24] показують, що для проведення експертного опитування доцільно призначати експертну групу з 5…7 експертів. Розглянемо приклад визначення пріоритетності артилерійських підрозділів (далі – АП) для оснащення їх безпілотними системами з використанням запропонованої методики. Для проведення експертизи було сформовано групу з $M = 5$ експертів. Пріоритетність оснащення БС пропонується визначати для трьох АП, $N = 3$.

За запропонованою методикою група експертів визначає перелік важливих АП для оснащення БС (див. рис. 1). За результатами експертного опитування на етапі 2, визначають бальні оцінки $k^n_{A_i}$ для кожного і -го показника важливості АП під час їх оснащення БС (табл. 3).

За результатами статистичної перевірки результатів опитування експертів (етап 3) встановлено узгодженість рішень експертів за співвідношеннями (1) – (5).

На етапі 4 проведено статистичну перевірку за допомогою коефіцієнта конкордації Кендала W, значення якого для показників важливості $A_1 ... A_4$ дорівнює: $W_{A_1} = 0{,}84$, $W_{A_2} = 0{,}84$, $W_{A_3} = 0{,}86$, $W_{A_4} = 1$, відповідно. Приклад статистичної перевірки результатів опитування експертів та узгодженості їх рішень наведено для показника важливості A_1. Отримані експертами $M = 5$ бальні оцінки показника важливості A_1 (див. табл. 3) для АП $N = 3$ наведено в табл. 4.

Отримані експертною групою у складі п’яти експертів бальні оцінки для трьох АП із застосуванням рекомендацій, наведених на етапі 3, перетворюють у ранги (табл. 5).

Далі визначають дисперсію рангів оцінок експертів D (табл. 6).

Застосовуючи співвідношення (4), (5), визначають максимальну дисперсію рангів оцінок експертів. За виразом (5) визначають t_m, k_m і T_m для кожного експерта.

Таблиця 3

Визначення важливості артилерійських підрозділів у процесі визначення пріоритетності їх оснащення безпілотними системами

Показник	Бальна оцінка показника важливості					$k^n_{A_i}$	$K^n_{A_i}$
	Експерт, $M_1 ... M_5$						
	1	2	3	4	5		
Артилерійський підрозділ № 1 (N_1)							
A_1 – ступінь впливу функціонування АП на результативність виконання оперативних (тактичних) завдань в операціях (діях)	9	7	8	9	7	8,0	0,98
A_2 – ступінь відповідності вогневих можливостей АП вимогам під час їх застосування в операціях (діях)	5	6	7	6	6	6,0	0,91
A_3 – ступінь відповідності маневрених можливостей АП вимогам під час їх застосування в операціях (діях)	7	5	6	6	5	5,8	0,89
A_4 – ступінь відповідності спроможності АП вимогам до виконання основних завдань за призначенням	9	9	8	8	7	8,2	0,99
Артилерійський підрозділ № 2 (N_2)							
A_1 – ступінь впливу функціонування АП на результативність виконання оперативних (тактичних) завдань в операціях (діях)	5	6	5	5	5	5,2	0,83
A_2 – ступінь відповідності вогневих можливостей АП вимогам під час їх застосування в операціях (діях)	4	5	5	4	5	4,6	0,73
A_3 – ступінь відповідності маневрених можливостей АП вимогам під час їх застосування в операціях (діях)	5	5	4	5	5	4,8	0,77
A_4 – ступінь відповідності спроможності АП вимогам до виконання основних завдань за призначенням	5	6	5	5	6	5,4	0,85
Артилерійський підрозділ № 3 (N_3)							
A_1 – ступінь впливу функціонування АП на результативність виконання оперативних (тактичних) завдань в операціях (діях)	5	6	5	5	7	5,6	0,88
A_2 – ступінь відповідності вогневих можливостей АП вимогам під час їх застосування в операціях (діях)	4	4	5	5	4	4,4	0,68
A_3 – ступінь відповідності маневрених можливостей АП вимогам під час їх застосування в операціях (діях)	7	8	7	7	6	7,0	0,96
A_4 – ступінь відповідності спроможності АП вимогам до виконання основних завдань за призначенням	3	4	3	4	4	3,6	0,47

Таблиця 4

Бальні оцінки показника важливості артилерійського підрозділу для його оснащення безпілотними системами

Артилерійські підрозділи	Бальні оцінки за показником A_1 – ступінь впливу функціонування АП на результативність виконання оперативних (тактичних) завдань в операціях (діях)				
	M_1	M_2	M_3	M_4	M_5
АП № 1 (N_1)	9	7	8	9	7
АП № 2 (N_2)	5	6	5	5	5
АП № 3 (N_3)	5	6	5	5	7

Таблиця 5

Ранги бальних оцінок, отриманих експертами за показником важливості A_1 для трьох артилерійських підрозділів

Експертна група	Бальні оцінки за показником A_1	Ранг бальних оцінок за показником A_1
Експерт M_1	{9; 5; 5}	{1; 2,5; 2,5}
Експерт M_2	{7; 6; 6}	{1; 2,5; 2,5}
Експерт M_3	{8; 5; 5}	{1; 2,5; 2,5}
Експерт M_4	{9; 5; 5}	{1; 2,5; 2,5}
Експерт M_5	{7; 5; 7}	{1,5; 3; 1,5}

Таблиця 6

Розрахунок дисперсії рангів бальних оцінок, отриманих експертами за показником важливості A_1

Артилерійські підрозділи	Ранги r_{nm}					$\sum_{m=1}^{M} r_{nm}$	$\sum_{n=1}^{N}\sum_{m=1}^{M} r_{nm}$	Δ_n	Δ_n^2	$D=\sum_{n=1}^{N}(\Delta_n)^2$
	Експерти									
	M_1	M_2	M_3	M_4	M_5					
АП № 1 (N_1)	1	1	1	1	1,5	5,5		-4,5	20,25	
АП № 2 (N_2)	2,5	2,5	2,5	2,5	3	13	5,5+13+11,5=30	3,0	9,0	20,5+9,0+2,25=31,5
АП № 3 (N_3)	2,5	2,5	2,5	2,5	1,5	11,5		1,5	2,25	

Експерт M_1 : $k_1=1$, $t_1=2$, $T_1=t_1^3-t_1=2^3-2=6$.

В оцінках експерта M_1 є одне повторення рангів: значення 2,5 повторено двічі.

Експерт M_2 : $k_2=1$, $t_2=2$, $T_2=t_2^3-t_2=2^3-2=6$.

Експерт M_3 : $k_3=1$, $t_3=2$, $T_3=t_3^3-t_3=2^3-2=6$.

Експерт M_4 : $k_4=1$, $t_4=2$, $T_4=t_4^3-t_4=2^3-2=6$.

Експерт M_5 : $k_5=1$, $t_5=1$, $T_5=t_5^3-t_5=2^3-2=6$.

Із застосуванням співвідношення (4) аналітична залежність для визначення максимальної дисперсії D_{max} рангів оцінок п'яти експертів для трьох АП матиме такий вигляд:

$$D_{max}=\frac{1}{12}M^2(N^3-N)-\frac{1}{12}M\cdot\sum_{m=1}^{M}T_m=\frac{1}{12}M^2(N^3-N)-\frac{1}{12}M\cdot(T_1+T_2+T_3+T_4+T_5). \quad (13)$$

Підставивши вхідні параметри, отримують розв'язок співвідношення (13):

$$D_{max}=\frac{1}{12}5^2(3^3-3)-\frac{1}{12}5\cdot(6+6+6+6+6)=50-12{,}5=37{,}5. \quad (14)$$

Відповідно до етапу 4 перевіряють виконання умов узгодженості оцінок експертів за співвідношенням (1), визначаючи коефіцієнт конкордації Кендала:

$$W_{A_1}=\frac{D}{D_{max}}=\frac{31{,}5}{37{,}5}=0{,}84. \quad (15)$$

Оскільки $W_{A_1}\geq 0{,}7$, то гіпотезу про узгодженість оцінок експертів приймають.

Пропонується обробляти результати експертного опитування (див. табл. 3) та обчислювати значення показника важливості $K^{n}_{A_i}$ за співвідношенням (7), застосовуючи розраховані усереднені значення бальних оцінок показників важливості АП $k^{n}_{A_i}$, обчислені за співвідношенням (6).

Перевіряють виконання умови $K^{n}_{A_i}>0{,}63$ для всіх показників важливості $(i\in\{1,4\})$ для всіх АП $(n\in\{1,N\})$. Оскільки для АП № 3 (N_3) значення $K^{3}_{A_4}=0{,}47<0{,}63$, пропонується вважати АП № 3 (N_3) неважливим. З решти (АП № 1 (N_1) та АП № 2 (N_2)) формують перелік АП для визначення пріоритетності їх оснащення БС.

За запропонованою методикою групою експертів визначається перелік пріоритетних АП для їх оснащення БС (див. рис. 2). При цьому, за результатами експертного опитування (етап 2) пропонується визначати бальні оцінки $k^{s}_{B_j}$ для кожного j-го показника пріоритетності застосування АП під час їх оснащення БС (табл. 7).

За результатами статистичної перевірки результатів опитування експертів (етап 3) встановлено узгодженість рішень експертів за співвідношеннями (1) – (5).

На етапі 4 проведено статистичну перевірку за допомогою коефіцієнта конкордації Кендала W, значення якого для показників пріоритетності застосування $B_1...B_5$ значення якого вказує на узгодженість рішень. Застосовуючи розраховані усереднені значення бальних оцінок показників важливості $k^{s}_{B_j}$ та значення показників пріоритетності застосування АП $K^{s}_{B_j}$, (див. табл. 7), за співвідношенням (12) визначають підсумкову оцінку (пріоритет) АП для оснащення його БС:

$$K^1=\frac{1}{9}\cdot(0{,}98+0{,}91+0{,}89+0{,}99)+\frac{1}{9}\cdot(0{,}97+0{,}97+0{,}89+0{,}98+0{,}92)=0{,}95; \quad (16)$$

$$K^2=\frac{1}{9}\cdot(0{,}83+0{,}73+0{,}77+0{,}85)+\frac{1}{9}\cdot(0{,}83+0{,}73+0{,}80+0{,}77+0{,}77)=0{,}79 \quad (17)$$

У наведеному прикладі значення вагових коефіцієнтів V_{A_i} і V_{B_j} серед усіх вагових

коефіцієнтів дорівнює 1/9. За підсумковими оцінками пріоритету АП № 1 – $K^1 = 0{,}95$ та пріоритету АП № 2 – $K^2 = 0{,}79$ упорядковують перелік важливих АП. Артилерійський підрозділ зараховують до однієї з груп пріоритетів: АП № 1 – до групи «дуже високий», оскільки $0{,}8 < k^1 = 0{,}95 \le 1{,}0$; АП № 2 – до групи «високий», оскільки $0{,}63 < k^2 = 0{,}79 \le 0{,}8$.

Таблиця 7

Визначення пріоритетності застосування артилерійського підрозділу для його оснащення безпілотними системами

Показник	Бальна оцінка показника важливості					$k^s_{B_j}$	$K^s_{B_j}$
	Експерт, $M_1...M_5$						
	1	2	3	4	5		
Артилерійський підрозділ № 1 (N_1)							
B_1 – ступінь участі АП в дезорганізації системи управління військами і зброєю, розвідки та радіоелектронної боротьби противника	8	7	7	7	7	7,2	0,97
B_2 – ступінь участі АП у протидії засобам ураження повітряного базування та протиповітряної оборони противника	7	7	7	9	7	7,4	0,97
B_3 – ступінь участі АП у вогневій протидії засобам вогневої підтримки противника	5	7	5	5	7	5,8	0,89
B_4 – ступінь участі АП у зниженні спроможностей частин (підрозділів) угруповання військ (сил) противника	7	7	9	9	7	7,8	0,98
B_5 – ступінь участі АП у порушенні логістичного забезпечення	7	5	7	7	5	6,2	0,92
Артилерійський підрозділ № 2 (N_2)							
B_1 – ступінь участі АП в дезорганізації системи управління військами і зброєю, розвідки та радіоелектронної боротьби противника	6	5	5	4	6	5,2	0,83
B_2 – ступінь участі АП у протидії засобам ураження повітряного базування та протиповітряної оборони противника	5	4	5	5	4	4,6	0,73
B_3 – ступінь участі частини АП у вогневій протидії засобам вогневої підтримки противника	5	6	5	4	5	5,0	0,80
B_4 – ступінь участі АП у зниженні спроможностей частин (підрозділів) противника	5	5	5	4	5	4,8	0,77
B_5 – ступінь участі АП у порушенні логістичного забезпечення	5	5	4	5	5	4,8	0,77

Висновки і перспективи подальших досліджень

Таким чином, у статті набула подальшого розвитку чинна методика [23]. Для обґрунтування рекомендацій щодо визначення пріоритетності РАП під час їх оснащення безпілотними системами запропоновано застосовувати дві групи показників: важливості та пріоритетності застосування РАП. Узгодження результатів експертного опитування у пропонованій методиці проведено за допомогою коефіцієнта конкордації Кендала. Бальні оцінки показників, отриманих експертами, приведено до єдиної безрозмірної шкали переваг, для чого використано узагальнену функцію переваг Харрінгтона. Це дало змогу виключити помилки в оцінках експертів, спричинені їх психологічними особливостями (нелінійним зв'язком між значеннями показника та його оцінкою експертом). Отримані внаслідок таких перетворень значення показників важливості та пріоритетності пропонується використовувати для розрахунку підсумкової оцінки і з'ясування пріоритету РАП в їх оснащенні безпілотними системами.

Методику пропонується застосовувати в органах військового управління під час визначення пріоритетності РАП для їх оснащення безпілотними системами.

Список бібліографічних посилань

1. Головченко О., Іщенко О., Линок Н. Здобуті уроки ведення бойових дій артилерійськими підрозділами в ході збройного конфлікту на Сході України за аспектом живучості в 2014–2015 роках. *Воєнно-історичний вісник*: зб. наук. пр. Київ, 2021. № 1(39). С. 82–96. DOI: https://doi.org/10.33099/2707-1383-2021-39-1-82-96.

2. Репіло Ю. Є., Головченко О. В., Іщенко О. В. Контент-аналіз уроків збройного конфлікту в Нагірному Карабасі щодо вогневої підтримки військових формувань Азербайджану в наступальних діях. *Збірник наукових праць Національної академії Державної прикордонної служби України. Військові та технічні науки*. Хмельницький, 2021. № 1 (84). С. 86–99. DOI: https://doi.org/10.32453/3.v84i1.805.

3. Репіло Ю. Є., Головченко О. В. Обґрунтування показників та критерію можливої живучості артилерійських підрозділів під час вогневої підтримки в наступальних діях.

Системи озброєння і військова техніка. Харків, 2021. № 3 (67). С 39–44. DOI: https://doi.org/10.30748/soivt.2021.67.05. **4. Репіло Ю. Є., Головченко О. В.** Аналіз базових концепцій і понять вогневої підтримки артилерійськими підрозділами в бою армій країн НАТО. *Грааль науки*. Вінниця, 2023. № 27. С. 209–211. DOI: https://doi.org/10.36074/grail-of-cience.12.05.2023.030. **5. STANAG 2484** AARTYP-05 Ed B *NATO Fire Support Doctrine*, 5 November 2015. URL: https://nato.int (дата звернення 12.05.2023). **6. FM 3-09** *Fire Support and Field Artillery Operations*, 30 April 2020. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **7. ATP 3-09.12** *Field Artillery Target Acquisition*, 24 July 2015. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **8. ATP 3-09.23** *Field Artillery Cannon Battalion*, 24 September 2015. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **9. ATP 3-09.24** *Techniques for the Fires Brigade*, 21 November 2012. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **10. ATP 3-09.42** *Fire Support for The Brigade Combat Team*, 1 March 2016. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **11. ATP 3-09.50** *The Field Artillery Cannon Battery*, 04 May 2016. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **12. ATP 3-09.70** *Paladin Operations*, 25 September 2015. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **13. ATP 3-09.90** *Division Artillery Operations and Fire Support for the Division*, 12 October 2017. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **14. Temiz Y. Z.** Artillery survivability (Monterey, California: Postgraduate School, 2016). URL: http://hdl.handle.net/10945/49399 (дата звернення: 07.02.2022). **15. Younglak S.** An analysis of «shoot-and-scoot» tactics (Monterey, California: Postgraduate School, 2017). URL: https://hdl.handle.net/10945/53047 (дата звернення: 24.08.2022). **16. Browne K. D.** Self-propelled wheeled howitzer for Marine Corps use: capability-based assessment (Monterey, California: Postgraduate School, 2018). URL: http://hdl.handle.net/ 10945/61319 (дата звернення: 03.01.2023). **17. Turk J. H**. Analysis of artillery survivability in distribute operations (Monterey, California: Postgraduate School, 2020). URL: http://hdl.handle.net/10945/64893 (дата звернення: 11.02.2023). **18. Репіло Ю. Є., Головченко О. В., Купрієнко Д. А.** Модель застосування ракетних та артилерійських підрозділів під час вогневої підтримки в операції (бою) з використанням теорії випадкових процесів зі скінченною множиною станів. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, 2021. № 2 (44). С. 28–37. DOI: https://doi.org/10.33099/2311-7249/2022-44-2-28-37. **19. Репіло Ю. Є., Іщенко О. В.** Методика оцінювання відповідності можливостей безпілотних авіаційних комплексів щодо повітряної розвідки в інтересах виконання вогневих завдань артилерією у збройних конфліктах. *Збірник наукових праць Національної академії Державної прикордонної служби України. Військові та технічні науки*. Хмельницький, 2022. № 3 (88). С. 125–149. DOI: https://doi.org/10.32453/3.v88i3.1252. **20. Khudov H., Oleksenko O., Lukianchuk V., Herasymenko V., Yaroshenko Y., Ishchenko O., Ikaiev D., Golovchenko O., Volobuiev A., Drob Y., Solomonenko Y., Khizhnyak I.** The determining the flight routes of unmanned aerial vehicles groups based on improved ant colony algorithms. *International Journal of Emerging Technology and Advanced Engineering.* 2021. Vol. 11, Issue 9. P. 23–32. DOI: https://doi.org/10.46338/IJETAE0921 03. **21. Майстренко О., Караванов О., Лихольт О.** Обґрунтування сукупності показників оцінювання стійкості функціонування розвідувально-вогневих систем. *Честь і закон*. 2022. No 1 (80). С. 19–25. DOI: https://doi.org/10.33405/2078-7480/2022/1/80/262458. **22. Гамора В. В.** Удосконалена методика визначення пріоритетності об'єктів ураження противника для нанесення ракетно-авіаційних ударів в операціях (бойових діях) Збройних Сил України. *Наука і техніка Повітряних Сил України*. Харків, 2014. № 4 (17). С. 5–9. **23. Коваль В. В., Сень М. П., Лагно Є. О., Ларін В. В., Таран І. А.** Методика визначення пріоритетності науково-дослідних та дослідно-конструкторських робіт, які пов'язані зі створенням (модернізацією) зразків озброєння та військової техніки. *Наука і техніка Повітряних Сил України*. Харків, 2022. № 3 (48). С. 7–16. DOI: https://doi.org/10.30748/nitps.2022.48.01.
24. Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання : монографія. Вінниця : ВНТУ, 2010. 171 с. **25. Лук'янчук В., Ніколаєв І., Опенько П, Дзеверін І, Угрінович О.** Методика визначення пріоритетності проектів науково-дослідних робіт у сферах розробок озброєння та військової техніки. *Journal of Scientific Papers «Social Development and Security»*. Київ, 2020. № 6 (10). С. 40–56. **26. Телелим В. М., Шевчук В. В., Баргилевич А. В.** Методичний підхід до визначення пріоритетності важливих об'єктів в зоні територіальної оборони, охорона та оборона яких покладається на формування територіальної оборони держави. *Наука і техніка Повітряних Сил України*. Харків, 2020. № 4 (41). С. 37–43. DOI: https://doi.org/10.30748/nitps.2020.41.04.
27. Ярош С. П., Філіпенко О. В. Удосконалена методика визначення важливості елементів оперативної побудови оперативного угруповання військ. *Збірник наукових праць Харківського національного університету Повітряних Сил України*. Харків, 2022. № 2 (72). С. 14–20. DOI: https://doi.org/10.30748/zhups.2022.72.02. **28. Теоретичні** основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / [О. М. Загорка, А. К. Павліковський, А. А. Корецький, С. О. Кириченко, І. О. Загорка] ; за заг. ред. І. С. Руснака. Київ: НУОУ ім. Івана Черняховського, 2020. 248 с. **29. Розвідувально-ударні**, розвідувально-вогневі комплекси (принципи побудови в умовах реалізації концепції мережецентричних війн, оцінка ефективності бойового застосування) : монографія / [В. М. Тарасов, Р. І. Тимошенко, О. М. Загорка] ; за заг. ред. В. М. Телелима. Київ : НУОУ ім. Івана Черняховського, 2015. 248 с. **30**. **Доктрина** «Ракетні війська і артилерія» затверджена Головнокомандувачем Збройних Сил України 03.11.2022, СДП 3-06,07(03).01.

METHOD FOR DETERMINING THE PRIORITY OF THE MISSILES AND ARTILLERY UNITS FOR THEIR EQUIPMENT WITH UNMANNED SYSTEMS

Repilo Iurii (Doctor of Military Sciences, Professor)
Golovchenko Oleg (Doctor of Philosophy)
Riman Oleksii (Candidate of Military Sciences, Associate Professor)

National Defence University of Ukraine, Kyiv, Ukraine

The results of the analysis of lessons learned in the use of troops (forces) in the course of military operations in recent years show that the success of operations (actions) will largely depend on effective fire support. In turn, achieving its desired effectiveness is impossible without timely and reliable intelligence data about enemy objects (targets) using unmanned systems. At the same time, in the theory and practice of managing missile and artillery units, an unacceptable discrepancy arose between the need to equip missile and artillery units with unmanned systems and the limited number of such systems based on priority.

So, there is a need to maximize the equipment of missile and artillery units depending on the specifics of fire support tasks, and on the other hand, there is a limited number of unmanned systems that can provide missile and artillery units with up-to-date intelligence on enemy objects (targets) for performance of fire support tasks in operations (actions). Based on this, the purpose of the article is to develop a methodology for determining the priority of missile and artillery units to be equipped with unmanned systems. In the article, the method of solving the problem of multi-criteria selection of the optimal solution among alternatives based on priority by the method of expert survey was further developed. At the same time, to determine the priority of the multidimensional system when solving the problem of multi-criteria selection, it is proposed to use two groups of indicators: the importance and priority of the use of missile and artillery units. The expert survey is agreed using Kendall's concordance coefficient. Scores of indicators obtained by experts lead to a single dimensionless scale of preferences, for which Harrington's generalized preference function is used. The proposed methodology is proposed to be used in the military administration bodies when determining the priority of missile and artillery units for their equipping with unmanned systems.

Keywords: *management, priority, importance, fire support, missile and artillery units, unmanned systems, expert survey, Kendall's concordance coefficient, Harrington's preference function.*

References

1. Holovchenko, O., Ishchenko, O., & Lynok, N., (2021). Lessons learned by artillery units in armed conflict in eastern Ukraine in the aspect of survival in 2014–2015. *Military Historical Bulletin*, 39(1), 8-–96. https://doi.org/10.33099/2707-1383-2021-39-1-82-96. **2. Repilo, I.**, **Golovchenko, O., & Ishchenko, O.,** (2021). Content analysis of lessons learned from armed conflict in Nagorno-Karabakh for fire support for maneuver formations of Azerbaijan in offensive actions. *Collection of Scientific Works of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences*, 84(1), 86–99. https://doi.org/10.32453/3.v84i1.805. **3. Repilo, I., & Golovchenko, O.,** (2021). Justification of indicators and criterion of possible survivability of artillery units during fire support in offensive operations. *Systems of Arms and Military Equipment*, 3(67), 39-44. https://doi.org/10.30748/soivt.2021.67.05. **4. Repilo, I., & Golovchenko, O.,** (2023). Analysis of basic concepts and definitions of fire support by artillery units in battle of the armies of NATO countries. *Grail of Science*, 27, 209-211. https://doi.org/10.36074/grail-of-science.12.05.2023.030.
5. STANAG 2484 AARTYP-05 Ed B *NATO Fire Support Doctrine*, 5 November 2015. URL: https://nato.int (дата звернення 12.05.2023). **6. FM 3-09** *Fire Support and Field Artillery Operations*, 30 April 2020. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **7. ATP 3-09.12** *Field Artillery Target Acquisition*, 24 July 2015. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **8. ATP 3-09.23** *Field Artillery Cannon Battalion*, 24 September 2015. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **9. ATP 3-09.24** *Techniques for the Fires Brigade*, 21 November 2012. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **10. ATP 3-09.42** *Fire Support for The Brigade Combat Team*, 1 March 2016. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **11. ATP 3-09.50** *The Field Artillery Cannon Battery*, 04 May 2016. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **12. ATP 3-09.70** *Paladin Operations*, 25 September 2015. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **13. ATP 3-09.90** *Division Artillery Operations and Fire Support for the Division*, 12 October 2017. URL: https://armypubs.army.mil (дата звернення 12.05.2023). **14. Temiz, Y. Z.,** (2016). Artillery survivability. Monterey, California: Postgraduate School. URL: http://hdl.handle.net/10945/49399 (дата звернення: 07.02.2022). **15. Younglak S.,** (2017). An analysis of «shoot-and-scoot» tactics. Monterey, California: Postgraduate School. URL: https://hdl.handle.net/10945/53047 (дата звернення: 24.08.2022). **16. Browne K. D.,** (2018). Self-propelled wheeled howitzer for Marine Corps use: capability-based assessment (Monterey, California: Postgraduate School,). URL: http://hdl.handle.net/10945/61319 (дата звернення: 03.01.2023). **17. Turk, J. H**. (2020). Analysis of artillery survivability in distribute operations. Monterey, California: Postgraduate School. URL: http://hdl.handle.net/10945/64893 (дата звернення: 11.02.2023). **18. Repilo, I., Golovchenko, O., & Kupriyenko, D.,** (2022). A model of the missiles and artillery units employment at the fire support in operation (combat) using the theory of random processes with a finite set of states. *Modern Information Technologies in the Sphere of Security and Defence,* 2 (44), 28-37, https://doi.org/10.33099/2311-7249/2022-44-2-28-37. **19. Repilo, I., & Ishchenko, O.,** (2022). The method of assessing the adequacy of the capabilities of unmanned aviation complexes regarding aerial reconnaissance in the interests of performing artillery fire tasks in armed conflicts. *Collection of Scientific Works of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences*, 88, 3, 125-149, https://doi.org/10.32453/3.v88i3.1252. **20. Khudov, H., Oleksenko, O., Lukianchuk, V., Herasymenko, V., Yaroshenko, Y., Ishchenko, O., Ikaiev, D., Golovchenko, O., Volobuiev, A., Drob, Y., Solomonenko, Y., Khizhnyak, I.,** (2021). The determining the flight routes of unmanned aerial vehicles groups based on improved ant colony algorithms. International Journal of Emerging Technology and Advanced Engineering, 11, 9, 23-32, https://doi.org/10.46338/IJETAE0921 03. **21. Maistrenko, O., Karavanov O., & Lykholot O.,** (2022). Substantiation of a set of indicators for assessing the stability of the functioning of reconnaissance and fire systems. *Honor and Law.* 1(80), 19–25, https://doi.org/10.33405/2078-7480/2022/1/80/262458.
22. Hamora, V. V., (2014). Improved method of determination of priority of defeat rocket objects opponent for -aviation inflictings blows in the operations (battle actions) of Military Forces of Ukraine, *Science and Technology of the Air Force of Ukraine*, 4(17), 5–9. **23. Koval, V., Sen, M., Lahno, E., Larin, V., & Taran, I.,** (2022). A methodology of determining the priority of research and development works related to the creation (modernization) of armament and military equipment samples. *Science and Technology of the Air Force of Ukraine*, No. 3 (48), pp. 7–16. https://doi.org/10.30748/nitps.2022.48.01.
24. Hrabovetskyi, B. Ye. (2010), Methods of expert evaluations: theory, methodology, directions of use" (Textbook), Vinnytsia. VNTU, 2010. p.171. **25. Lukyanchuk, V.,** et al., (2020). Methods of Determining the Priority of Research Projects in the Field of Development of Armament and Military Equipment. *Social Development and Security*, 10, 6, 40-56, doi: 10.33445/sds.2020.10.6.5. **26. Telelim, V., Shevchuk, V., & Bargilevich, A.,** (2020). Methodical approach to determining the priority of important objects and communications of the territorial defense, the protection and defense of the territorial defense units. *Science and Technology of the Air Force of Ukraine*, (4(41), 37-43. https://doi.org/10.30748/nitps.2020.41.04. **27. Yarosh, S., & Filippenkov, O.,** (2022). The improved methodology of determination of the importance of objects from deployment design of the combined arms task force. *Scientific Works of Kharkiv National Air Force University*, 2(72), 14-20. https://doi.org/10.30748/zhups.2022.72.02. **28. Zagorka, O., Pavlikovskyi, A., Koretskyi, A., Kyrychenko, S. & Zagorka, I.,** (2020) Theoretical foundations of managing a group of troops (forces) in modern conditions of armed struggle. (Textbook), Kyiv. NUOU, 248. **29. Tarasov, V., Tymoshenko, R., & Zagorka, O.,** (2015). Reconnaissance and strike, reconnaissance and fire complexes (principles of construction in the implementation of the concept of network-centric wars, assessment of the effectiveness of combat use). (Textbook), Kyiv. NUOU, 2015. 184. **30. Doktryna** «Raketni viiska i artyleriia» zatverdzhena Holovnokomanduvachem Zbroinykh Syl Ukrainy 03.11.2022, SDP 3-06,07(03).01.

DOI:**10.33099/2311-7249/2023-47-2-67-74**

УДК 004.94:355

Дядечко Андрій Олександрович *(доктор філософії)* [1]
Даценко Іван Петрович *(кандидат технічних наук)*[2]

[1] ***Національний університет оборони України, Київ, Україна***
[2] ***Воєнна академія імені Євгенія Березняка, Київ, Україна***

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТРОЛОГІЧНОГО ОБСЛУГОВУВАННЯ ЗАСОБІВ ВИМІРЮВАЛЬНОГО КОНТРОЛЮ ПАРАМЕТРІВ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

У статті теоретично проаналізовані положення керівних документів та урядових програм стосовно підвищення ефективності систем забезпечення Сил оборони держави, а саме, системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки Збройних сил України. Проаналізовано наукові публікації, в яких досліджувались шляхи підвищення ефективності системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки та визначені їх основні недоліки. Під час написання статті застосовані методи аналізу та синтезу складних систем, а також теорія діагностики, зокрема методи технічного діагностування технічних систем. Цей підхід дав змогу обґрунтувати рекомендації стосовно підвищення ефективності метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння та військової техніки. Для досягнення цього було розроблено низку організаційно-технічних заходів. Їх реалізація дасть змогу удосконалити існуючу систему метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки й підвищити ефективність її функціонування. Запропоновано удосконалення системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння та військової техніки шляхом синтезу її існуючих підсистем і підсистеми моніторингу й діагностики засобів вимірювального контролю, як додаткового елементу системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки. Практичним значенням статті є обґрунтування рекомендацій щодо застосування на зразках озброєння і військової техніки універсального пристрою контролю метрологічних характеристик, як технічного рішення, що дозволить здійснювати контроль за станом засобів вимірювального контролю в режимі, що наближений до реального часу. Це, в свою чергу, дасть змогу своєчасно реагувати на відмови в роботі агрегатів і систем зразків озброєння і забезпечить підтримання їх готовності до виконання завдань за призначенням.

Ключові слова: *метрологічне обслуговування, засоби вимірювання, інформаційно-вимірювальна система, вимірювальна інформація, вимірювальний контроль, діагностика.*

Вступ

Постановка проблеми. Виклики та загрози національній безпеці України, зацікавленість України в набутті членства в Європейському союзі (далі – ЄС) і НАТО та відповідно до цього – впровадження в діяльність Збройних сил України (далі – ЗС України) стандартів НАТО вимагають від керівництва держави основну увагу приділяти необхідності підтримання обороноздатності на потрібному для захисту від агресії рівні та створення сучасних, професійних, високомобільних, оснащених якісною технікою збройних сил, що в свою чергу вимагає проведення цілеспрямованої політики в побудові ефективної системи метрологічного забезпечення (далі – МлЗ) військ (сил).

Оскільки головною функцією системи МлЗ озброєння та військової техніки (далі – ОВТ) є своєчасне та повне виконання комплексу заходів спрямованих на забезпечення єдності вимірювань у військових частинах, установах та достовірності вимірювального контролю параметрів зразків ОВТ, то очевидно, що ефективна робота системи дасть змогу підтримувати зразки ОВТ в постійній готовності до використання за призначенням [1].

Основою МлЗ є проведення вимірювань на об’єктах ОВТ, контроль параметрів основних вузлів та агрегатів, а також засобів їх контролю. Враховуючи те, що основною складовою частиною системи МлЗ є система метрологічного обслуговування (далі – МлОб) засобів вимірювального контролю (далі – ЗВК) параметрів зразків ОВТ, то основну увагу необхідно звернути саме на удосконалення цієї системи, що вплине на ефективність функціонування системи МлЗ в цілому.

Аналіз остатніх досліджень і публікацій. В керівних документах та Державних урядових програмах [2-5] визначено низку заходів на короткострокову перспективу до 2025 року та

довгострокову перспективу, що спрямовані на удосконалення систем забезпечення Сил оборони держави, зокрема ЗС України. Однією з ключових систем забезпечення є система МлЗ та її основна складова – підсистема МлОб ЗВК параметрів зразків ОВТ.

Проте реалізація зазначених заходів задовольнить потреби ЗС України щодо організації функціонування системи МлОб ЗВК параметрів зразків ОВТ лише частково. Отже актуальним постає питання обґрунтування рекомендацій щодо підвищення ефективності МлОб ЗВК параметрів зразків ОВТ. Їхня реалізація, разом із виконанням заходів регламентованих керівними документами та урядовими програмами, забезпечить необхідний рівень ефективності функціонування системи МлОб ЗВК параметрів зразків ОВТ.

Разом з тим в проаналізованих наукових працях [6–9] досліджувались питання підвищення ефективності системи МлЗ в цілому, проте ефективність системи МлОб ЗВК параметрів зразків ОВТ, як складової частини системи МлЗ, досліджувалась опосередковано.

У зазначених наукових працях були запропоновані шляхи щодо підвищення ефективності системи МлОб ЗВК параметрів зразків ОВТ які можна розділити на два основних підходи:

підвищення ефективності системи за рахунок зменшення часу проведення МлОб зразків ОВТ з урахуванням часу роботи виїзних метрологічних груп (далі – ВМГ) та періодичності проведення обслуговування;

підвищення ефективності системи за рахунок визначення раціонального складу ВМГ та розподілу їх у відповідності до завдань з МлОб.

Проте у вищевказаних роботах не надано рекомендацій щодо врахування впливу МлОб на показники надійності ЗВК та ОВТ, можливостей системи МлОб реагувати на відмови в роботі ЗВК, а також щодо достовірності результатів МлОб.

Мета статті. Обґрунтування рекомендацій щодо підвищення ефективності метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння та військової техніки.

Виклад основного матеріалу дослідження

Відповідно до Стратегічного оборонного бюлетеню України [2] та Стратегії воєнної безпеки України [3] передбачені такі основні напрями удосконалення системи МлОб ЗВК параметрів зразків ОВТ:

розвиток та перехід парку вимірювальної техніки, що необхідна для контролю параметрів і характеристик агрегатів та систем зразків ОВТ, з аналогової на цифрову;

організація автоматизації процесів управління та прийняття рішення (в тому числі й щодо фактичного технічного стану зразків ОВТ);

підвищення рівня бойових можливостей наявних бойових броньованих машин шляхом оснащення новими і модернізованими системами та сучасними засобами контролю параметрів, зв'язку, автоматизації, управління та навігації;

формування Єдиної автоматизованої системи управління Збройних Сил (C4ISR) та інтеграція до неї автоматизованих систем усіх видів та спеціальних військ.

Виконання цих напрямів дасть змогу організувати функціонування перспективної системи МлОб, відповідно до схеми, наведеної на рис. 1.

Крім того, реалізація визначених напрямів дасть змогу здійснювати безперервний об'єктивний контроль за станом агрегатів та систем зразків ОВТ. Разом із тим ЗВК параметрів зразків ОВТ залишаються поза безперервним об'єктивним контролем, що може призвести до появи прихованих та неприхованих відмов в їх роботі і як наслідок призвести до виходу з ладу агрегатів та систем зразків ОВТ. Отже, з урахуванням цього існує потреба удосконалення системи метрологічного обслуговування для підвищення ефективності її функціонування.

Основною метою розвитку вимірювальної техніки визначається забезпечення потрібного для підтримання боєготовності та відтворення боєздатності військ (сил) рівня достовірності контролю параметрів ОВТ на усіх стадіях та етапах їх життєвого циклу на основі вдосконалення існуючого парку засобів вимірювання та створення автоматизованої магістрально-модульної багатофункціональної апаратури для комплексної оцінки технічного стану існуючого ОВТ та ОВТ нового покоління (в тому числі того, яке надходить від держав-партнерів).

В свою чергу, основною метою розвитку системи МлОб ЗВК параметрів зразків ОВТ визначається створення ефективної, мобільної, автономної та оперативної системи на основі впровадження автоматизації процесу МлОб та здійснення контролю метрологічних характеристик засобів вимірювання. За їхньою допомогою здійснюється контроль параметрів агрегатів і систем зразків ОВТ в режимі, що наближений до реального часу. Крім того, до мети розвитку означеної системи входять реалізація нових засобів і методів вимірювання фізичних величин й передача їхніх розмірів.

Для досягнення цієї мети потрібно вирішити комплекс таких науково-технічних і організаційних заходів:

науково-теоретичне обґрунтування можливостей втілення у військову практику єдності і точності вимірювань на основі нової метрологічної техніки;

адаптація керівних документів з питань МлЗ до сучасних вимог організації та проведення МлОб ЗВК параметрів зразків ОВТ, зокрема з питань перегляду інтервалів між проведенням МлОб, організування та проведення оцінювання стану забезпечення єдності вимірювань у ЗС України;

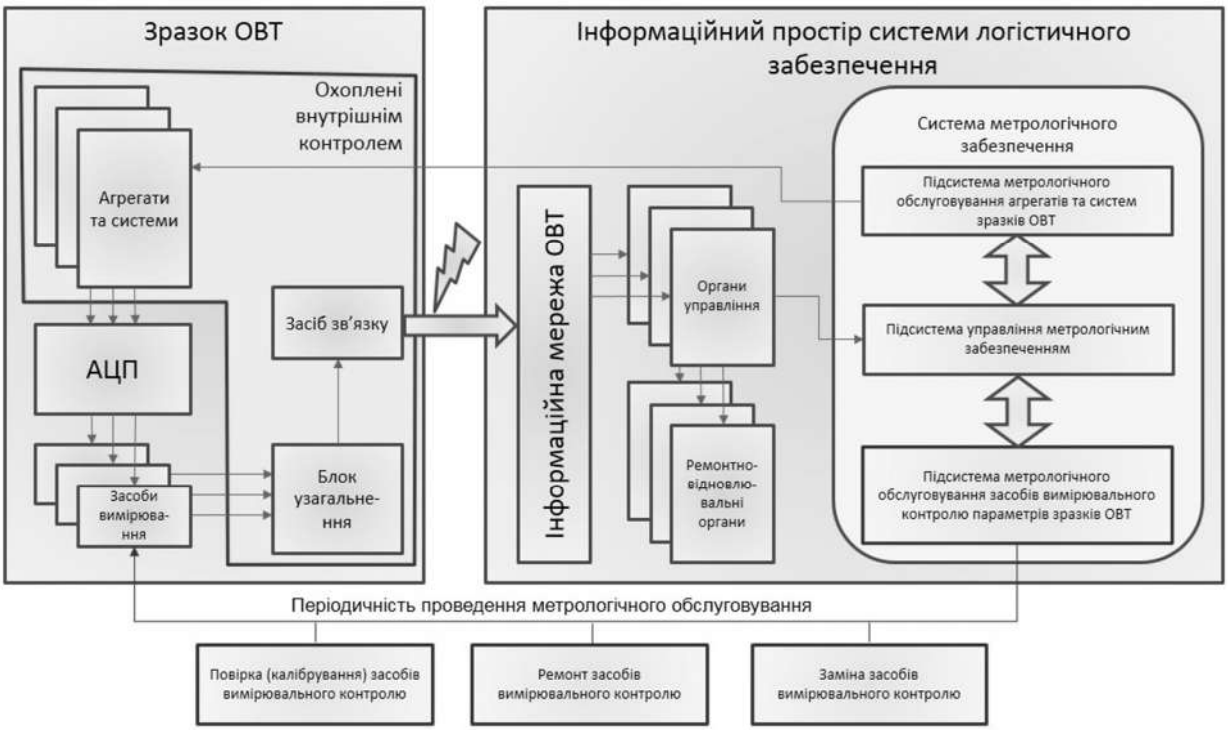


Рисунок 1 – Схема функціонування перспективної системи МлОб ЗВК параметрів зразків ОВТ

удосконалення програм підготовки фахівців-метрологів та штатних розрахунків (екіпажів, обслуги) ОВТ з питань МлОб ЗВК;

реорганізація існуючої структури системи МлОб ЗВК параметрів зразків ОВТ за рахунок введення додаткового елементу системи, який дає змогу здійснювати незалежний контроль за станом засобів вимірювання та параметрами зразків ОВТ;

розвиток наукових основ воєнної метрології, системи воєнно-метрологічного супроводження розроблення і створення ОВТ, вдосконалення законодавчої метрології;

оснащення зразків ОВТ сучасними цифровими ЗВК параметрів;

оснащення зразків ОВТ незалежними засобами контролю метрологічних характеристик засобів вимірювання та параметрів агрегатів та систем зразків ОВТ для забезпечення їх моніторингу та діагностики в режимі наближеному до реального часу;

інтеграція зразків ОВТ в єдину систему логістичної підтримки;

застосування стандартів передачі вимірювальної інформації на основі LXI-технології під час проведення МлОб ЗВК параметрів зразків ОВТ;

оснащення метрологічних частин і підрозділів новим поколінням калібрувального (повірочного) обладнання.

Розвиток методів і засобів забезпечення єдності і точності вимірювань необхідно проводити за такими напрямками:

пошук нових методів вирішення вимірювальних задач, створення нормативної бази для впровадження комплексної атестації вимірювальних процесів, яка дасть можливість оцінювати сумарну похибку всього вимірювального процесу. Водночас потрібно враховувати вплив допоміжного обладнання і засобів обробки інформації, рівень кваліфікації персоналу та ін. Вже попередні результати досліджень, що здійснюються за цим напрямком, підтверджують можливість підвищити точність виконання повірочних робіт і достовірність їх результатів, за одночасного скорочення загальних витрат, у 3–4 рази;

підвищення рівня автономності системи МлОб ЗВК параметрів зразків ОВТ шляхом створення розподілених і сукупних групових мір;

визначення інтервалів між проведенням МлОб ЗВК контролю параметрів зразків ОВТ у відповідності з їх реальним технічним станом. Хід розроблення методик визначення міжповірочних та міжкалібрувальних інтервалів [10; 11] та методики оцінювання реагування системи МлОб на відмови в роботі ЗВК [12] свідчить про можливість подовження інтервалів між проведенням метрологічного обслуговування засобів вимірювання за деякими видами вимірювань у 1,5–2 рази, що дасть змогу скоротити витрати на проведення метрологічних робіт на 30-40 %;

широке впровадження у практику МлОб ЗВК параметрів зразків ОВТ інструментального оцінювання стану метрологічного обслуговування. Це дасть змогу підвищити правильність прийняття рішення про стан засобів вимірювання і зразків ОВТ і зменшити вплив на нього суб'єктивних факторів.

Забезпечення практичної передачі розмірів одиниць фізичних величин шляхом обладнання зразків ОВТ відповідними технічними засобами, дає змогу передавати вимірювальну інформацію

про стан ЗВК, а також агрегатів та систем зразка ОВТ на усіх рівнях військових повірочних схем. Це можливо завдяки укомплектуванню новим поколінням вимірювальних приладів, що підключені до інформаційного простору системи логістичного забезпечення, метрологічних частин і підрозділів.

Постійне підвищення вимог до якісних показників ОВТ, зростання впливу МлЗ на боєздатність військ вимагають подальшої реорганізації існуючої структури системи МлОб ЗВК параметрів зразків ОВТ та порядку проведення МлОб засобів вимірювання. За таких умов метрологічні частини та підрозділи мають відповідати встановленим вимогам до оперативності виявлення відмов засобів вимірювання та їх усунення, маневрування, здатності розподілу на самостійні підрозділи, достатності виробничих потужностей. Рекомендації щодо структури та функціонування системи МлОб ЗВК параметрів зразків ОВТ наведені на рис. 2.

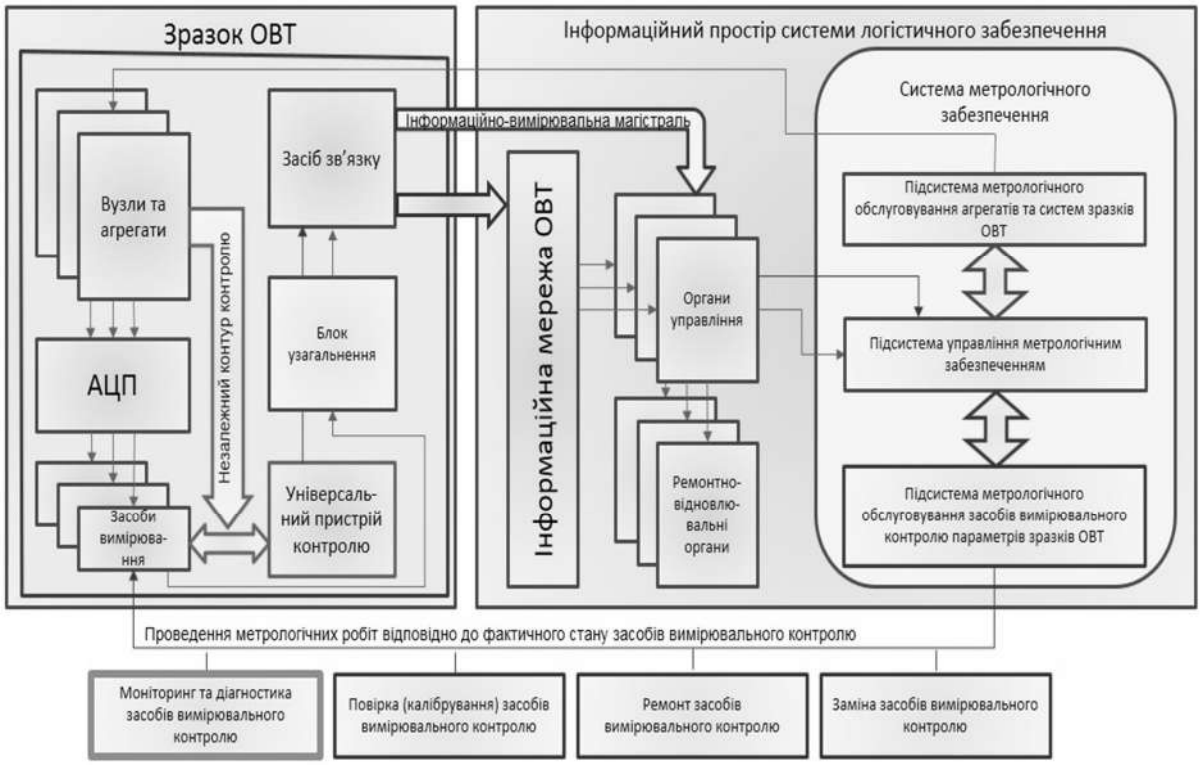


Рисунок 2 – Рекомендації щодо структури і функціонування системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків ОВТ

Застосування певних технічних рішень на зразках ОВТ для проведення моніторингу та діагностики ЗВК дасть змогу отримувати достовірну оперативну інформацію про стан засобів вимірювання та визначати вид метрологічних робіт, які необхідно провести. В свою чергу, подальше вдосконалення технічних засобів на наступних етапах реформування військової системи МлЗ, можна здійснювати за такими напрямками: укомплектовувати існуючі та перспективні зразки ОВТ незалежними засобами контролю метрологічних характеристик; поступово укомплектовувати метрологічні військові частини та підрозділи сучасним калібрувальним (повірочним) обладнанням та приладами національного та зарубіжного виробництва з підтримкою стандарту LXI (LAN eXtensions for Instruments); розробляти автоматизовані повірочні комплекси, приймати їх на озброєння і забезпечувати ними метрологічні частин, забезпечувати військові метрологічні підрозділи переносними комплексами для проведення метрологічних робіт на ЗВК параметрів зразків ОВТ.

Методи технічного діагностування забезпечують надійність функціонування технічних систем. Іншими словами діагностування – один із важливих заходів забезпечення та підтримання надійності технічних об'єктів [13].

Можливість виявлення змін технічного стану засобу вимірювального контролю на ранній стадії їх виникнення обумовлена достатньою параметричною надмірністю та процесами зниження працездатності, що повільно протікають. Наприклад, встановлено, що зниження працездатності гідросистеми літака через неполадки засобів вимірювального контролю параметрів її агрегатів в основному відбувається протягом часу, що перевищує в декілька разів тривалість одного чи декількох польотів, проте такі відмови виникають між інтервалами проведення

метрологічного обслуговування. Виключення складають руйнування шлангів та трубопроводів при екстремальних навантаженнях та відмови електрогідравлічних кранів і золотникових пристроїв в наслідок відмов електроживлення або забруднення золотників. Аналогічно відбуваються процеси зниження працездатності зразків бронетанкового озброєння та техніки, систем протиповітряної оборони, протитанкових ракетних комплексів, зенітних ракетних комплексів, радіотехнічних засобів розвідки та навігації тощо [14].

Діагностика оцінює залишкову працездатність ЗВК та параметрів агрегатів та систем зразків ОВТ в момент отримання результатів, що відображують минулі умови їх експлуатації. Моніторинг означає постійне спостереження, оцінку та прогноз їх стану, при якому діагностування ЗВК, агрегатів та систем зразків ОВТ проводиться з необхідною частотою. Водночас результати діагностування мають відображати безперервну послідовність станів ЗВК, агрегатів та систем зразків ОВТ у визначених інтервалах часу. Моніторинг забезпечує мінімальні інтервали діагностування наближені до реального часу, щоб не пропустити аварійну ситуацію, що викликана різким погіршенням стану ЗВК, агрегату чи системи не тільки в наслідок зносу, але, перш за все, через негативний вплив людського фактору. Тому стає зрозумілим, що моніторинг ЗВК параметрів критично важливих агрегатів та систем може здійснюватись тільки автоматичними системами, що повністю виключають людину-оператора з процесу постановки діагнозу, представлення й доведення його результатів до осіб, що приймають рішення.

На підставі викладеного, як відповідне технічне рішення, пропонується використання універсального пристрою контролю метрологічних характеристик на зразках ОВТ для здійснення моніторингу та діагностики ЗВК параметрів зразків ОВТ та незалежного контролю за станом агрегатів та систем зразків ОВТ, що дозволить підвищити ефективність роботи системи МлОб ЗВК параметрів зразків ОВТ. Візуалізація універсального пристрою контролю метрологічних характеристик відображена на рис. 3, у вигляді його структурної схеми [15].

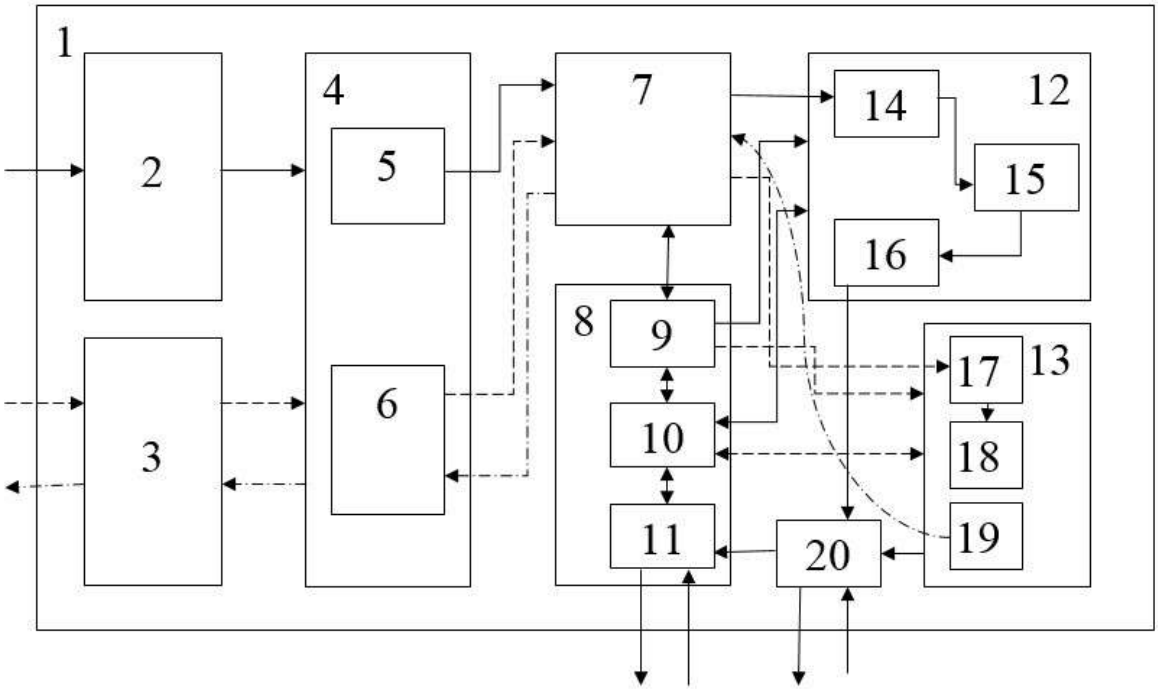


Рисунок 3 – Структурна схема універсального пристрою контролю метрологічних характеристик

Рисунок показує, що універсальний пристрій контролю метрологічних характеристик конструктивно містить: 1 – корпус, 2 – діагностичний канал, 3 – вимірювальний канал, 4 – блок комутації, 5 – модуль комутації діагностичних сигналів, 6 – модуль комутації вимірювальних та стимулюючих сигналів, 7 – блок узгодження, 8 – блок управління, 9 – модуль управління і синхронізації, 10 – модуль пам'яті з базою даних, 11 – модуль мережевих інтерфейсів, 12 – блок розпізнавання, 13 – блок вимірювання, 14 – аналізатор, 15 – модуль формування діагностичних ознак, 16 – модуль прийняття рішень, 17 – модуль обробки вимірювального сигналу, 18 – модуль порівняння, 19 – генератор стимулюючих сигналів, 20 – блок відображення та реєстрації. Цей пристрій працює у двох режимах: діагностування та вимірювання.

У режимі діагностування сигнал з датчиків зразка озброєння діагностичним каналом 2 через модуль комутації діагностичних сигналів 5, який розміщений в блоці комутації 4, потрапляє до блоку узгодження 7, де здійснюється узгодження вихідних опорів датчиків з вхідними опорами елементів пристрою. Після обробки діагностичного

сигналу в блоці узгодження 7 діагностичний сигнал потрапляє в модуль управління і синхронізації 9, який розміщений в блоці управління 8, та в аналізатор 14, який розміщений в блоці розпізнавання 12. Діагностичний сигнал з модуля управління і синхронізації 9 передається в модуль пам'яті з базою даних 10 де проводиться порівняння його характеристик з еталонними характеристиками, записаними в модуль пам'яті з базою даних 10, результати порівняння повертаються в модуль управління і синхронізації 9 та в блок розпізнавання 12. Паралельно з цим діагностичний сигнал аналізується в аналізаторі 14, визначається його тип й направляється в модуль формування діагностичних ознак 15 де формуються ознаки стану вузлів та агрегатів зразка озброєння на підставі характеристик діагностичного сигналу. Далі сигнал діагностичних ознак та оброблений сигнал з модуля пам'яті з базою даних 10 надсилаються в модуль прийняття рішень 16 де за результатами обробки інформації еталонних значень характеристик діагностичного сигналу та сформованих діагностичних ознак формується сигнал про стан вузла або агрегату зразка озброєння. Сформований сигнал стану з модуля прийняття рішень 16 надходить в блок відображення та реєстрації 20 для подальшої передачі засобами зв'язку оператору, виведення на засоби відображення інформації та реєстрації.

У режимі вимірювання сигнал із ЗВК параметрів зразків озброєння через вимірювальний канал 3 надходить в модуль комутації вимірювальних та стимулюючих сигналів 6, який розміщений в блоці комутації 4. Далі вимірювальний сигнал з модулю комутації вимірювальних та стимулюючих сигналів 6 надходить в блок узгодження 7 де здійснюється узгодження вихідних опорів ЗВК параметрів зразків озброєння з вхідними опорами елементів пристрою. Після обробки вимірювального сигналу в блоці узгодження 7 вимірювальний сигнал потрапляє в модуль управління і синхронізації 9, який розміщений в блоці управління 8, та в модуль обробки вимірювального сигналу 17, який розміщений в блоці вимірювання 13. Вимірювальний сигнал з модуля управління і синхронізації 9 передається в модуль пам'яті з базою даних 10 де проводиться ідентифікація фізичних величин вимірювального сигналу та разом з еталонними значеннями цих одиниць фізичних величин, записаними в модуль пам'яті з базою даних 10, повертаються в модуль управління і синхронізації 9 та в модуль порівняння 18, який розміщений в блоці вимірювання 13. Паралельно з цим вимірювальний сигнал обробляється у модулі обробки вимірювального сигналу 17, який розміщений в блоці вимірювання 13, де вимірюється його величина та розмірність і надсилається до модулю порівняння 18, де його значення порівнюється із еталонним значенням, яке надходить з модуля пам'яті з базою даних 10, та визначається похибка. Результати вимірювання з блоку вимірювання 13 через блок відображення та реєстрації 20 надходить в модуль мережевих інтерфейсів 11, який розміщено у блоці управління 8, звідки через засоби зв'язку надсилається оператору. З блоку оповіщення, відображення та реєстрації 20 результати вимірювання виводяться на засоби відображення та реєстрації. У випадках коли необхідно стимулювання вимірювальних сигналів у процесі визначення похибок ЗВК параметрів зразків озброєння стимулюючий сигнал з генератора стимулюючих сигналів 19, який розміщений у блоці вимірювання 13, за відповідною командою з модуля управління і синхронізації 9, що розміщений у блоці управління 8, через блок узгодження 7 та модуль комутації вимірювальних та стимулюючих сигналів 6, який знаходиться у блоці комутації 4, вимірювальним каналом 3 надсилається до відповідного ЗВК параметрів зразків озброєння, що забезпечує формування відповідного вимірювального сигналу.

Використання на зразках ОВТ описаного універсального пристрою контролю метрологічних характеристик дасть змогу вчасно виявляти відмови в роботі ЗВК параметрів зразків ОВТ, а також здійснювати незалежний контроль за станом характеристик агрегатів та систем зразків озброєння. Отримана інформація про стан ЗВК, агрегати та системи зразків ОВТ обробляється та передається засобами зв'язку в метрологічні військові частини та підрозділи, а також в органи управління метрологічним забезпеченням, де приймається рішення щодо фактичного стану засобів вимірювання та відповідних агрегатів чи систем зразка ОВТ та визначається обсяг метрологічних робіт які необхідно провести на ЗВК параметрів зразків ОВТ.

Головним завданням універсального пристрою контролю метрологічних характеристик є своєчасне виявлення відмов в роботі ЗВК параметрів зразків ОВТ, оповіщення про ці відмови фахівців метрологічних військових частин та підрозділів, а також незалежний контроль характеристик агрегатів та систем зразків ОВТ. Це в свою чергу підвищить достовірність результатів контролю параметрів зразків ОВТ, та дасть змогу запобігти передчасному виходу з ладу важливих агрегатів та систем зразків ОВТ.

Висновки й перспективи подальших досліджень

Таким чином, в статті обґрунтовані рекомендації щодо підвищення ефективності

метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки, які можна умовно розділити на дві підгрупи заходів:

організаційні, які спрямовані на удосконалення системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки через реалізацію низки заходів щодо визначення раціональної структури та порядку функціонування системи метрологічного обслуговування, удосконалення організації управління та адміністрування процесів метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки. Виконання цих заходів суттєво вплине на ефективність функціонування системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки;

технічні, які спрямовані на удосконалення парку вимірювальної техніки в ЗС України, вихідних та робочих еталонів військового призначення, застосування сучасних вимірювальних стандартів, такі як стандарт LXI, у процесі виконання вимірювань та оснащення зразків озброєння і військової техніки універсальними засобами моніторингу та діагностики метрологічних характеристик засобів вимірювального контролю параметрів зразків озброєння і військової техніки. Виконання цих заходів забезпечить якісне проведення метрологічних робіт на засобів вимірювального контролю, своєчасне виявлення прихованих відмов у роботі засобів вимірювального контролю, агрегатів та систем зразків озброєння і військової техніки та підтримання зразків озброєння і військової техніки у боєздатному стані.

Сукупно, реалізація запропонованих рекомендацій матиме позитивний вплив на ефективність системи метрологічного забезпечення в цілому. Напрямами подальших досліджень можна визначити пошук та обґрунтування альтернативних способів удосконалення системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння і військової техніки, які поряд з зазначеними рекомендаціями сприятимуть підвищенню ефективності метрологічного обслуговування.

Список бібліографічних посилань

1. Положення про метрологічну службу Міністерства оборони України та Збройних Сил України: Наказ Міністерства оборони України від 24.05.2017 № 288 (зі змінами). URL: https://zakon.rada.gov.ua/rada/show/v0288322-17#Text (дата звернення: 05.06.2023). **2. Про рішення** Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 17.09.2021 № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 05.06.2023). **3. Про рішення** Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.2021 № 121/2021. URL: http://zakon.rada.gov.ua/laws/show/121/2021#n8 (дата звернення: 05.06.2023). **4. Деякі** питання розвитку критичних технологій у сфері виробництва озброєння та військової техніки: затв. розпорядженням Кабінету Міністрів України від 30.08.2017 № 600-р (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/600-2017-%D1%80#Text (дата звернення: 06.06.2023). **5. Основні** напрями розвитку озброєння та військової техніки на довгостроковий період: Розпорядження Кабінету Міністрів України від 14.06.2017 № 398-р (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/398-2017-%D1%80#Text (дата звернення: 06.06.2023). **6. Кононов В. Б., Запека В. Ю., Ревін О. В.** Оцінювання ефективності планування метрологічного обслуговування зразків озброєння та військової техніки військових частин. *Збірник наукових праць Харківського Національного університету Повітряних Сил*, Харків: ХНУПС ім. І.Кожедуба, 2022, № 3 (73), С. 65–69. **7. Павловський О., Сова О., Коваль В.** Шляхи удосконалення системи метрологічного забезпечення в сучасних умовах розвитку Збройних Сил України. *Journal of Scientific Papers «Social Development and Security»*. 2021. Vol. 11. № 4. С. 169–176. DOI:10.33445/sds.2021.11.4.15. **8. Гудима В. П.** Фактори підвищення ефективності системи метрологічного забезпечення у сфері оборони. *Збірник наукових праць Харківського університету Повітряних Сил*. 2014. № 1 (38). С. 217–220. **9. Борисенко М. В., Герасимов С. В.** Пропозиції з удосконалення системи метрологічного забезпечення військових підрозділів в умовах реформування. *Системи озброєння та військова техніка.* 2013. № 2 (34). С. 10–14. **10. Бойко В. М., Ноженко О. М., Меркулов О. А., Герасимов С. В.** Метод визначення та коригування міжкалібрувальних інтервалів військових вихідних еталонів. *Системи озброєння та військова техніка,.* 2020. № 3 (63). С. 7-12. DOI: https://doi.org/10.30748/soivt.2020.63.01. **11. Васілевський О. М.** Методика визначення міжповірочного інтервалу засобів вимірювання на основі концепції невизначеності. *Технічна електродинаміка.* 2014. № 6. С. 81–88. **12. Дядечко А.** Методичний підхід щодо оцінювання ефективності системи метрологічного обслуговування засобів вимірювального контролю параметрів зразків озброєння та військової техніки. *Journal of Scientific Papers «Social Development and Security»*. 2021. Vol. 11. № 3. С. 179-188. DOI: 10.33445/sds.2021.11.3.17. **13. Чорний О. П., Зачепа Ю. В., Титюн В. К., Чорна О. А.** Моніторинг і діагностика електромеханічних об'єктів: навч. посіб. Кременчуг: КрНУ ім. М.Остроградського, 2019. 122 с. **14. Володарський Є. Т., Кухарук В. В., Поджаренко В. О., Сердюк Г. Б.** Метрологічне забезпечення вимірювань і контролю: навч. посіб. Вінниця: ВДТУ, 2001. 223 с. **15. Універсальний** пристрій контролю метрологічних характеристик: пат. № 150591 Україна, МПК (2021.01) G01D 3/00. № u202106161; заявл. 02.11.2021; опубл. 02.03.2022; Бюл. № 9/2022. 9 с.

RECOMMENDATIONS FOR IMPROVING THE EFFICIENCY OF METROLOGICAL MAINTENANCE OF MEASURING INSTRUMENTS FOR WEAPON AND MILITARY EQUIPMENT PARAMETERS CONTROL

***Diadechko Andrii** (PhD)* [1]
***Datsenko Ivan** (Candidate of Technical Sciences)* [2]

[1] *National Defense University of Ukraine, Kyiv, Ukraine*
[2] *Military Academy named after Yevhen Bereznyak, Kyiv, Ukraine*

The article theoretically analyzes the provisions of the governing documents and government programs regarding the improvement of the efficiency of the State Defense Forces support system, in particular the metrological maintenance system of measuring instruments for weapons and military equipment parameters control of the Armed Forces of Ukraine. An analysis of scientific publications was conducted, which investigated ways to improve the efficiency of the metrological maintenance system of measuring instruments for weapons and military equipment parameters control, and identified their main drawbacks. The article utilized methods of analysis and synthesis of complex systems, as well as the theory of diagnostics, specifically the methods of technical diagnostics of technical systems. This allowed for the substantiation of recommendations to enhance the efficiency of the metrological maintenance system of measuring instruments for weapons and military equipment parameters control. The recommendations were based on the implementation of a series of organizational and technical measures, which will improve the existing metrological maintenance system and enhance its effectiveness in functioning. It is proposed to improve metrological maintenance system of measuring instruments for weapons and military equipment parameters control by synthesizing its existing subsystems and the subsystem of measuring instruments monitoring and diagnosing, as an additional element of the metrological maintenance system of measuring instruments for weapons and military equipment parameters control. The practical significance of the article is the substantiation of recommendations regarding the use of a universal device for monitoring metrological characteristics on samples of weapons and military equipment, as a technical solution that will allow control of the condition of measuring instruments in a mode close to real time. This, in turn, will make it possible to respond in a timely manner to failures in the operation of units and systems of weapons samples and ensure their readiness to perform tasks as intended.

Key words: *metrological maintenance, measurement tools, information and measurement system, measurement information, measurement control, diagnostics.*

References

1. Regulations on the metrological service of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine: approved. by order of the Ministry of Defense of Ukraine dated May 24, 2017 No. 288 (as amended). **2. On the decision** of the National Security and Defense Council of Ukraine dated August 20, 2021 «On the Strategic Defense Bulletin of Ukraine»: Decree of the President of Ukraine dated September 17, 2021 No. 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (date of application: 06/05/2023). **3. On the decision** of the National Security and Defense Council of Ukraine dated March 25, 2021 "On the Military Security Strategy of Ukraine": Decree of the President of Ukraine dated March 25, 2021 No. 121/2021.
URL: http://zakon.rada.gov.ua/laws/show/121/2021#n8 (date of application: 06/05/2023). **4. Some issues** of the development of critical technologies in the field of production of weapons and military equipment: approved by order of the Cabinet of Ministers of Ukraine dated August 30, 2017 No. 600-r (as amended). URL: https://zakon.rada.gov.ua/laws/show/600-2017-%D1%80#Text (date of application: 06.06.2023). **5. The main directions** of the development of weapons and military equipment for the long-term period: by order of the Cabinet of Ministers of Ukraine dated 14.06.2017 No. 398-r (as amended). URL: https://zakon.rada.gov.ua/laws/show/398-2017-%D1%80#Text (date of application: 06.06.2023). **6. Kononov, V. B., Zapeka, V. Yu., Revin, O. V.,** (2022). Evaluating the effectiveness of planning metrological maintenance of samples of weapons and military equipment of military units. Collection of scientific works of the Kharkiv National University of the Air Force, Kharkiv: KhNUPS named after I. Kozhedub, 3 (73), 65-69. **7. Pavlovsky, O., Sova, O., Koval, V.,** (2021). Ways to improve the system of metrological support in modern conditions of development of the Armed Forces of Ukraine. Journal of Scientific Papers «Social Development and Security». 11, 4, 169-176. DOI: 10.33445/sds.2021.11.4.15. **8. Hudyma, V. P.,** (2014). Factors of increasing the effectiveness of the metrological support system in the field of defense. Collection of scientific papers of the Kharkiv University of the Air Force, Kharkiv: KhUPS named after I. Kozhedub. 1 (38), 217-220. **9. Borysenko, M.V., Gerasimov, S. V.,** (2013). Proposals for improving the system of metrological support of military units in the conditions of reform. Weapon systems and military equipment, Kharkiv: KhUPS. 2 (34), 10-14. **10. Boyko, V. M., Nozhenko, O. M., Merkulov, O. A., Gerasimov, S. V.,** (2020). The method of determining and adjusting the inter-calibration intervals of military output standards. Weapon systems and military equipment, Kharkiv: KhNUPS named after I. Kozhedub, 3 (63), 7-12. **11. Vasilevsky, O. M.,** (2014). Methodology for determining the inter-verification interval of measuring instruments based on the concept of uncertainty. Technical Electrodynamics, Kyiv: Institute of Electrodynamics of the National Academy of Sciences of Ukraine. 6, 81-88. **12. Diadechko, A**. (2021). A methodical approach to evaluating the effectiveness of the metrological maintenance system of measuring instruments for weapons and military equipment parameters control. Journal of Scientific Papers "Social Development and Security". 11, 3, 179-188. DOI: 10.33445/sds.2021.11.3.17. **13. Chernv, O. P., Zacheda, Y. V., Titvun, V. K., Chorna, O. A.,** (2019). Monitoring and diagnostics of electromechanical objects: training. manual Kremenchug: KrNU named after M. Ostrogradskyi, 122. **14. Volodarskyi, Y. T., Kuharuk, V. V., Podzharenko, V. O., Serdyuk, G. B.** (2001). Metrological support of measurements and control: training. manual Vinnytsia: VDTU,. 223. **15. Universal device** for monitoring metrological characteristics: pat. No. 150591 Ukraine, IPC (2021.01) G01D 3/00. No. u202106161; statement 02.11.2021; published 02.03.2022; Bul. No. 9/2022.9.

DOI:**10.33099/2311-7249/2023-47-2-75-84**

УДК 519.622

Маслюк Леонід Анатолійович *(кандидат технічних наук, старший науковий співробітник)*
Гавалко Василь Іванович *(кандидат технічних наук, доцент)*
Колодяжний Анатолій Михайлович
Джигомон Сергій Костянтинович

Національний університет оборони України, Київ, Україна

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА ОРГАНІЗАЦІЇ РОБОТИ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ ПІД ЧАС ПЛАНУВАННЯ ОПЕРАЦІЇ

Одним із ключових напрямів підвищення ефективності управління військами (силами) під час планування операції і прийняття обґрунтованих рішень на сучасному етапі ведення збройної боротьби є забезпечення спільної та синхронізованої роботи командних груп зі значною кількістю осіб в органах військового управління. У зв'язку з цим, основним завданням статті є визначення можливих підходів до підвищення ефективності роботи органів військового управління завдяки інформаційно-аналітичній підтримці організації їх роботи у процесі планування операції. Для досягнення поставленого завдання були використані методи системного аналізу, мережевого планування і управління та методи нотації з моделювання бізнес-процесів BPMN, як основні засоби опису процесів функціонування органів військового управління. Зазначений методологічний підхід дає змогу більш детально розкрити і проаналізувати процес організації роботи в органах військового управління, визначити основні проблемні питання та можливі шляхи їх вирішення. У статті запропоновано підходи до оптимізації роботи органів військового управління у процесі планування операції на основі завчасно підготовлених типових планів і форм документів, обґрунтовано функції інформаційно-аналітичної підтримки процесу організації роботи, запропоновано склад програмних засобів й розроблено узагальнений порядок їх функціонування, формалізовано модель типового плану та плану підготовки операції у вигляді ієрархічних структур діаграм процесів на основі сформульованих основних визначень її елементів, запропоновано підхід щодо використання зазначеної моделі для організації оперативного контролю виконання заходів (завдань) плану. Елементи наукової новизни полягають в уточненні та конкретизації відомої нотації моделювання процесів BPMN і поширення її застосування на інформаційні об'єкти у сфері організації роботи органів військового управління, що забезпечує можливості розробки моделей процесів у цій сфері, проведення моделювання і більш глибокого їх дослідження. Отримані результати є подальшим удосконаленням методичних підходів до розробки програмного забезпечення інформаційно-аналітичної підтримки організації роботи органів військового управління. Сьогодні, інформаційно-аналітична підтримка організації роботи органів військового управління під час планування операції у Збройних силах України здійснюється з використанням програмного забезпечення зі складу Microsoft Office або окремих застосувань з низьким рівнем функціональності, що не забезпечує високоефективної підтримки роботи службових осіб, обмежує можливості з автоматизації функцій управління і, головне, не дозволяє реалізувати системні підходи у процесі створення автоматизованих систем управління військами. Вищеозначене підкреслює актуальність теми статті.

Ключові слова *підготовка операції, планування операції, процес прийняття військового рішення, організація роботи органів військового управління.*

Вступ

Постановка проблеми. Досвід ведення бойових дій в умовах повномасштабної агресії російської федерації проти України свідчить про: високу динаміку сучасних операцій, зміни у формах і способах ведення бойових дій, використання методів ведення гібридної війни, суттєвий рівень невизначеності ситуації, ведення збройної боротьби в густонаселених районах та вчинення противником терористичних актів, а також перенесення акцентів у інформаційний простір.

Усе це суттєво впливає на процеси підготовки операцій та їх планування. Збільшується кількість факторів, які потрібно враховувати під час підготовки операції і прийняття обґрунтованих рішень, розширюється спектр заходів, що необхідно провести для якісної підготовки військ (сил) та органів управління, скорочуються терміни

підготовки, особливо в екстремальних умовах під час ведення бойових дій, застосовуються різні методи роботи командувача і органу військового управління та їх комбінування.

Характерною особливістю підготовки і планування операції у Збройних Силах України (далі – ЗС України) в сучасних умовах є залучення до проведення операцій сил і засобів усіх силових структур держави. Крім того, ЗС України постійно отримують на озброєння сучасні системи управління зброєю та новітні зразки озброєння і військової техніки країн НАТО та інших розвинутих у військовій сфері країн світу. Це обумовлює необхідність залучення до планування і підготовки операції великої кількості службових осіб органів військового управління (далі – ОВУ), виконання додаткової специфічної сукупності заходів з метою врахування нових можливостей військ (сил) і озброєння та забезпечення відповідної якісної логістики.

У таких умовах якісне і своєчасне виконання завдань з планування і підготовки операції суттєво залежить від чіткої організації роботи службових осіб в усіх задіяних ланках управління, частинах, підрозділах, службах. У свою чергу, однією з основних умов ефективного виконання є наявність відповідних засобів автоматизації та високоефективної інформаційно-аналітичної підтримки у складі автоматизованих систем управління військами. Реалізація таких підходів забезпечить злагоджену й ефективну роботу командувача (командира), ОВУ й усіх підпорядкованих частин і підрозділів в єдиному інформаційному середовищі для досягнення поставленої мети, автоматизацію процесів підготовки, постановки й доведення завдань до виконавців, контролю їх виконання, проведення відповідних розрахунків і формування документів.

Враховуючи відсутність, на цей час, у ЗС України таких засобів автоматизації, необхідність суттєвого підвищення ефективності управління силами та засобами на сучасному етапі ведення збройної боротьби, дослідження й вироблення рекомендацій у цій галузі є актуальним науковим завданням.

Аналіз останніх досліджень і публікацій. Дослідження з питань проблемної тематики у ЗС України проводились під час:

командно-штабних навчань у Національному університеті оборони України в період з 2018 р. по 2021 р.;

опитування слухачів університету на навчальних заняттях;

виконання оперативних завдань щодо підготовки оперативного складу штабів з'єднань і частин;

прийняття участі науково-педагогічного складу університету у заходах оперативної підготовки ОВУ;

участі в роботі комісій з приймання етапів виконання дослідно-конструкторської роботи (далі – ДКР) із розроблення автоматизованої системи управління військами (далі – АСУВ) для ЗС України.

В результаті проведених досліджень було встановлено, що, в нинішніх умовах, в органах управління ЗС України різних рівнів під час підготовки і планування операцій використовується, зазвичай, програми офісного пакету Microsoft або окремих програмних застосувань з низьким рівнем функціональності. Використання такого підходу не забезпечує ефективної інформаційно-аналітичної підтримки усіх процесів управління під час планування операції і вирішення існуючої проблеми на системному рівні. Водночас робота виконується різними службовими особами практично вручну, багато часу витрачається на проведення розрахунку часу, формування документів з організації роботи ОВУ, автоматизований обмін потрібною інформацією й доведення завдань до виконавців не передбачається, не забезпечується контроль виконання поставлених завдань і, як результат, низький рівень оперативності роботи ОВУ.

У збройних силах країн НАТО, питанням організації роботи ОВУ під час планування воєнної операції, надається особлива увага. У їхніх доктринальних положеннях розглядаються дві основні категорії планування: завчасне планування і планування у відповідь (з реагування) на кризові ситуації (кризове планування) [1, 3, 4]. За завчасного планування передбачається розроблення, так званих, типових планів, у яких чітко розкривається потрібний перелік заходів і завдань, що необхідно виконати за настання тієї чи іншої ситуації (потенційно можливої кризи). У подальшому, за потреби підготовки конкретної операції (настанні конкретної кризи), типові плани використовуються як основа для організації роботи ОВУ під час її підготовки і планування. У вибраний за основу типовий план вносяться доповнення і корективи відповідно до поставленої мети операції, конкретних умов обстановки, часових обмежень і визначеного методу роботи службових осіб ОВУ. Реалізація такого підходу сприяє підвищенню обізнаності командувача (командира) й начальника штабу, можливості врахування специфіки ситуації, що у значній мірі спрощує процес організації роботи й підвищує оперативність під час розроблення реального плану операції.

Організація роботи ОВУ під час підготовки і планування операції за стандартами НАТО детально розкривається у розроблених для різних рівнів ОВУ так званих процесах прийняття військового рішення (далі – ППВР) [2]. Такий процес розглядається військовими фахівцями НАТО як модель планування, що встановлює процедури аналізу завдання, розроблення, аналіз та порівняння варіантів дій за визначеними

критеріями, вибір оптимального варіанту дій та розроблення плану операції або наказу. Стандартизовані процеси, розкриті у ППВР для усіх етапів планування, допомагають командирам і штабам візуалізувати хід підготовки операції, застосовуються у всьому спектрі конфліктів і низки військових операцій. Командири і ОВУ використовують ППВР для організації своїх планових заходів, спільного розуміння завдання, наміру командира та розроблення ефективних планів і розпоряджень.

Одним із можливих напрямків досягнення високого рівня ефективності інформаційно-аналітичної підтримки при організації роботи ОВУ можна досягти шляхом реалізації у програмному забезпеченні методів моделювання бізнес-процесів. Такі підходи на даний час широко застосовуються у різних сферах діяльності для детального опису процесів, проведення досліджень, оптимізації і вдосконалення діяльності організацій і установ шляхом усунення вузьких місць, дублювання функцій тощо.

Найбільш розповсюдженими способами опису бізнес-процесів є текстовий, табличний та графічний. Текстовий та табличний способи забезпечують достатньо повний опис бізнес-процесу, однак є складними для аналізу, незручними в користуванні при наявності великих розгалужень або ієрархічних структур у процесі тощо. До того ж їх практично неможливо використовувати для моделювання. Тому, на цей час сформувалися і використовуються декілька стандартів з графічним описом бізнес-процесів. Найпоширенішими серед них є мови (нотації) графічного моделювання бізнес-процесів: Подієвий ланцюжок процесів (Event-Driven Process Chain (EPC)), Уніфікована мова моделювання (Unified Modeling Language (UML)), Методологія функціонального моделювання і графічного опису процесів (I-CAM DEFinition або Integrated DEFinition «об'єднане визначення» (IDEF)), Нотація и модель бізнес-процесів (The Business Process Modeling Notation (BPMN)) й інші та їх подальші модифікації [5–8].

Як відзначають багато фахівців [7], діаграми IDEF і EPC дозволяють описувати бізнес-процеси, однак мають низький рівень виразності, точності та однозначності, що не дозволяє створювати об'єктивні моделі процесів діяльності, або спонукає розроблювачів створювати додаткові методи для забезпечення необхідної функціональності (забезпечення відображення часової послідовності виконання завдань, опису процесу із застосуванням ієрархічних структур тощо).

Нотація UML (як і багато інших бізнес-нотацій XML-мов) [7, 8] мають велику надмірність та абстрактне представлення опису, складні при вивченні і впровадженні, тому використовуються в основному вузькопрофільними спеціалістами для системного аналізу та проєктування, і дуже рідко для моделювати бізнес-процесів.

Найбільш доцільною для використання в програмному забезпеченні організації роботи (далі – ПЗ ОР) є нотація з моделювання бізнес-процесів BPMN, що на цей час у багатьох відносинах перевершує практично всі традиційні нотації, є стандартом і специфікацією для моделювання бізнес-процесів і мережевих послуг [5, 6]. Нотація BPMN описує умовні позначення для відображення бізнес-процесів у вигляді діаграм. BPMN орієнтована як на розробників, так і на користувачів й керівників. Отже, BPMN покликана служити сполучною ланкою між фазою дизайну бізнес-процесу і фазою його реалізації. Для цього мова використовує базовий набір інтуїтивно зрозумілих елементів, які дають змогу визначати складні семантичні конструкції, і у поєднанні з графічним редактором забезпечує зручність й оперативність побудови діаграм планів і візуалізацію процесів їх виконання у наглядній формі.

Метою статті є визначення можливих напрямів та розроблення рекомендацій щодо створення й реалізації програмного забезпечення у складі автоматизованої системи управління військами для забезпечення високоефективної інформаційно-аналітичної підтримки організації роботи органів військового управління під час планування операції з урахуванням досвіду збройних сил НАТО.

Виклад основного матеріалу дослідження

Планування операції (бою) – найважливіша складова її (його) підготовки, що полягає у детальній розробці змісту та послідовності виконання військами (силами) бойових завдань, розподілу їх зусиль за напрямами дій, взаємодії, всебічного забезпечення та управління. Весь комплекс запланованих заходів спрямований на забезпечення досягнення мети операції. Планування операції може здійснюватися як завчасно, так і під час ведення бойових дій. Разом із цим, робота командувача і органу військового управління залежить від умов оперативно-тактичної обстановки, отриманого завдання і наявності часу. В процесі планування задіяні усі службові особи органу військового управління та підпорядковані війська, комплекс заходів охоплює широкий спектр питань, які необхідно вирішити для прийняття обґрунтованих рішень та розроблення ефективних планів застосування військ (сил). Успішне вирішення завдань планування залежить від організації роботи органу військового управління на цьому етапі, що передбачає, в першу чергу, забезпечення спільного розуміння завдання та налагодження узгодженої спільної роботи усіх структурних підрозділів (секцій) і службових осіб, чітке визначення переліку завдань усім службовим особам, проведення розрахунків щодо визначення часових

значень показників виконання заходів, формування документів з організації роботи, своєчасне доведення завдань до виконавців і контролювання їх виконання.

У зв'язку з цим, ПЗ ОР ОВУ, що здійснює інформаційно-аналітичну підтримку роботи ОВУ під час планування операції, розглядається як важлива складова перспективної АСУВ. З урахуванням підходів, висвітлених у керівних документах армій країн НАТО, в основу побудови ПЗ ОР закладається ідеологія завчасної підготовки типових планів для різних умов підготовки операції, часових обмежень і методів роботи ОВУ, а також шаблонів і форм основних документів щодо організації роботи командувача та ОВУ, а під час підготовки конкретної операції на їх основі – розроблення реальних планів її підготовки, проведення потрібних розрахунків та формування проєктів електронних документів.

Інформаційно-аналітична підтримка організації роботи ОВУ має забезпечити автоматизацію виконання таких основних функцій:

завчасне формування функціональної структури ОВУ, розподіл службових осіб за пунктами управління (секціями, групами, службами) та визначення їх повноважень щодо доступу до даних;

завчасне розроблення типових планів підготовки операції у вигляді деталізованого переліку заходів (завдань) службовим особам ОВУ із встановленням орієнтовного дольового розподілу часу на виконання заходів;

завчасне формування шаблонів і форм електронних документів;

розроблення плану підготовки операції на основі даних вибраного типового плану;

проведення розрахунку значень часових показників заходів;

доведення визначених завдань до виконавців;

затвердження плану підготовки операції, запуск процесу його виконання, відображення стану його виконання у вигляді діаграм процесів та станів виконання заходів;

контроль виконання заходів (завдань) службовими особами ОВУ;

формування та корегування проєктів основних електронних документів.

Для автоматизації перелічених функцій у ПЗ ОР пропонується використання наступних видів структур даних.

Типовий план, план підготовки операції – це розроблена командувачем (начальником штабу) та упорядкована за часом, метою, місцем та виконавцями сукупність взаємопов'язаних заходів (завдань), яка визначає порядок дій службових осіб ОВУ під час підготовки операції в певних умовах.

Типові плани розробляються завчасно для різних видів операцій й різних умов їх підготовки. За безпосередньої підготовки операції такі плани використовуються як шаблони для розроблення реальних планів, що суттєво скорочує час на формування відповідних документів й постановку реальних завдань.

Типовий план і план підготовки операції є ієрархічними структурами, які на верхніх рівнях доцільно представити двома загальними процесами:

«Процес оперативного планування», що деталізується на етапи, які, в свою чергу, – на завдання керівникам функціональних підрозділів або окремим службовим особам;

«Процес за напрямами підготовки операції», що деталізується на окремі напрями підготовки (військ, району операції, системи управління, логістики тощо). Окремі напрями підготовки містять завдання керівникам функціональних підрозділів (секцій) або окремим службовим особам.

Верхні рівні планів визначають порядок роботи в цілому, тому власником даних цієї частини ієрархічної структури завжди є командувач, при цьому модифікація цих даних можлива тільки ним особисто, або іншою службовою особою від імені командувача з відповідними правами. Кожна службова особа є відповідальним виконавцем усіх завдань, отриманих від командувача, і може у подальшому їх деталізувати для визначення завдань своїм підлеглим, поглиблюючи ієрархічну структуру планів.

Місце завдання в ієрархічній структурі визначає такі поняття, як старше завдання і підпорядковане завдання. Усі завдання типового плану не мають конкретних значень часових показників, а лише орієнтовну тривалість виконання у відсотках.

План підготовки операції створюється на основі підготовленого й обраного командувачем типового плану, який найбільшою мірою відповідає виду операції, умовам її підготовки й визначеному методу роботи службових осіб ОВУ. У плані підготовки операції перелік заходів (завдань) може уточнюватися і для них розраховуються значення часових показників на основі поставлених завдань щодо підготовки конкретної операції і дольового розподілу часу на виконання завдань у вибраному типовому плані. Значення часових показників певних завдань у плані можуть бути зафіксованими і в процесі перерахунку часу змінюватися не будуть.

Для визначення чіткої послідовності виконання завдань кожний рівень підпорядкованих завдань у складі старшого завдання представляється у вигляді діаграми.

Діаграма – це графічна візуалізація сукупності завдань, елементів управління, подій, повідомлень, документів та зв'язків між ними, які визначають послідовність, умови і результати виконання завдань. Усі елементи діаграми, що визначені як завдання, містять такі основні дані: назву завдання, дані щодо власника завдання та відповідального виконавця, значення часових показників (дата та час початку і завершення або відсотки), стан виконання.

Приклад діаграми, яка деталізує 1-й етап «Отримання завдання» заходу «Процес оперативного планування», наведений на рис. 1.

Процес – це відображення роботи командувача і ОВУ відповідно до розробленого й затвердженого плану підготовки операції, або – відображення елементів плану в динаміці виконання запланованих завдань. Для візуалізації процесу також застосовується ієрархічна структура даних й діаграм.

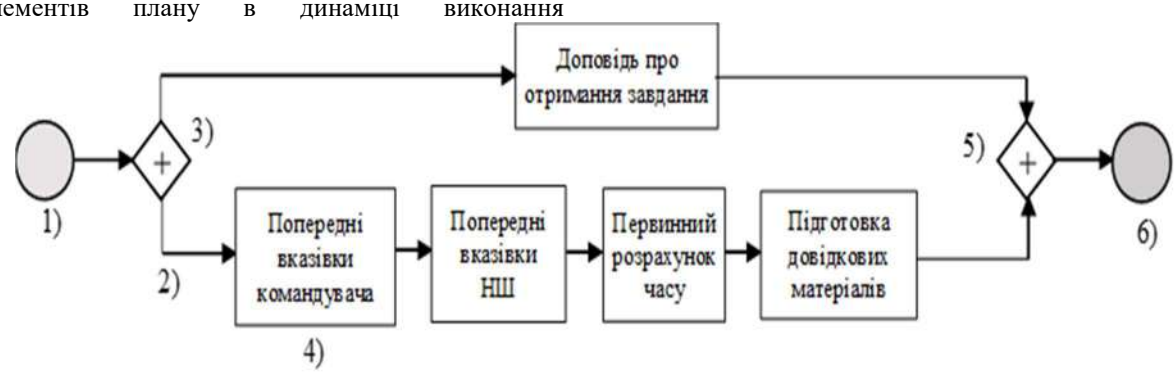


Рисунок 1 – Приклад діаграми виконання заходу «Отримання завдання»:
1, 6 – відповідно стартова та завершальна події; 2 – зв'язки; 3, 5 – відповідно розгалужувач та з'єднувач потоків управління, 4 – завдання.

Узагальнений порядок функціонування програмного забезпечення для реалізації запропонованих підходів можна представити так:

1. Отримання з бази даних АСУВ списку користувачів, допущених до роботи з системою.
2. Формування функціональної структури ОВУ і посад.
3. Розподіл користувачів за посадами у функціональній структурі.
4. Створення груп користувачів, надання користувачам прав доступу та модифікації даних.
5. Розроблення типових планів для різних видів операцій й різних умов їх підготовки.
6. Формування шаблонів і форм документів «Розрахунок часу на підготовку операції», «Календарний план підготовки операції» та «План-графік роботи командувача і штабу».
7. Формування плану підготовки операції на основі вибраного типового плану, проведення попереднього розрахунку значень часових показників плану.
8. Коригування та проведення розрахунку значень часових показників плану, затвердження плану підготовки операції,.
9. Формування на основі підготовленого шаблону проекту документа «Розрахунок часу на підготовку операції».
10. Формування на основі підготовленого шаблону проекту документа «Календарний план підготовки операції».
11. Формування проекту документа «План-графік роботи командувача і штабу».
12. Завантаження плану підготовки операції на виконання.
13. Управління станом виконання завдань та контроль їх виконання.

Кожний створений інформаційний об'єкт зберігається у базі даних ПЗ ОР. Автоматизація визначених функцій під час організування роботи ОВУ й реалізація запропонованого порядку може бути забезпечена таким складом функціональних модулів програмного забезпечення (рис. 2).

Модуль «*Персонал*» призначений для ведення реєстру користувачів і управління їхнім доступом до даних. Модуль має забезпечувати виконання таких функцій: формування списку користувачів на основі даних бази даних (далі – БД) АСУВ; формування груп користувачів; визначення повноважень для кожного користувача в групі стосовно доступу до даних.

Модуль «*Функціональна структура ОВУ*» забезпечує: формування ієрархічної функціональної структури ОВУ; формування переліку посад у структурах; розподіл користувачів за пунктами управління та посадами.

Сформовані дані у модулях «Персонал» та «Функціональна структура ОВУ» зберігаються у БД ПЗ ОР. У подальшому вони використовуються іншими модулями для формування діаграм, шаблонів і проєктів документів.

Модуль «*Діаграми*» призначений для побудови моделей процесів підготовки операції і має забезпечувати виконання таких функцій: створення моделей процесів роботи (діаграм) ОВУ як типових планів або планів підготовки конкретних операцій; редагування діаграм, зміна їх складу, додавання, видалення та редагування елементів діаграм, зміна зв'язків між елементами; перевірка діаграм та їх елементів на предмет коректності даних (коректності значень часових показників, постановників та виконавців завдань, наявності обов'язкових зв'язків між елементами тощо); зміна стану моделей процесів та окремих завдань (зі стану «Проєкт» в стан «Затверджено»).

Для забезпечення сприйняття типових планів і планів підготовки операцій службовими особами ОВУ як цілісних ієрархічних структур й з повною деталізацією на кожному рівні ієрархії та забезпечення зручності роботи з такими структурами даних модуль «Діаграми» доцільно

реалізувати у вигляді двох взаємопов'язаних компонент: «Плани» та «Редактор діаграм».

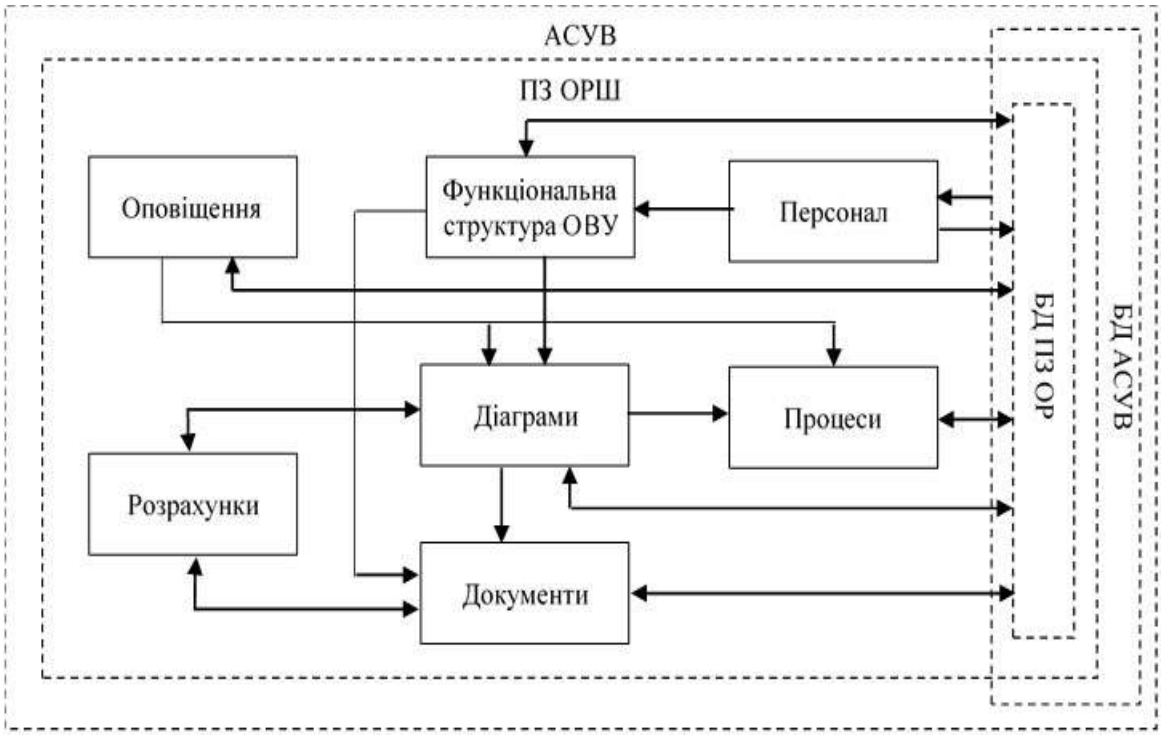


Рисунок 2 – Склад функціональних модулів програмного забезпечення організації роботи ПЗ ОР

У компоненті «Плани» забезпечується візуалізація типових планів або планів підготовки операцій у вигляді ієрархічних структур завдань з наведенням для кожного з них відповідних основних даних та забезпечується виконання усіх процедур роботи як із звичайними ієрархічними структурами. При створенні нового типового плану доцільно організувати автоматичну його деталізацію двома загальними процесами: «Процес оперативного планування» та «Процес за напрямами підготовки операції», що виконуються паралельно. При створенні нового плану підготовки операції у компоненті необхідно забезпечити можливість вибору типового плану як шаблону. В обох випадках передбачається можливість введення вихідних даних (назви, значень часових показників, виконавців тощо). Виділений у компоненті «Плани» елемент ієрархічної структури (захід, завдання) автоматично представляється для деталізації в компоненті «Редактор діаграм». В останній необхідно забезпечити можливість оперативної побудови діаграми процесу на визначеному рівні ієрархії (для отриманого заходу, завдання) і можливість введення усіх основних даних для завдань діаграми. Після успішної перевірки цілісності діаграми і збереження у БД даних за модифікований таким чином план, здійснюється автоматична деталізація отриманого завдання вкладеними, що визначені у діаграмі, й оновлення даних у компоненті «Плани». Якщо виділене у компоненті «Плани» завдання уже деталізоване, у компоненті «Редактор діаграм» здійснюється автоматична візуалізація його діаграми процесу і забезпечується можливість її редагування. При формуванні нового плану підготовки операції за вибраним типовим планом усі діаграми процесів останнього копіюються у створюваний план.

Модуль «*Процеси*» призначений для виконання моделей процесів. У модулі використовуються дані щодо планів підготовки операції, сформовані у модулі «Діаграми» й збережені у БД ПЗ ОР. Використання можливе тільки за умов затверджених планів підготовки операції.

Модуль «Процеси» підтримує реалізацію планів роботи і має забезпечувати виконання наступних функцій: візуалізація моделі процесу; запуск та зупинка процесу; скасування процесу в цілому або окремих його завдань; виконання окремих завдань на діаграмі процесу відповідно до команд користувача; активація окремих елементів діаграми процесу відповідно до просування потоків управління; автоматичне виконання умов, що присутні на діаграмі та не потребують втручання користувача (наприклад, старт та завершення діаграми, розгалуження або з'єднання потоків управління); формування оповіщень користувачів ПЗ ОР про зміни під час виконання процесів.

Модулі «Діаграми» й «Процеси» є основними складовими ПЗ ОР. Їх доцільно реалізувати з використанням нотації BPMN, що дасть змогу провести якісне та детальне моделювання процесів, що відбуваються під час роботи штабу при плануванні операцій та може забезпечити

ефективне виконання організаційних заходів. Реалізація такого підходу забезпечить злагоджену й ефективну роботу командувача (командира), штабу й усіх підпорядкованих частин і підрозділів, автоматизацію процесів підготовки, постановки й доведення завдань до виконавців, контролю їх виконання, проведення відповідних розрахунків і формування документів.

Будь-які зміни в діаграмах, що відбуваються під час завчасного або безпосереднього планування, а також в моделях процесів в ході виконання запланованих завдань (заходів), фіксуються як події і зберігаються у базі даних. Відомості про такі події автоматично обробляються в модулі «Оповіщення» та потім надсилаються на робочі місця службових осіб для оновлення даних.

Модуль «Документи» призначений для формування проєктів звітних електронних документів: «Розрахунок часу на підготовку операції», «План-графік роботи командувача (командира) і штабу» та «Календарний план підготовки операції». Цей модуль має забезпечувати виконання таких функцій: побудова шаблонів і форм документів, їх збереження, модифікація, видалення; надання переліку доступних шаблонів для вибору користувачем під час формування документа; вибір відповідних вихідних даних для заповнення шаблону; формування, корегування змісту та відображення документа, його збереження і друк. Під час формування шаблонів і документів у модулі слід передбачити також можливість внесення змін до форм їх подання відповідно змін у керівних документах.

Структуру модуля «Документи» доцільно реалізувати відповідно до типу і форми розроблюваних документів. Під час формування документів «Розрахунок часу на підготовку операції» й «Календарний план підготовки операції» через однотипність їх основних частин можна застосувати одну і ту саму структуру (рис. 3) і порядок роботи за таких умов однаковий. Виключення складає тільки відсутність у структурі документа «Календарний план підготовки операції» змістовної частини «Вихідні дані», через що при формуванні цього документа відповідна компонента модуля не використовується і не візуалізується.

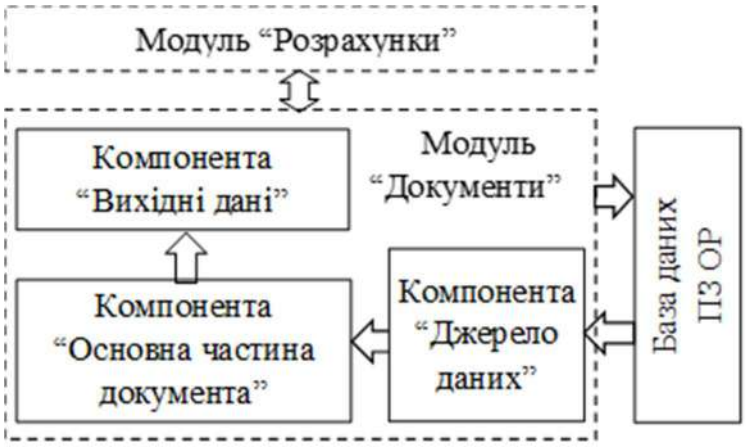


Рисунок 3 – Структура модуля «Документи» у процесі формування документів «Розрахунок часу на підготовку операції» й «Календарний план підготовки операції»

Усі компоненти модуля забезпечують візуалізацію ієрархічних структур даних за аналогією з компонентою «Плани» модуля «Діаграми» й можливість виділення окремих елементів структур для їх копіювання або видалення. У компоненті «Вихідні дані» для кожного завдання слід забезпечити можливість візуалізації додаткових часових показників (за визначенням службової особи): наявність часу на виконання завдання, у тому числі світлого та темного.

Роботу в модулі під час формування вказаних документів слід організувати у два етапи: формування шаблону документа і формування проєкту електронного документа. У процесі формування шаблону документа у компоненту «Джерело даних» із БД ПЗ ОР завантажується вибраний типовий план, зі складу якого необхідні у документі завдання (заходи) виділяються і переносяться у компоненту «Основна частина документа». За аналогією, з останнього завдання переносяться у компоненту «Вихідні дані», але, водночас, для кожного з них визначається, які його дані необхідно виводити на відображення. Після виконання зазначених дій шаблон документа готовий і зберігається у БД ПЗ ОР. Під час формування проєкту електронного документа із БД ПЗ ОР спочатку завантажується вибраний шаблон документа, потім у компоненту «Джерело даних» завантажується план підготовки операції, здійснюється автоматичне співставлення усіх елементів шаблону і плану й оновлюються часові показники завдань. У процесі формування документа «Розрахунок часу на підготовку операції» усі завдання компоненти «Вихідні дані», для яких визначаються додаткові часові показники,

віддаються у модуль «Розрахунки», і після проведення розрахунків оновлюються дані цієї компоненти. Проєкт електронного документа готовий і може бути збереженим й виведеним у текстовий редактор.

Під час формування документа «План-графік роботи командувача (командира) і штабу» структуру модуля «Документи» доцільно реалізувати на базі графічного редактора. Слід передбачити можливість формування усіх форм графічних елементів, визначених керівними документами, прив'язку графічних елементів завдань до часової осі та їх масштабування. Шаблон цього документа формувати недоцільно, тому що у документі використовуються реальні часові показники завдань. Формування документа здійснюється на основі даних БД ПЗ ОР щодо функціональної структури ОВУ та даних плану підготовки операції.

Модуль «*Розрахунки*» призначений для проведення розрахунків значень часових показників планів роботи і документів. Цей модуль має забезпечувати виконання таких функцій: розрахунок розподілу часового ресурсу у відсотках між елементами типового процесу згідно з вимогами керівних документів та початкових даних, встановлених користувачем; розрахунок значень часових показників плану роботи згідно розподілу за типовим планом та вихідних даних, встановлених користувачем; перерахунок окремих частин плану, або плану загалом у разі внесення змін користувачем, корегування змісту та порядку виконання завдань в плані; виконання перевірки коректності розподілу часового ресурсу між елементами типового процесу; перевірка коректності розрахунку значень часових показників плану; розрахунок ресурсу часу на виконання визначених завдань, у зокрема світлого та темного часу. Основою математичного забезпечення модуля «Розрахунки» можуть бути методи мережевого планування і управління. Водночас необхідно удосконалити алгоритм розрахунку часових показників мережевого графіка, який забезпечуватиме можливість проведення розрахунків з урахуванням ієрархічної структури завдань планів, перерахунок відсотків часу в завданнях типового плану в реальні часові показники планів підготовки операції, а також урахування зафіксованих користувачем значень часових показників певних завдань. Під час проведення розрахунків удосконалений алгоритм має забезпечувати перевірку коректності часових показників плану. Для забезпечення розрахунків наявності ресурсу часу (світлого та темного) на виконання визначених завдань інформаційне забезпечення ПЗ ОР має містити дані щодо тривалості світлового дня від сходу Сонця до його заходу за різними порами року (місяцями – залежно від необхідної точності результатів) й різними регіонами, де планується підготовка операцій. Розробка такого удосконаленого алгоритму є окремим науковим завданням та предметом подальших наукових досліджень.

Слід відмітити, що процес проведення розрахунків часових значень показників завдань плану здійснюється в автоматичному режимі і буде займати незначний проміжок часу. Тому доцільно підготовлювати шаблони і форми документів «Розрахунок часу на підготовку операції» з повним переліком заходів і завдань плану. Цей документ може повноцінно замінити документ «Календарний план підготовки операції». Таким чином можна скоротити кількість документів з організації роботи в органах військового управління.

Спеціальне програмне забезпечення інформаційно-аналітичної підтримки організації роботи органів військового управління під час підготовки і планування операції, реалізоване за такими підходами, дає змогу досягти таких результатів: формування структур даних відповідно до вимог керівних документів, у тому числі з урахуванням стандартів НАТО; оперативне внесення змін до структури шаблонів і форм документів відповідно до змін вимог керівних документів без внесення змін до програмного забезпечення; автоматизація практично усіх вищенаведених функцій управління; забезпечення можливості оперативної підготовки нових типових планів й шаблонів документів на основі створених; суттєве підвищення оперативності розроблення плану операції завдяки використанню завчасно підготовлених типових планів і проведенню розрахунків значень часових показників завдань плану за лічені секунди; досягнення високого рівня оперативності підготовки проєктів електронних документів після розроблення плану операції; забезпечення простоти та зручності використання програмного забезпечення, наочності процесу виконання плану в динаміці й простоту контролю виконання завдань службовими особами ОВУ.

Висновки й перспективи подальших досліджень

Проведений у статті аналіз стану розробки й впровадження програмного забезпечення для інформаційно-аналітичної підтримки організації роботи органів військового управління в Збройних силах України під час підготовки і планування операції, аналіз вимог керівних документів країн-членів НАТО щодо організації роботи на цьому етапі та застосовані методи проведення досліджень дозволили сформулювати такі висновки і пропозиції.

Рівень автоматизації процесів щодо організації роботи органів військового управління під час підготовки і планування операції у Збройних силах України залишається вкрай низьким. Тому вирішення наукових та організаційних проблемних питань щодо створення відповідного програмного забезпечення є надзвичайно актуальним завданням.

Для забезпечення спільного розуміння завдання та налагодження сумісної, злагодженої і одночасної роботи великих колективів органів військового управління під час планування операції і прийняття обґрунтованих рішень, оперативного обміну інформацією та доведення завдань програмне забезпечення організації роботи доцільно реалізувати як окрему важливу складову автоматизованої системи управління військами.

Для суттєвого підвищення рівня оперативності роботи органів військового управління під час планування операції у процесі розробки програмного забезпечення організації роботи доцільно реалізувати запропоновані у статті оптимізаційні підходи до їхньої діяльності на основі завчасно підготовлених типових планів та форм документів.

Обґрунтовані у статті функції інформаційно-аналітичної підтримки процесу організації роботи і узагальнений порядок функціонування програмного забезпечення організації роботи, відповідають доктринальним документам з організації роботи органів військового управління країн-членів НАТО, запропонований склад програмного забезпечення, підходи та методи програмної реалізації його окремих функціональних модулів можуть бути використаними під час побудови перспективної автоматизованої системи управління військами.

Типові плани і плани підготовки операції доцільно подавати у вигляді ієрархічних структур діаграм процесів, що забезпечує як цілісне, так і детальне подання процесу підготовки операції, оперативність проведення розрахунків, формування документів з організації роботи органів військового управління та організацію оперативного контролю виконання заходів (завдань) плану підготовки операції.

Обґрунтовані у статті підходи і методи, що доцільно використовувати у процесі програмної реалізації програмного забезпечення організації роботи, є подальшим удосконаленням методичних підходів до розробки програмного забезпечення інформаційно-аналітичної підтримки організації роботи органів військового управління.

Перспективними напрямами подальших досліджень можуть бути розширення функціональності програмного забезпечення організації роботи завдяки розробленню та впровадженню методів і алгоритмів, що забезпечують:

автоматичний розрахунок часових показників заходів (завдань) плану підготовки операції з урахуванням специфіки структури плану і певних часових обмежень;

узгодження в автоматичному режимі часових показників заходів і завдань планів підготовки операції на усіх рівнях управління;

можливість розробки більш широкого набору форм документів з організації роботи органів військового управління під час підготовки операції і надання їх службовим особам у процесі виконання завдань щодо розробки відповідних проєктів електронних документів.

можливість відстеження в автоматичному режимі процесу виконання завдань у підпорядкованих органах управління та інформування вищих штабів про реалізацію своїх планів підготовки операції.

Список бібліографічних посилань

1. Стандарт НАТО AJP-5: Доктрина об'єднаних сил НАТО щодо планування операцій. Київ : НУОУ, 2019. 141 с. **2. Методичні** рекомендації з планування та організації бою за стандартами НАТО (штаб бригади (батальйону) та їм рівних). URL: https://jurkniga.ua/contents/ metodichni-rekomendatsii-z-planuvannya-ta-organizatsii-boyu-za-standartami-nato-shtab-brigadi-batalyonu-ta-im-rivnikh.pdf (дата звернення 20.05.2023). **3. Порядок** оперативного планування в органах військового управління НАТО: навч. посіб. / [А. М. Сиротенко, В. М. Тарасов, С. М. Салкуцан та ін.]. Київ: НУОУ, 2019. 232 с. **4. Процедури** процесу прийняття військового рішення (за стандартами НАТО): навч. посіб. / Музиченко Д.П., Філюнкин Є.В. та ін. Київ : НУОУ, 2018. 140 с. **5. Система** для моделирования процессов в нотации BPMN. URL: https://www.terrasoft.ua/page/ru/bpmn (дата звернення 22.05.2023). **6. BPMN** – Википедия. URL: https://uk.wikipedia.org/wiki/BPMN (дата звернення 22.05.2023). **7. Особливості** опису бізнес-процесів в сучасних IT-системах. URL: http://www.economy.nayka.com.ua/?op=1&z=3514 (дата звернення 22.05.2023). **8. Методи** опису бізнес-процесів. URL: https://manageable.com.ua/ metody-opysu-biznes-protsesiv/ (дата звернення 22.05.2023).

INFORMATION AND ANALYTICAL SUPPORT FOR THE ORGANIZATION OF THE WORK OF MILITARY ADMINISTRATION BODIES DURING PLANNING OPERATIONS

Macliuk Leonid *(Candidate of Technical Sciences, Senior Researcher)*
Havalko Vasyl *(Candidate of Technical Sciences, Associate Professor)*
Kolodiazhnyi Anatolii
Dzhygomon Sergii

National Defence University of Ukraine, Kyiv, Ukraine

One of the key areas of increasing the effectiveness of the management of troops (forces) during operation planning and making informed decisions at the modern stage of the armed struggle is to ensure the joint and synchronized work of command groups with a significant number of people in the military administration. In this regard, the main task of the article is to determine possible approaches to increase the efficiency of the work of military management bodies thanks to the information and analytical support of the organization of their work in the process of planning the operation. To achieve the task, the methods of system analysis, network planning and management, and BPMN business process modeling notation methods were used as the main means of describing the functioning of military administration bodies. The specified methodological approach makes it possible to reveal and analyze in more detail the process of organizing work in military administration bodies, to determine the main problematic issues and possible ways to solve them. The article proposes approaches to optimizing the work of military administration bodies in the process of planning an operation based on pre-prepared standard plans and forms of documents, substantiates the functions of information and analytical support for the work organization process, proposes the composition of software tools and develops a generalized procedure for their operation, formalizes the model of a standard plan and of the operation preparation plan in the form of hierarchical structures of process diagrams based on the formulated basic definitions of its elements, an approach is proposed regarding the use of the specified model for the organization of operational control of the implementation of the activities (tasks) of the plan. The elements of scientific novelty consist in clarifying and concretizing the well-known BPMN process modeling notation and extending its application to information objects in the field of organizing the work of military administration bodies, which provides opportunities for developing process models in this field, conducting simulations, and deeper research into them. The obtained results are a further improvement of methodical approaches to the development of information and analytical support software for the organization of the work of military administration bodies. Currently, information and analytical support for the organization of the work of military administration bodies during operation planning in the Armed Forces of Ukraine is carried out using software from Microsoft Office or individual applications with a low level of functionality, which does not provide highly effective support for the work of officials, limits automation opportunities management functions and, most importantly, does not allow implementing systemic approaches in the process of creating automated military management systems. The above emphasizes the relevance of the topic of the article.

Keywords: *preparation of the operation, planning of the operation, the process of making a military decision, organizing the work of the military administration bodies.*

References

1. NATO Standard AJP-5: NATO Joint Forces Doctrine for Planning Operations, (2019). Kyiv: NUOU. **2. Methodical** recommendations for planning and organizing a battle according to NATO standards (brigade (battalion) headquarters and their equals) [online]. Available at: https://jurkniga.ua/contents/ metodichni-rekomendatsii-z-planuvannya-ta-organizatsii-boyu-za-standartami-nato-shtab-brigadi-batalyonu-ta-im-rivnikh.pdf [Accessed: 20 May 2023]. **3. The procedure** for operational planning in the NATO military command bodies: training. manual. A. M. Syrotenko, V. M. Tarasov, S. M. Salkutsan, etc., (2019). Kyiv: NUOU. **4. Procedures** of the military decision-making process (according to NATO standards): training. manual / Muzychenko D. P., Filyunkin E. V. etc., (2018). Kyiv: NUOU. **5. System** for modeling processes in BPMN notation [online]. Available at: https://www.terrasoft.ua/page/ru/bpmn [Accessed: 22 May 2023]. **6. BPMN** - Wikipedia. [online]. Available at: https://uk.wikipedia.org/wiki/ BPMN [Accessed: 22 May 2023]. **7. Features** of the description of business processes in modern IT systems. [online]. Available at: http://www.economy.nayka.com.ua/?op=1&z=3514 [Accessed: 22 May 2023]. **8. Methods** of describing business processes [online]. Available at: https://manageable.com.ua/metody-opysu-biznes-protsesiv/ [Accessed 22 May 2023].

DOI:**10.33099/2311-7249/2023-47-2-85-90**

УДК 355.41

Паценко Степан Володимирович
***Ганненко Юрій Олександрович** (доктор філософії)*

Національний університет оборони України, Київ, Україна

ФУНКЦІОНУВАННЯ СИСТЕМИ ПОСТАЧАННЯ МАТЕРІАЛЬНИМИ ЗАСОБАМИ ЗБРОЙНИХ СИЛ УКРАЇНИ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У статті, на основі функціонування логістичної системи Збройних сил України, визначено основні проблемні питання, що пов'язані з постачанням матеріальними засобами військ (сил) Збройних сил України, запропоновано заходи стосовно впровадження сучасних інформаційних технологій в логістичну систему Збройних сил України з метою поліпшення ефективності та оптимізації цього процесу. У процесі дослідження застосовано метод системного аналізу. Зазначений методологічний підхід дозволяє прогнозувати постачання матеріальними засобами, створювати інтегровані системи управління та контролю їх руху, розробляти системи логістичного обслуговування, оптимізувати запаси з використанням інформаційних технологій. Останнім часом, з моменту отримання міжнародної технічної допомоги від країн-партнерів, значна увага надається аспектам постачання матеріальними засобами військам (силам) Збройних сил України. Так, з моменту повномасштабного вторгнення військ російської федерації в Україну, Збройні сили України, за умови задовільного постачання під час бойових дій, продемонстрували власну спроможність виконувати бойові завдання згідно їхнього прямого призначення. З метою підвищення ефективності функціонування системи постачання матеріальними засобами Збройних сил України проаналізовано досвід провідних країн світу. Країни, які входять до НАТО використовують різні автоматизовані системи управління логістичною системою. Зокрема, під час проведення міжнародних навчань і тренувань, вони застосовують спеціалізоване програмне забезпечення LOGFAS. Також у статті сформульовані напрями подальших досліджень щодо удосконалення системи постачання матеріальними засобами військ (сил) Збройних сил України з використанням інформаційних технологій. Стаття має важливе прикладне значення, оскільки запропоновані заходи дадуть змогу підвищити ефективність постачання матеріальними засобами військ (сил) Збройних сил України, скоротити час на одержання та всебічне оцінювання відомостей про військове майно на всіх етапах його руху, а також збільшити ефективність підтримки військ (сил) і покращити взаємодію з аналогічними системами країн-партнерів НАТО.

***Ключові слова**: військове майно, логістика, логістична система, система забезпечення, матеріальні засоби, міжнародна технічна допомога, перевезення, постачання.*

Вступ

На сьогоднішній день у сучасному світі інформаційні технології займають передове місце для розвитку людини, тому важливість інформаційних технологій у впровадженні в системі постачання матеріальними засобами Збройних сил України (далі – ЗС України) відіграє важливу роль в обороноздатності нашої держави. Нині, під час постачання матеріальними засобами, інформаційні технології відіграють важливу роль, як ключовий логістичний показник. Завдяки сучасним інформаційним технологіям можливо удосконалити систему постачання матеріальних засобів в ЗС України.

Інформаційні технології в логістичній системі розглядаються як автоматизовані системи управління логістичними процесами, які в свою чергу складаються з апаратного забезпечення, програмного забезпечення, кодифікації матеріальних засобів та інтерфейсу користувача. У ЗС України автоматизовані системи управління логістики використовуються з метою автоматизованого управління логістичними процесами. Логістичні інформаційні системи відрізняються як своїми особливостями, так і підсистемами, що їх забезпечують.

У 2021 році було запропоновано впровадження автоматизованої системи контролю наявності нафтопродуктів. Для здійснення комплексної автоматизованої підтримки процесів управління логістичним забезпеченням була створена відповідна автоматизована система управління. Складовою частиною системи є логістична інформаційна система, що розроблена в межах діяльності Багатонаціонального об'єднаного

координаційного комітету з питань військового співробітництва та оборонного реформування за сприянням США. Проте, ця система не була впроваджена в логістичну систему постачання матеріальними засобами ЗС України.

Надходження міжнародної технічної допомоги для ЗС України надало можливість впровадження спеціалізованого програмного забезпечення «Системи функціональних областей логістики» (Logistics Functional Area Services (LOGFAS)) для обліку військового майна, що надійшло від наших партнерів як матеріальна технічна допомога.

Постановка проблеми. З початком широкомасштабної збройної агресії російської федерації проти України виникли численні проблемні питання, пов'язані з постачанням матеріальних засобів військам (силам), а саме:

застарілий облік матеріальних засобів;

недофінансування заходів із закупівлі матеріальних засобів;

недостатній обсяг оперативних і стратегічних запасів матеріальних засобів;

ускладнення доставки й переміщення матеріальних засобів через наявність перешкод, таких як зруйновані дороги, мости та інфраструктура, захоплення ворогом значних територій та основних логістичних шляхів, що призводило до збільшення часу, необхідного для виконання замовлення;

обмежений доступ до місцевих матеріальних ресурсів;

скорочення складських фондів, незадовільний стан вивільнених (законсервованих) складських фондів військових містечок;

мобілізаційні договори, що були укладені заздалегідь для забезпечення потреб ЗС України, залишились нереалізованими;

значне збільшення кількості військових частин (підрозділів) ЗС України під час мобілізації в Україні.

Аналіз останніх досліджень і публікацій. За період з початку збройної агресії військ російської федерації проти України до нині, з'явилася значна кількість нормативних документів, зокрема [1–5], що регулюють виконання завдань з логістичного забезпечення військ (сил) в ході проведення антитерористичної операції та операції Об'єднаних сил на території Донецької та Луганської областей та забезпечують удосконалення системи постачання матеріальними засобами військ (сил) із впровадження сучасних інформаційних технологій в ЗС України.

Нормативні документи [6–12] унормовують логістичне забезпечення ЗС України, організацію залучення, використання, облік та моніторинг міжнародної технічної допомоги в Міністерстві оборони України та ЗС України. Крім того, врегульовано звітність про наявність у ЗС України військового майна, отриманого як міжнародна технічна допомога, а також – постачання наземних військ та взаємодопомогу в логістиці тощо.

У наукових статтях Ю. О. Ганненка, В. С. Кивлюка, В. І. Лазоренка [13–14] авторами запропоновано:

удосконалення системи забезпечення військ (сил) ЗС України шляхом створення автоматизованої системи управління логістики, що, в свою чергу, можуть підвищити ефективність системи постачання матеріальними засобами у ЗС України та досягти поставлених цілей;

створення ефективної системи забезпечення сил оборони України, що спроможна здійснювати планування та управління процесами забезпечення військ (сил) військовим майном як у мирний час, так і в особливий період та буде сумісною із системою НАТО.

Водночас, на сьогодні варто констатувати, що питання використання інформаційних технологій для забезпечення належного функціонування системи постачання в ЗС України у науковому дискурсі недостатньо висвітлене.

Метою статті є визначення основних проблем функціонування системи постачання матеріальними засобами Збройних сил України з використанням інформаційних технологій.

Виклад основного матеріалу дослідження

Система постачання матеріальними засобами ЗС України є складним та відповідальним завданням, оскільки вона забезпечує надходження різних видів матеріальних засобів до військових частин, які беруть участь у військових операціях – відбитті широкомасштабного вторгнення збройної агресії військ російської федерації (далі – рф). Аналізуючи функціонування системи постачання матеріальними засобами ЗС України, можна виділити наступні аспекти: організаційний, фінансовий, кадровий та логістичний.

Так, організаційний аспект – це система постачання матеріальними засобами, яка має чітку організаційну структуру, що включає у себе відповідальних за забезпечення матеріальними засобами осіб на кожному рівні управління. Проте, іноді виникають проблеми з координацією та комунікацією між різними рівнями управління, що може призвести до неефективного постачання матеріальними засобами.

Фінансовий аспект – постачання матеріальними засобами є доволі таки витратним процесом, тому ефективне фінансування є необхідним для забезпечення військових частин матеріальними засобами. Однак, іноді фінансування може бути обмеженим, що може призвести до затримок у закупівлі матеріальних засобів.

Кадровий аспект – система постачання матеріальними засобами, що має потребувати висококваліфікованих кадрів, які здатні ефективно керувати цим процесом і забезпечувати військові частини необхідними матеріальними засобами.

Але, іноді кадрове забезпечення має недоліки щодо призначення не кваліфікованих фахівців.

Логістичний аспект – система постачання матеріальними засобами має складну логістичну структуру, що включає різні етапи – від закупівлі матеріальних засобів до їхньої доставки до військових частин. Цей процес вимагає ефективного планування і контролю, щоб уникнути затримок у поставках та забезпечити надходження матеріальних засобів вчасно.

Використання інформаційних технологій в системі постачання матеріальними засобами ЗС України має багато переваг, таких як швидкість і точність обліку, ефективне управління запасами та зниження витрат на зберігання й обробку даних, але потребує також виконання певних вимог, зокрема:

необхідність високотехнологічного обладнання та програмного забезпечення для підтримки інформаційних систем, яке може призвести до високих витрат на обладнання та програмне забезпечення, що можуть бути вищими, ніж витрати на традиційні системи управління запасами;

залежність інфраструктури від інформаційних технологій і лімітоване, на деяких територіях, з'єднання з інтернетом призводить до обмеження доступу деяких об'єктів військових операцій до необхідних матеріальних засобів через відсутність зв'язку з центральною базою даних;

можливість кібератак та злому системи, якщо система не захищена, що може призвести до втрати даних або несанкціонованого доступу до закритої інформації обліку матеріальних засобів;

використання інформаційних технологій у системі постачання матеріальними засобами ЗС України потребує додаткової підготовки персоналу, щоб вони могли професійно користуватися системою та забезпечувати її безпеку.

В НАТО використовується спеціалізоване програмне забезпечення LOGFAS з 1995 року, яке успішно застосовується для автоматизованої підтримки системи логістики НАТО під час операцій та навчань. LOGFAS використовується з метою задоволення технічних вимог для мінімізації часу планування і максимізації спроможності швидкого обміну відповідними матеріальними засобами, логістичними планами, звітами та іншою інформацією [9–12].

Система функціональних областей логістики LOGFAS – це спеціалізоване програмне забезпечення НАТО в сфері логістики, що дозволяє здійснювати обмін даними між штаб-квартирою НАТО, підрозділами та державами, що їх виділяють, на всіх етапах планування та проведення забезпечення військ за рахунок використання серії інтегрованого програмного забезпечення. LOGFAS складається з логістичної бази даних (LOGBASE), системи НАТО з розгортання і перевезення (далі – ADAMS), програмного забезпечення НАТО з оптимізації ресурсів (ACROSS) та системи звітування з логістичного забезпечення (LOGREP) (рис.1).

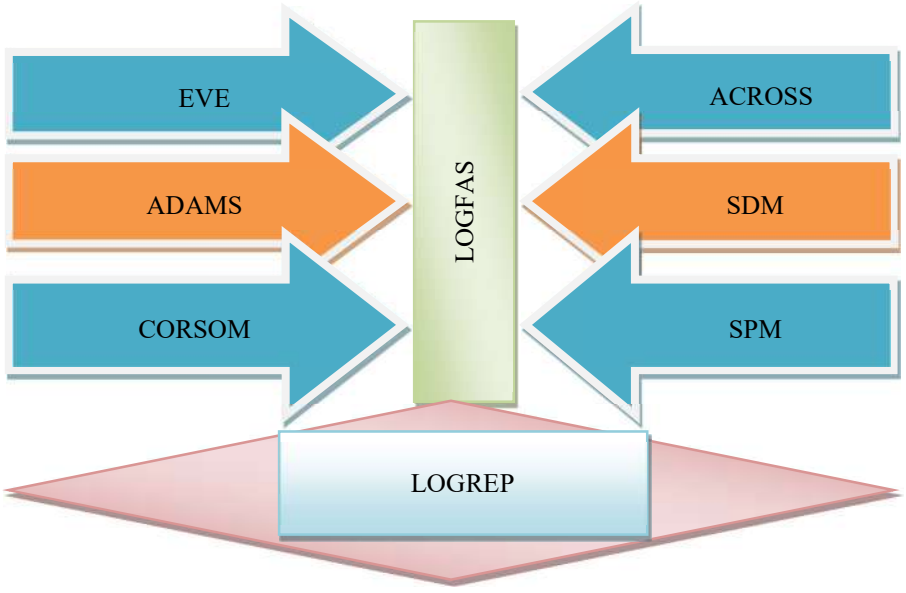


Рисунок1 – Організація функціонування програмного забезпечення LOGFAS

До складових LOGFAS належать:

«Модуль управління даними LOGFAS» (LOGFAS Data Management Module (LOGFAS LDM)), що призначений для управління даними не географічного характеру (предмети, сили і засоби, організація військ і підпорядкованість, запаси та профілі поповнення запасів сил, план операції, визначення вимог тощо). У режимі перегляду LDM відображається головне меню з панеллю інструментів із піктограмою швидкого доступу для запуску відповідних функціональних можливостей програми та дисплей головного вікна, де будуть

показані відповідні функціональні можливості програми зі складних меню;

«Модуль планування сталого розвитку» (Sustainment Planning Module (SPM)), що призначений для оперативного планування логістичного забезпечення підрозділів. Цей модуль може бути використаний для планування довготермінових запасів, логістичного забезпечення підрозділів під час операцій;

«Інструмент логістичної звітності» (Logistic Reporting Tool (LOGREP)), що призначений для створення зокрема стандартних звітів «оновлення логістичних даних» (LOGUPDATE) та «логістичний список» (LOGASSESSREP), а також аналізу карт та мереж, створення та управління профілями сил, наявними запасами (holdings) та списками предметів постачання (RIL);

«Програмна система оптимізації ресурсів» (Allied Commands Resource Optimisation Software System (ACROSS)), що призначений для підтримки прийняття рішень в плануванні запасів (stockpiles), зокрема боєприпасів та амуніції, що є критичними для здійснення операцій;

«Система розгортання і пересування засобів» (Allied Deployment and Movements System (ADAMS)), що призначений для планування, оцінки і моделювання (симуляції) переміщення та транспортування, з метою підтримки операцій. Призначений для зменшення часу на планування розгортання і надання засобів для обміну даними та планами розгортання між країнами;

«Прийом коаліцій, становлення та подальший рух» (Coalition Reception, Staging and Onward Movement (CORSOM)), що призначений для планування, моніторингу і усунення конфліктів під час дій з прийому, організації та переміщення далі (RSOM) сил у процесі розгортання. Включно з виконанням та управлінням розгортання сил, використовуючи детальні плани розгортання (DDP) з ADAMS;

«Модуль розподілу постачання» (Supply Distribution Module (SDM)), що призначений для верифікації та моделювання (симуляції) спланованого логістичного забезпечення;

«Ефективне візуальне оформлення» (Effective Visual Execution (EVE)), що призначений для оперативного контролю логістичного забезпечення виконання операцій;

«Модуль управління географічними данними» (Geographical Data Management Module (GEOMAN)), що призначений для відображення географічних (картографічних) даних;

«Модуль менеджера підключень» (LOGFAS Connection Manager Module (LCM)), що призначений для управління базами даних та контролю вибору і керування базами даних, що були створені для використання з програмами LOGFAS.

Усі програми LOGFAS отримують доступ до активної бази даних, керованої в LCM, ця база даних може бути розміщена на локальній машині або на сервері. LCM дозволяє також створювати, видаляти, імпортувати та експортувати бази даних. Віддалені бази даних можна підключати або від'єднувати лише від клієнта, вони створюються як локальні бази даних на сервері, і зазвичай доступ до них здійснюється через мережу. Конфігурація налаштувань версії бази даних також обробляється в LCM, окрім географічного посилання, яке оновлюється за допомогою географічного менеджера Geoman.

ЗС України з 2019 року включені до переліку держав, які використовують спеціалізоване програмне забезпечення LOGFAS. Так, було ухвалено угоду на 5 років між Генеральним штабом ЗС України та Секретаріатом штаб-квартири НАТО з консультацій, командування та управління.

Але, на даний час існують проблемні питання із запровадженням інформаційних технологій в системі постачання матеріальних засобів в ЗС України. Для належного функціонування програмного забезпечення необхідно використовувати захищену мережу передачі даних, але не у всіх військових частинах підрозділах вона застосовується, та є нагальна потреба в забезпеченні більш сучасними та потужними персональними електронно-обчислювальними машинами і відповідним обладнанням [13–14];

Отже, проблемні питання системи постачання матеріальними засобами ЗС України з використанням інформаційних технологій показали напрями подальших досліджень щодо удосконалення до певного рівня системи забезпечення, яка б відповідала вимогам сьогодення, своєчасно та повною мірою забезпечувала би потреби військ (сил).

Так, використання інформаційних технологій має бути одним з пріоритетних напрямів роботи з підвищення ефективності системи постачання матеріальними засобами в ЗС України. Створення нових і модернізація існуючих автоматизованих систем постачання матеріальними засобами на основі передових інформаційних технологій дозволить підвищити ефективність системи постачання матеріальними засобами ЗС України, скоротити час на одержання і всебічну оцінку відомостей про військове майно на всіх етапах їх руху, підвищити ефективність сил підтримки, а також покращити взаємодію з аналогічними системами країн-партнерів НАТО.

Висновки й перспективи подальших досліджень

Наприкінці зазначимо, що у статті:

проведено аналіз функціонування системи постачання матеріальними засобами Збройних сил України;

визначено основні проблемні питання постачання матеріальними засобами військ (сил) Збройних сил України і використання

інформаційних технологій в провідних країнах світу;

запропоновано впровадження сучасних інформаційних технологій, що використовуються в країнах НАТО, в логістичну систему Збройних сил України.

Перспективи подальших досліджень вбачаються в розробці науково-методичного апарату оцінювання ефективності функціонування системи постачання матеріальних засобів у Збройних силах України з використанням інформаційних технологій.

Використання інформаційних технологій під час організації постачання матеріальними засобами має бути одним з пріоритетних напрямів роботи з підвищення ефективності діяльності логістичної системи Збройних сил України. Створення нових і модернізація існуючих автоматизованих систем управління логістики на основі передових інформаційних технологій дозволить підвищити ефективність постачання матеріальними засобами, скоротити час на одержання і всебічну оцінку відомостей про військове майно на всіх етапах їх руху, підвищити ефективність підтримки військ (сил), а також покращити взаємодію з аналогічними системами країн-партнерів НАТО.

Список бібліографічних посилань

1. Доктрина об'єднана логістика: наказ Головнокомандувача ЗС України від 24.09.2020 № 2861. 37 с. **2. Доктрина** з організації переміщень та перевезень (транспортувань) у Збройних Силах України: наказ Генерального штабу Збройних Сил України від 20.08.2020 року № 2464. **3. Доктрина** забезпечення матеріально-технічними засобами, роботами та послугами: наказ Генерального штабу Збройних Сил України від 21.01.2021 року № 225. **4. Доктрина** Сил логістики: затверджена Головнокомандувачем ЗС України 08.02.2021 р. **5. Доктрина** Застосування сил логістики: затверджена начальником ГШ ЗС України 04.02.2021 року. ALP-4 – доктрина НАТО з логістики. URL: https://sprotyvg7.com.ua/wp-content/uploads/ (дата звернення: 15.05.2023). **6. Про затвердження** Основних положень логістичного забезпечення Збройних Сил України: наказ Міністерства оборони України від 11.10.2016 № 522. URL: http://arcdrmis.rit.org.ua/WWW/arch_mod/docs (дата звернення: 15.05.2023). **7. Про затвердження** Інструкції про організацію залучення, використання, обліку та моніторингу міжнародної технічної допомоги в Міністерстві оборони України та Збройних Силах України зі змінами та доповненнями : наказ Міністерства Оборони України від 01.02.2018 №37. URL: https://zakon.rada.gov.ua/laws/show/z0222-18 (дата звернення: 15.05.2023). **8. Про затвердження** Інструкції з надання звітності про наявність у Збройних Силах України військового майна, отриманого як міжнародна технічна допомога : наказ Головнокомандувача Збройних Сил України від 18.08.2020 №116. **9. STANAG** 2961 – Класи предметів постачання наземних військ НАТО. CLASSES OF SUPPLY OF NATO FORCES ВДВ 01.300.001 – 2016 (01) URL: https://www.mil.gov.ua/content/pdf/Standart_NATO/ (дата звернення: 15.05.2023). **10. STANAG 2034** – Стандартні процедури НАТО щодо взаємодопомоги в логістиці. Настанова з логістики НАТО, Штаб квартира НАТО, Брюссель, 2012. URL: https://www.mil.gov.ua/content/mil_standard/List_of_standarts_and_doc_NATO (дата звернення: 15.05.2023). **11. AJP-01(D):** Доктрина об'єднаних сил НАТО, довідкові матеріали. Київ : НУОУ ім. Івана Черняховського. 2016. С. 130. **12. NATO** Logistics Handbook. Brussels: NATO HQ, 2012. 207 с. URL: https://www.nato.int/docu/logi-en/logist97.htm (дата звернення: 15.05.2023). **13. Ганненко Ю. О.** Аналіз функціонування системи логістики у провідних країнах світу. *Сучасні інформаційні технології у сфері безпеки та оборони.* Київ : НУОУ. 2019. № 3(36). С. 115–122. URL: http://sit.nuou.org.ua/article/view/190490/190343 (дата звернення: 15.05.2023). **14. Кивлюк В. С., Лазоренко В. І., Ганненко Ю. О.** Проблеми управління системою забезпечення військовим майном військ (сил) Збройних Сил України та шляхи їх вирішення. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2021. №1(40). С. 111–116. URL: http://sit.nuou.org.ua/article/view/231844 (дата звернення: 15.05.2023).

FUNCTIONING OF THE SYSTEM OF SUPPLYING THE ARMED FORCES OF UKRAINE WITH MATERIAL RESOURCES USING INFORMATION TECHNOLOGIES

Patsenko Stepan
Gannenko Yurii ***(Doctor of Philosophy)***

The article, based on the functioning of the logistics system of the Armed Forces of Ukraine, identifies the main problematic issues related to the supply of material resources to the troops (forces) of the Armed Forces of Ukraine, and proposes measures to introduce modern information technologies into the logistics system of the Armed Forces of Ukraine with a view to improving the efficiency and optimisation of this process. In the course of the study, the method of system analysis was applied. This methodological approach allows forecasting the supply of material resources, creating integrated systems for managing and controlling their movement, developing logistics service systems, and optimising stocks using information technology. Recently, since receiving international technical assistance from partner countries, considerable attention has been paid to the aspects of supplying the troops (forces) of the Armed Forces of Ukraine. Thus, since the full-scale invasion of Ukraine by the Russian Federation, the Armed Forces of Ukraine have demonstrated their ability to perform combat missions in accordance with their intended purpose, provided they are satisfactorily supplied during combat operations. In

order to improve the efficiency of the Armed Forces of Ukraine's materiel supply system, the experience of the world's leading countries was analysed. NATO member states use various automated logistics management systems. In particular, during international exercises and training, they use specialised software LOGFAS. The article also formulates directions for further research on improving the system of supplying the troops (forces) of the Armed Forces of Ukraine with the use of information technology. The practical significance of the article lies in the fact that it will be possible to increase the efficiency of supplying the troops (forces) of the Armed Forces of Ukraine with materiel, reduce the time for obtaining and comprehensive assessment of information on military property at all stages of its movement, as well as increase the efficiency of support for troops (forces) and improve interaction with similar systems of NATO partner countries.

Key words: *military property, logistics, logistics system, support system, material means, international technical assistance, transportation, supply.*

References

1. Joint Logistics Doctrine: Order of the Commander-in-Chief of the Armed Forces of Ukraine of 24.09.2020 No. 2861. 37 c. **2. Doctrine** on the organization of movements and transportation in the Armed Forces of Ukraine: Order of the General Staff of the Armed Forces of Ukraine of 20.08.2020 No. 2464. **3. Doctrine** on the provision of material and technical means, works and services: Order of the General Staff of the Armed Forces of Ukraine of January 21, 2021, No. 225. **4. Doctrine** of the Logistics Forces: approved by the Commander-in-Chief of the Armed Forces of Ukraine on February 08, 2021. **5. Doctrine** on the Use of Logistics Forces: approved by the Chief of the General Staff of the Armed Forces of Ukraine on February 04, [online], (2021). ALP-4 is NATO's logistics doctrine. Available at: https://sprotyvg7.com.ua/wp-content/uploads/ [Accessed 15 May 2023]. **6. On Approval** of the Basic Provisions of Logistics Support of the Armed Forces of Ukraine: Order of the Ministry of Defense of Ukraine of 11.10 No. 522 [online], (2016). Available at: http://arcdrmis.rit.org.ua/WWW/arch_mod/ docs [Accessed 15 May 2023]. **7. On approval** of the Instruction on the organization of attracting, using, accounting and monitoring of international technical assistance in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine as amended: Order of the Ministry of Defense of Ukraine of 01.02 No. 37. [online], (2018). Available at: https://zakon.rada.gov.ua/laws/show/z0222-18 [Accessed 15 May 2023]. **8. On Approval** of the Instruction on Reporting on the Availability of Military Property Received as International Technical Assistance in the Armed Forces of Ukraine: Order of the Commander-in-Chief of the Armed Forces of Ukraine of 18.08.2020 No. 116 **9. STANAG 2961** - Classes of supply items for NATO ground forces. CLASSES OF SUPPLY OF NATO FORCES 01.300.001 - 2016 (01) [online], (2016). Available at: https://www.mil.gov.ua/content/pdf/Standart_NATO/ [Accessed 15 May 2023]. **10. STANAG** 2034 - NATO Standard Operating Procedures for Mutual Assistance in Logistics. NATO Logistics Manual, NATO Headquarters, Brussels, [online], (2012). Available at: https://www.mil.gov.ua/content/mil_standard/List_of_standarts_and_doc_NATO [Accessed 15 May 2023]. **11. AJP-01(D):** NATO Joint Force Doctrine, background materials. Kyiv: Ivan Chernyakhovsky National University. (2016), 130. **12. NATO** Logistics Handbook. Brussels: NATO HQ, 207 (2012) [online], available at: https://www.nato.int/docu/logi-en/logist97.htm [Accessed 15 May 2023]. **13. Analysis** of the functioning of the logistics system in the leading countries of the world / Modern information technologies in the field of security and defense. Kyiv: NOU, 3(36), 115-122. [online], (2019). Available at: http://sit.nuou.org.ua/article/view/190490/190343 [Accessed 15 May 2023]. **14. Kivliuk, V. S., Lazorenko, V. I., Hannenko, Y. O.,** (2021). Problems of managing the system of providing military property to the troops (forces) of the Armed Forces of Ukraine and ways to solve them. Modern information technologies in the field of security and defense, 1(40), 111-116.

DOI:**10.33099/2311-7249/2023-47-2-91-95**

УДК 621.37

Нещерет Іван Григорович [1]
Злобін Кирило В'ячеславович [1]
Цикало Юрій Григорович [2]

[1] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2] ***Військова частина А0707, Гайсин, Україна***

ОСОБЛИВОСТІ ПОБУДОВИ ТА РЕКОМЕНДАЦІЇ СТОСОВНО ВИКОРИСТАННЯ РАДІОМОДУЛЯ nRF24L01 У ВІЙСЬКОВІЙ ТЕХНІЦІ

Сьогодні, приймально-передавальна апаратура зазнала суттєвого розвитку, здебільшого, завдяки цифровізації. Цифрова техніка стає все популярнішою під час прийому й передачі інформації. Восьмирозрядні мікроконтролери (наприклад, nRF24L01) володіють достатньою швидкістю обробки даних. Забезпечивши аналого-цифрове перетворення та маючи можливості в програмуванні даних мікроконтролерів, відкриваються перспективи для реалізації трансивера. Серія виробів провідної корпорації Nordic Semiconductor містять вбудовані високопродуктивні мультиплексори, що з'єднані з Flash-пам'яттю (ядром) мікроконтролера індустріального стандарту 8052 (наприклад, nRF24L01), та підтримує декілька стандартів конфігурації послідовного порту. Ці вироби є першими інтегрованими схемами, які можна назвати «інтелектуальними прийомо-передавачами» для систем збирання та обробки даних на одному кристалі. На першому етапі обробка фізичних сигналів полягає в необхідності отримання інформації, що міститься в них. Ця інформація наявна в амплітуді сигналу, в частоті або спектральному складі, у фазі чи у відносних часових залежностях декількох сигналів. У деяких випадках бажано змінити формат інформації, яка знаходиться в пакеті сигналу. Наприклад, зміна формату відбувається під час передавання звукового сигналу в телефонній системі з багатоканальним доступом і частотним розділенням. У випадку цифрового зв'язку аналогова звукова інформація спочатку перетворюється на цифрову за допомогою аналого-цифрового перетворювача. Цифрова інформація, що втілює в собі індивідуальні звукові канали, мультиплексується (багатоканальний доступ з часовим розділенням (TDMA)) та передається через послідовну цифрову лінію зв'язку. Метою статті є проведення аналізу особливостей побудови та надання рекомендації щодо застосування радіомодуля nRF24L01 у техніці військового призначення, а також – порівняння основних принципів та стандартів моделювання сигналів і завад в електронних системах, принципів дискретизації, кодування сигналів.

Ключові слова: *радіозв'язок, амплітудна модуляція, частотна модуляція, бездротовий зв'язок, комунікаційний пристрій, супутникова навігація, Інтернет речей.*

Вступ

Забезпечення основних вимог до систем бездротового зв'язку, забезпечення стійкості бездротового радіозв'язку від завадоперешкод, оперативна доставка інформації та даних із забезпеченням необхідного рівня захисту вимагає цифрової обробки сигналу та шифрування даних. Безпека інформації – найважливіший елемент у технології бездротового зв'язку. Використовуючи бездротове з'єднання, необхідно звертати увагу на захист особистих даних. Можна легко підключитися до незахищених бездротових маршрутизаторів. Проблема полягає в тому, що будь-хто, хто підключений до бездротового маршрутизатора, що використовується користувачем, може отримувати доступ до його даних та займатися діяльністю, яка є незаконною згідно з українським законодавством. Наприклад, це може включати нелегальне завантаження фільмів та музики з піратських сайтів, порушуючи законодавство про авторське право.

В бездротовому зв'язку використовується широкий діапазон електромагнітного спектру, від радіохвиль низької частоти в кілька кілогерц до видимого світла, частота якого складає приблизно 8*1014Гц. Взагалі, якщо проаналізувати весь електромагнітний спектр, то можна зробити висновок, що фактично всі діапазони можна використовувати для передавання даних. Радіо, мікрохвильовий, інфрачервоний діапазони, а також видиме світло можуть бути використані для передавання сигналів за допомогою амплітудної, частотної чи фазової модуляції хвиль. Ультрафіолетове, рентгенівське і гамма випромінення були б навіть кращими завдяки їхнім високим частотам, однак їх складно генерувати і

модулювати, вони погано проходять крізь будинки і, крім того, вони небезпечні для всього живого.

Постановка проблеми. Знання умов розповсюдження електромагнітного поля дуже важливе для визначення небезпечних відстаней, на яких можливий несанкціонований доступ технічних засобів розвідки до даних, що містяться у сигналах, які перехоплюються. В разі потреби, простір, у межах якого існує небезпека перехоплення, контролюється, щоб виключити наявність технічних засобів розвідки. В інших випадках, потрібно вдаватися до заходів захисту даних, що переносяться електромагнітними полями, які є інформативними для розвідки.

Аналіз останніх досліджень і публікацій. У роботах [1; 6–8] докладно описано приклади обробки і перетворення отриманого інформаційного або керуючого сигналу та їх обробки. Останнім часом, сама організація і методи передачі даних або інформації каналами бездротового зв'язку, зазнали значних змін. За таких умов, для забезпечення високої пропускної спроможності радіоканалів приймаються інноваційні технічні рішення. Відповідно, для практичної реалізації бездротового зв'язку необхідні знання і розвиток методів цифрової обробки сигналів з урахуванням специфіки поширення сигналів у системах радіозв'язку. І хоча протягом останніх років з`явилася значна кількість технічної літератури, що присвячена даній проблематиці, проте питання методів передачі даних або інформації каналами бездротового зв'язку висвітлене не достатньо. Досі відчувається дефіцит простих публікацій на тематику цифрового оброблення сигналів в системах мобільного і бездротового зв'язку з урахуванням сучасного рівня та тенденцій розвитку телекомунікацій.

Мета статті. Проведення аналізу особливостей побудови та надання рекомендації щодо використання радіомодуля nRF24L01 у техніці військового призначення, а також – порівняння основних принципів та стандартів моделювання сигналів і завад в електронних системах, принципів дискретизації, кодування сигналів.

Виклад основного матеріалу дослідження

У сучасних комунікаційних пристроях, крім стандарту GSM [2], також використовуються інші радіоінтерфейси, наприклад WI-FI та Bluetooth. Без WI-FI було б неможливо підключитися до мережі Інтернет через маршрутизатори доступу, які дозволяють передавати дані. А одне з найвідоміших, але не єдине застосування Bluetooth – це можливість підключення до віддалених аудіосистем, наприклад, автомобільні комплекти гучного зв'язку або бездротові навушники.

На споживчому ринку спостерігається зростання передових технологій, що базуються на бездротових з'єднаннях. Крім технології зв'язку GSM, тепер можна використовувати, наприклад, супутникову Global Positioning System (далі – GPS) навігацію або інші конкуруючі системи супутникової навігації. Ця технологія стала настільки доступною, що зараз використовується не лише для комунікаційної навігації, а й для геотегування фотографій та інших подібних можливостей.

Паралельно з розвитком супутникової навігації, технологія Інтернету речей Internet of Things (далі – IoT) також стрімко розвивається. Термін IoT вперше було означено у 1999 році. Це концепція комунікації між об'єктами, що використовують технологію для взаємодії цих об'єктів з навколишнім середовищем. Також концепція передбачає керування певними діями пристроїв без втручання людини. Отже, всі пристрої в офісах, будинках, автомобілях, без втручання користувача виконують обробку інформації, її аналіз та обмін між собою, і залежно від результату, приймають рішення для виконання певної дії.

Масове використання радіозв'язку користувачами, які мають кваліфікацію та ліцензію Укрчастотнагляду і допущені до роботи з приймально-передавальними пристроями, вимагає дотримання регламенту. Для таких комунікаційних пристроїв смуги частот, на яких вони працюють, можуть бути виділені без отримання дозволів. Пристрої, що працюють у цих діапазонах, мають дотримуватися законодавчо визначеної обмеженої потужності та використовувати лише виділені частоти (діапазони). Найчастіше це діапазони «Промисловість, наука, медицина» (Industrial, Scientific and Medical (далі – ISM)), що зарезервовані для промислових, наукових та медичних потреб. У різних країнах використовуються різні частоти для бездротових пристроїв. Під час проєктування пристрою, що працює в діапазоні ISM, важливо враховувати відповідні частоти.

Комунікаційні пристрої ISM радіозв'язку мають багато переваг. Вони характеризуються зручністю та вигідністю виробництва, а також простотою у налаштуванні. Водночас –забезпечують необмежену мобільність у визначеному діапазоні частот. Але вони також мають і недоліки. Один з таких недоліків полягає в тому, що передача по радіоканалах зв'язку вимагає все більш складного шифрування сигналу для запобігання перехопленню даних або їх модифікації в злочинних цілях. Іншою проблемою можуть бути електромагнітні завади, що викликають згасання чи спотворення сигналу.

Загальні поняття і принципи передачі даних та модуляцій їх сигналу.

З технічної точки зору, для передачі даних потрібен радіомодем та система прийомо-передавача, тобто трансивер [3]. Модем перетворює цифровий сигнал, що складається з послідовності нулів і одиниць, в аналоговий сигнал, який може бути переданий через радіоканал.

Одним із найбільш відомих методів є модуляція Frequency Shift Keying (далі – FSK) (рис. 1), або частотна модуляція (далі – ЧМ) та її варіації.

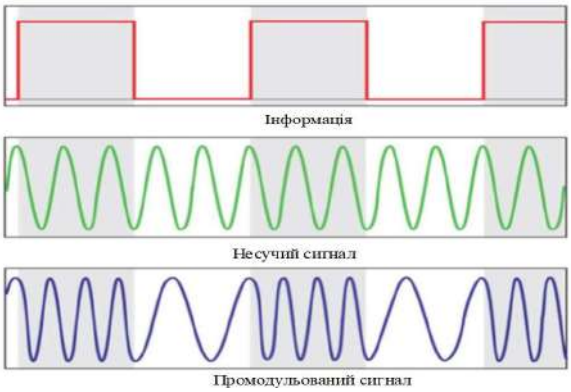


Рисунок 1 – Частотна модуляція

Дані модуляції полягають у дискретній зміні частоти носія залежно від інформаційного біта, який передається. Модуляція FSK та її модифікація є більш стійкими до завад, і тому їх ефективніше використовувати. В частотній модуляції відповідно до модулювального сигналу Sm(t) змінюється частота або початкова фаза опорного сигналу. Так, за фазовоъ модуляції сигнал може бути формалізований виразом:

$$\varphi(t) = kSm(t). \quad (1)$$

Отже, частотно-модульований сигнал визначається за формулою 2:

$$Spm(t) = A\cos(\varphi 0 + kSm(t)). \quad (2)$$

Інший вид модуляції – це модуляція Amplitude Shift Keying ASK (далі – ASK), або амплітудна модуляція (далі – AM) [4]. Для кращого розуміння – це сигнал з логічного нуля, коли амплітуда сигналу носія дорівнює нулю, а сигнал логічної одиниці має максимальне значення. Тому, модем перетворює промодульований сигнал у послідовність нулів і одиниць, як показано на рисунку 2, для передачі інформації кореспонденту.

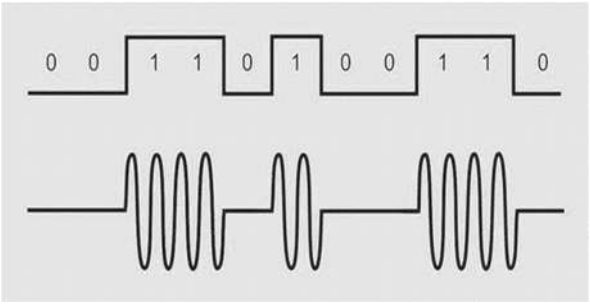


Рисунок 2 – Перетворення аналогово промодельованого сигналу в цифровий

Припустимо, що S(t) – інформаційний сигнал $(S(t) \le 1)$ та $Uc(t)$ – опорний сигнал. Тоді амплітудно-промодельований сигнал буде мати такий вигляд:

$$Uam(T) = Uc(t)[1 + mS(t)], \quad (3)$$

де m – певна константа, що називається коефіцієнтом модуляції. Вищезазначена формула описує сигнал носій $Uc(t)$, промодельований за амплітудою сигналом $S(t)$ з коефіцієнтом модуляції m.

Організувати та забезпечити радіозв'язок можна по-різному. У невибагливих рішеннях використовуються прості радіо модулі. Вони ефективно виконують свою роль передачі за технологією точка-точка. Прикладом може служити зчитування температури з датчика, встановленого на зовнішній поверхні. Основна схема (метеостанція) відправляє по радіоканалу запит на замір температури, а датчик (термометр) відправляє обмірюване значення. Такі модулі мають вбудовану просту логіку і буфери даних. У більш сучасних системах можуть бути механізми підтвердження відправлених пакетів даних (інформацій) та захисту їх за допомогою контрольних сум (поліномів). Це рішення має одну перевагу – низька вартість на апаратному рівні.

У спеціалізованих пристроях, модулі радіозв'язку виконані з використанням спеціально розроблених та стандартизованих протоколів обміну даних. Універсального рішення тут немає, і стандарт радіозв'язку обирається відповідно до вимог програмного забезпечення. На прикладному рівні протоколи обміну даними описуються за допомогою багаторівневих моделей. У кожній з цих моделей існує поділ на нижній фізичний рівень, що включає апаратні рішення, та вищі рівні, які визначаються для конкретного протоколу. У бездротових інтерфейсах фізичний рівень являє собою радіоприймач, який працює в заданому діапазоні частот з певною модуляцією та вихідною чутливістю. Інтерфейс повинен мати можливість модулювати сигнал носій частотного каналу потоком цифрових даних, які передаються, і демодулювати отримані дані.

Стандарти бездротового зв'язку добре задокументовані на законодавчому рівні, тому їхню кодову реалізацію може бути здійснено без проблем. Однак в екстрених умовах воєнного часу це вимагає значних зусиль та затрат часу з боку фахівців у галузі програмування. Тому на ринку доступні готові модулі, що складаються з високочастотної компоненти підключеної до мікроконтролера, який містить прошивку, що виконує більшість функцій, необхідних для встановлення з'єднання, передачі та обробки помилок. Залежно від версії, реалізовано підтримку двох нижніх рівнів: обладнання та доступу до media access control (далі - MAC-каналу) або всього протоколу з елементами прикладного рівня.

Основні переваги частотної модуляції у порівнянні з амплітудною модуляцією:

вища завадостійкість;

енергетично більш вигідна, так як пелюстки корисного сигналу більші за амплітудою, ніж частотний носій.

Основні недоліки частотної модуляції у порівнянні з амплітудною модуляцією:

більш широкий спектр гармонік;

потребує більш складної конструкції модулятора та демодулятора.

Практичні приклади радіомодулів передачі даних.

Якщо потрібно забезпечити з'єднання типу точка-точка [5], оптимальним рішенням будуть прості радіомодулі. Наприклад, модулі на базі мікросхеми nRF24L01, від провідного виробника Nordic Semiconductor, які стали своєрідним стандартом. Своєю популярністю вони завдячують поєднанню невисокої ціни та широких можливостей. Модулі з мікросхемою nRF24L01 широко використовуються в середовищі Arduino, що також сприяє її великій популярності.

Блок-схема ядра модуля nRF24L01 зображено на рисунку 3.

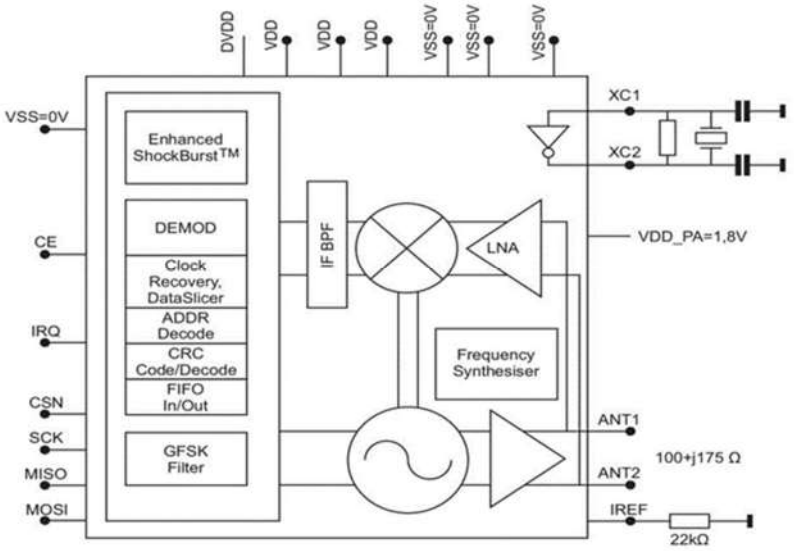


Рисунок 3 – Блок-схема ядра модуля nRF24L01

Пристрій працює у діапазоні ISM 2,4 – 2,5 ГГц з Гаусівською частотною модуляцією. Це модифікована версія частотної модуляції, де потік вхідних даних фільтрується в цифровому вигляді за допомогою фільтра Гауса. Схема має вбудований радіотракт із синтезатором частот, підсилювачем проміжної частоти та високочастотним підсилювачем. Він може діяти як передавач, так і приймач у напівдуплексному режимі. Доступний радіодіапазон поділено на 125 каналів. Час перемикання між каналами менше ніж 200 мКс.

Є два режими роботи модуля nRF24L01:

у першому режимі Shock Burst (прямий) хост (мікроконтролер) записує до внутрішнього буфера дані розміром 256 байт із вибраною швидкістю передачі через послідовний периферійний інтерфейс. Після того, як усі дані були відправлені до внутрішнього буфера, логіка, яка керує процесом, ініціює радіопередачу зі швидкістю 1 Мбіт/с або 250 Кбіт/с. У прямому режимі дані надсилаються зі швидкістю, яку хост відправляє на чіп nRF24L01;

у другому режимі роботи модуля nRF24L01 можна згенерувати контрольний поліном циклічного надлишкового коду апаратно у схемі передавача та підтвердити передачу на основі цього циклічного надлишкового коду у приймачі. Модулі з мікросхемою nRF24L01 досить надійні, тому можуть успішно використовуватися для вирішення складних завдань, незважаючи на відсутність підтримки радіопротоколів.

Є і більш простіші радіомодулі, що працюють на частотах 433 МГц та 868 МГц. Найчастіше, це набір з двох складових – передавача та приймача. Проте цей комплект має суттєві обмеження функціональності, оскільки у такій конфігурації неможливо реалізувати двосторонню передачу даних (сигналу). В них використовувалася амплітудна модуляція.

Висновки й перспективи подальших досліджень

В даній статті проведено аналіз особливостей побудови та застосування радіомодуля nRF24L01 у техніці військового призначення. За результатами аналізу технологій побудови пристроїв Інтернету речей обґрунтовано доцільність використання безпровідних технологій та встановлено, що для обміну даними в таких системах у всьому світі надаються неліцензовані радіочастотні діапазони, які можуть використовуватися без оформлення спеціального дозволу і абсолютно безкоштовно за умови дотримання вимог щодо ширини смуги частоти, випромінюваної потужності. А отже впровадження даної технології надасть змогу зменшити собівартість побудови Інтернету речей у військових цілях.

Також в статті розглянуто основні методи розширення спектру частот для адаптивної селекції каналів зв'язку для пристроїв Інтернет речей, їх недоліки та переваги.

Подальшими науковими дослідженнями буде відпрацювання науково-дослідної роботи та розроблення дослідно-конструкторської роботи щодо застосування радіомодуля nRF24L01 на зразках військової техніки.

Список бібліографічних посилань

1. Білинський Й. Й., Огородник К. В.,. Юкиш М. Й. Електронні системи. Вінниця : ВНТУ, 2018. 208 с. **2. Кузьмин І. В., Кедру В. А.**Основи теорії інформації та кодування. Київ : Вища школа, 2003. 220 с. **3. Бойко В.І., Гурій А. М., Жуйков В. Я. та ін.** Основи технічної електроніки: У 2 кн. Кн.2 Схемотехніка: підручник. Київ: Вища школа, 2007. 510 с. **4. Овчарук А. А., Барась С. Т., Овчарук Т. І.** Квадратурна амплітудна модуляція зі змінним значенням частоти-носія. *Восточно-Европейский журнал передовых технологий.* 2011. № 4/9. С. 47–51. **5. Рябенький В. М., Жуйков В. Я., Гулий В. Д.** Цифрова схемотехніка : навч. посібник. Львів : «Новий світ-2000», 2009. 736 с. **6. Сайко В. Г., Оксіюк О. Г., Дікарєв О. В.** Основи цифрового оброблення сигналів в системах цифрового радіозв'язк : навч. посібник. Київ : ДУТ, 2016. 128 с. **7. Бабак В.П.** Обробка сигналів у радіоканалах цифрових систем передавання інформації: Навч. посібник за заг. ред. чл.-кор. НАН України В.П. Бабака. Київ : Книжкове вид-во НАУ, 2005. 476 с. **8. Кривуца В. Г., Барковський В. В., Беркман Л. Н.** Математичне моделювання телекомунікаційних систем: навчальний посібник. Київ : Зв'язок, 2007. 270 с.

CONSTRUCTION FEATURES AND RECOMMENDATIONS FOR USE nRF24L01 RADIO MODULE IN MILITARY TECHNOLOGY

Neshcheret Ivan [1]
Zlobin Kirilo [1]
Tsykalo Yurii [2]

[1] ***Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine,***
[2] ***Military unit A0707, Haisyn, Ukraine***

Today, receiving and transmitting equipment has undergone significant development, mostly due to digitalization. Digital technology is becoming increasingly popular when receiving and transmitting information. Eight-bit microcontrollers (for example, nRF24L01) have sufficient data processing speed. Having provided analog-digital conversion, possibilities in programming data of microcontrollers, it is possible to implement a transceiver. A series of products from the leading Nordic Semiconductor Corporation contain embedded high-performance multiplexers that are connected to the flash memory (core) of an industry-standard 8052 microcontroller (such as the nRF24L01), and support multiple serial port configuration standards. These products are the first integrated circuits that can be called "intelligent transceivers" for data collection and processing systems on a single chip. At the first stage, the processing of physical signals consists in the need to obtain the information contained in them. This information is available in the amplitude of the signal, in the frequency or spectral composition, in the phase or in the relative time dependences of several signals. In some cases, it is desirable to change the format of the information contained in the signal packet. For example, the format change occurs during the transmission of an audio signal in a telephone system with multiple access and frequency division. In the case of digital communication, the analog audio information is first converted to digital using an analog-to-digital converter. Digital information representing individual audio channels is multiplexed (time division multiple access (TDMA)) and transmitted over a serial digital communication line. The purpose of the article is to conduct an analysis of construction features and provide a recommendation for the use of the nRF24L01 radio module in military equipment, as well as a comparison of the basic principles and standards of modeling signals and interference in electronic systems, principles of discretization, signal coding.

Keywords: *radio communication, amplitude modulation, frequency modulation, wireless communication, communication device, satellite navigation, Internet of things.*

References

1. Bilinsky, Y. Y. and Ogorodnyk, K. V., (2018). *Electronic systems.* Vinnytsia: VNTU. **2. Kuzmin, I. V., Kedru, V. A.,** (2003). *Basics of information theory and coding.* Kyiv: Vysha Shkola. **3. Boyko, V. I**. **Gurii, A. M., Zhuykov, V. Y. and others,** (2007). *Basics of technical electronics.* Kyiv: Higher School. **4. Ovcharuk, A. A., Baras, S. T., Ovcharuk, T. I.,** (2011). Quadrature amplitude modulation with a variable value of the carrier frequency. *Eastern-European journal of advanced technologies*, 4/9, 47-51. **5. Ryabenkyi, V. M., Zhuykov, V. Y., Guly, V. D.,** (2009). *Digital circuitry:* teacher. Manual. Lviv: «New World-2000». **6. Saiko, V. G., Oksiyuk, O. G., Dikarev, O. V.,** (2016). *Fundamentals of digital signal processing in digital radio communication systems.* Kyiv : DUT. **7. Babaka, V. P.,** (2005). Signal processing in radio channels of digital information transmission systems. Kyiv : NAU. **8. Kryvutsa, V. G., Barkovsky, V. V., Berkman, L. N.,** (2007). Mathematical modeling of telecommunication systems. Kyiv : Zvyazok.

DOI:**10.33099/2311-7249/2023-47-2-96-112**

УДК 621.396.4

Машталір Вадим Віталійович *(доктор історичних наук, професор)* [1]
Жук Олександр Володимирович *(доктор технічних наук, доцент)* [1]
Міненко Людмила Миколаївна *(доктор філософії)* [1]
Артюх Сергій Григорович [2]

[1] ***Національний університет оборони України, Київ, Україна***
[2] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***

КОНЦЕПТУАЛЬНІ ПІДХОДИ ЗАСТОСУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ АРМІЯМИ ПЕРЕДОВИХ КРАЇН СВІТУ

Війна рф проти України спонукала до об'єктивного оцінювання існуючих мереж зв'язку і систем командування, налаштованих за нормами концепції C4ISR, що означає «Command and Control, Computers, Communications, Intelligence – Surveillance – Reconnaissance» (Командування і контроль, Зв'язок, Комп'ютеризація, Розвідка – Спостереження – Рекогносцировка) та являє собою інтегрований підхід до керування й координації військових операцій у сучасних війнах. На сьогодні ця концепція, через кібер та інші загрози розширилася і містить вже сім сталих компонентів – «Command and Control, Computers, Communications, Intelligence – Surveillance – Reconnaissance, Combat systems, Cyber, Collaboration,» (Командування і контроль, Комп'ютеризація, Зв'язок, Розвідка – Спостереження – Рекогносцировка, Співпраця між державним і приватним секторами, Оборонна кібербезпека, Співпраця та оперативна сумісність з партнерами і союзниками). Для найменування цього виду системи застосовується абревіатура C7ISR. Крім того, успішне функціонування цієї системи забезпечується додатковими можливими факторами і засобами «Convergence. Cohesion. Combine, Co-operation, Coordination, Continuous, Connected networks, Multi-clouds» (узгодженість, згуртованість, взаємодія, поєднання, координація, постійність, використання пов'язаних мереж і мультихмарного середовища тощо). Тому використання у військовій сфері нових технологій і надалі породжуватиме варіації таких систем, їхніх назв та абревіатур. За своїм призначенням такі мережі зв'язку і системи командування мають невідкладно реагувати на масовані кібератаки, ракетні удари та інші загрози. Під час російсько-української війни, використання передових технологій НАТО, зокрема завдяки потенціалу C4ISR, і подальших її модифікацій, дало змогу викрити нарощування ворожих військ на україно-російсько-білоруському кордоні, та опорні пункти агресора. Саме гнучкі автоматизовані системи управління, що своєчасно реагують на вплив різноманітних зовнішніх факторів, дають змогу українським військовим швидко пристосуватися до мінливої ситуації на полі бою. Система C4ISR, із гнучким застосуванням додаткових факторів і засобів (наприклад, C5ISR, C6ISR, C7ISR) та її архітектура оптимально адаптується до середовища функціонування і забезпечує збір й аналіз багатовимірної розвідувальної інформації на суходолі, у повітрі та водному просторі, коли є значна кількість різного виду сигналів: електронних, електрооптичних, інфрачервоних і супутникових. Це допомагає покращити процес прийняття оперативних рішень, гарантує миттєве й ефективне їх доведення до виконавців, забезпечує здатність до супроводу, здійснює контроль і, за потреби, регулює виконання поставлених бойових завдань. Ключовим інструментом для одержання, опрацювання і пересилання даних, що забезпечують належне функціонування систем C4ISR (C5ISR, C6ISR, C7ISR) є мобільні бездротові сенсорні мережі (сенсорні системи). Маємо констатувати, що російсько-українська війна, актуалізувала важливість використання сенсорних систем з метою отримання розвідувальної інформації та її комплексного аналізу для забезпечення ефективного прийняття рішень командувачами (командирами). Здатність до швидкого розгортання, самоорганізація і відмовостійкість є ключовими особливостями бездротових сенсорних мереж, що роблять їх надійним інструментом для ефективного виконання оперативних завдань. Метою статті є аналіз тактико-технічних характеристик, особливостей функціонування і прикладного застосування бездротових сенсорних мереж армій передових країн світу для напрацювання фахових рекомендацій стосовно подальшого їх впровадження в сфері безпеки та оборони України, а також – гарантування інноваційності розроблення вітчизняних зразків гнучких автоматизованих систем управління в збройних силах нашої держави. Для науково-обґрунтованого написання статті застосовано методи аналізування, синтезу, прогнозування. Зазначений методичний інструментарій дав змогу концептуально охарактеризувати автоматизовані системи управління військами НАТО (C4ISR і розширену C7ISR), розкрити тактико-технічні характеристики сенсорних систем спеціального

(військового) призначення, особливості їх функціонування, узагальнити призначення мобільних бездротових сенсорних мереж оперативного рівня, а також – розробити рекомендації щодо впровадження таких систем у вітчизняній військовій сфері та їхнього подальшого інноваційного розвитку. В статті проаналізовано Стратегічний оборонний бюлетень України в частині необхідності тотальної цифровізації Міністерства оборони і Генерального штабу Збройних Сил України та застосування бездротових сенсорних мереж для розроблення гнучких автоматизованих систем управління у військовій сфері, дано концептуальну характеристику стандарту військового керування у НАТО, проведено аналіз провідних наукових досліджень і публікацій стосовно завдань управління, використовуючи сенсорні системи, сучасного стану мобільних бездротових сенсорних мереж, а також перспектив їх розвитку і доцільність застосування для побудови інноваційних автоматизованих систем управління в Збройних Силах України. Висвітлено тактико-технічні характеристики, описано конструктивні ознаки та виділено особливості функціонування сенсорних систем спеціального (військового) призначення. Зокрема, розглянуто сенсорні системи AUSSNet, Vigilis, REM-Sense, AN/PRS-9A BAIS, BAIS-i, Reconnaissance (ISR) UGS, Pathfinder, Claw, Forester, Camel (США), Mineseeker (Великобританія), Carabas II, Flexnet (Швеція), Primrose (Ізраїль). З'ясовано, що в складі вузлів сенсорних систем використовуються акустичні, електрооптичні, інфрачервоні, магнітні, температурні, акселометричні та сейсмічні датчики. Узагальнено призначення і напрями застосування та сформульовано рекомендації щодо використання бездротових сенсорних мереж у військовій сфері України, зокрема, для побудови гнучких автоматизованих систем управління збройними силами. Проаналізоване сприяє поглибленню наукових знань стосовно технологічних, архітектурних, конструктивних особливостей окремих вузлів (модулів) сенсорних систем з метою їх удосконалення та ефективного впровадження у військовій сфері, що формується на основі принципів і стандартів держав-членів НАТО. Прикладне використання мобільних бездротових сенсорних мереж, якісно покращує характеристики автоматизованої системи C4ISR та її подальших модифікацій і забезпечує її оптимально-адаптовану інтеграцію до автоматизованих систем управління вітчизняними оборонними ресурсами.

Ключові слова: *Стратегічний оборонний бюлетень, гнучка автоматизована система управління, C4ISR, сенсорні системи, бездротові сенсорні мережі, тактико-технічні характеристики, передові технології створення сенсорних систем.*

Вступ

Постановка завдання в загальному вигляді. Указом Президента України від 17 вересня 2021 року № 473/2021 було затверджено Стратегічний оборонний бюлетень України [10; 11]. Цим документом унормовано основні напрями реалізації національної воєнної політики в контексті всеохоплюючого захисту України. Крім того, у ньому встановлено Перспективну модель збройних сил нашої держави та інших складових сил оборони, конкретизовано вимоги до її побудови. У цьому зв'язку, окреслено візію й місію сил оборони, затверджено мету і стратегічні цілі розвитку на період до 2030 року. Визначено основні завдання і заходи, що після їх реалізації та отримання очікуваних результатів, мають охарактеризувати ступінь досягнення головних спроможностей наміченого.

Водночас, Стратегічним оборонним бюлетенем України схвалено, що одним із першорядних напрямів реалізації воєнної політики України є побудова системи об'єднаного керівництва силами оборони та військового управління у Збройних Силах України, яка має здійснюватися відповідно до передового досвіду, принципів і стандартів держав-членів НАТО [11]. З цією метою, інноваційному розвитку підлягають форми та способи застосування сил і засобів розвідки, її спроможності поєднуються в єдиному розвідувально-інформаційному середовищі, а процеси добування (збору), обробки, аналізу (відображення) та доведення розвідувальної інформації реалізуються з необхідним рівнем автоматизації. Такі процеси здійснюються в контексті раніше впровадженої та успішно функціонуючої автоматизованої системи оперативного (бойового) управління, зв'язку, цифровізації, розвідки та спостереження (Command and Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (далі – C4ISR)), а також її подальших модифікацій [9; 14; 15].

За таких умов, побудову системи кібероборони має бути спрямовано на набуття необхідних спроможностей суб'єктами підготовки, здійснення заходів кібероборони, створення і розвиток сил, засобів та інструментів протиборства в кіберпросторі (через кіберпростір), які забезпечать формування необхідного потенціалу сил оборони для стримування і відбиття можливої воєнної агресії в кіберпросторі. Через це, для протидії силам і засобам ворога необхідно реалізувати комплексні підходи стосовно застосування радіоелектронної боротьби та взаємодії у кіберпросторі, за умови, що дистанційний безконтактний вплив на противника визначатиметься як основний спосіб досягнення цілей бою та операції.

Заради досягнення сформованої мети пропонується імплементувати на практиці низку стратегічно важливих цілей. Зокрема, «стратегічна ціль 1» передбачає формування ефективного оборонного менеджменту і системи об'єднаного керівництва силами оборони та військового

управління у Збройних Силах України, що здійснюються на засадах демократичного цивільного контролю, інших принципах і стандартах НАТО. Вказана ціль обумовлює виконання «завдання 1.5» «Цифровізація діяльності та впровадження сучасних інформаційних технологій, у тому числі електронних комунікацій, у сфері оборони». В свою чергу, «стратегічна ціль 5» передбачає набуття необхідної якості інтегрованих оперативних (бойових та спеціальних) спроможностей сил оборони, що повинні забезпечувати стримування, стійкість і відсіч збройної агресії проти України, протидіяти гібридним загрозам. Досягнення цілі має бути здійснене шляхом реалізації «завдання 5.5» «Створення ефективної системи об'єднаної розвідки сил оборони з урахуванням принципів і стандартів НАТО» [11]. Для досягнення означених цілей (кожної окремо), проаналізований нормативний документ містить перелік спеціальних заходів. Їхнє фахове послідовне та/або паралельне виконання забезпечує синергійне здобуття бажаних результатів щодо всебічного захисту в цій сфері. Разом із тим, з метою практичного провадження Стратегічного оборонного бюлетеня України, розробляються і реалізуються державні цільові програми, а також інші програмні та планувальні документи і проєкти.

Як відомо, однією із найважливіших вимог для досягнення переваги над противником є забезпечення оперативною інформацією військ (сил) в умовах інтенсивних бойових дій. Таку перевагу можна здобути лише у випадку, коли оперативна (бойова) інформація про поточну обстановку доступна всім ланкам управління, від окремого військовослужбовця до керівника вищого рівня. У зв'язку з цим, сьогодні, активно проводяться експерименти за напрямом розроблення мобільних бездротових сенсорних мереж, що мають здатність приймати і передавати розвідувальну інформацію про стан супротивника, а також надавати зазначену інформацію певним споживачам, гарантуючи ефективне функціонування гнучких автоматизованих систем управління Збройними силами України [16]. Тому, обраний нами напрям наукового дослідження є достатньо актуальним завданням, що сприятиме інноваційному розвитку національних сенсорних систем військового призначення та, за потреби, використання на практиці закордонних аналогів, заради формування дієво-змінної оборонної структури нашої незалежної держави.

Аналіз останніх досліджень і публікацій. У роботі [7], проведено аналіз завдань управління сенсорними мережами, а також запропоновано функціональну модель системи управління сенсорною мережею, обґрунтовані принципи її побудови, структура та функції. У статті [3] розглядаються перспективи розвитку тактичних сенсорних мереж, здійснено класифікацію і вимоги, що висуваються до них. Крім того, стаття містить результати аналізу проблем розроблення таких мереж і їх розвитку в сучасних умовах. У дослідженні [8] виконано аналітичний огляд сучасних наукових праць стосовно стану мобільних бездротових сенсорних мереж (далі – БСМ), а також надано загальне визначення бездротових сенсорних мереж з мобільними сенсорами та наводиться класифікація їхніх архітектур [6]. Водночас, детального аналізування тактико-технічних характеристик сенсорних систем, що розглянуто у цій статті, у тому числі їхніх конструктивних особливостей та унікальних аспектів функціонування, з урахуванням специфіки прикладного застосування для побудови гнучких автоматизованих систем управління у військовій сфері, досі не проводилося.

Метою статті є аналіз тактико-технічних характеристик, особливостей функціонування і прикладного застосування бездротових сенсорних мереж армій передових країн світу з метою напрацювання фахових рекомендацій стосовно подальшого їх впровадження в сфері безпеки та оборони України, а також для гарантування інноваційності розроблення вітчизняних зразків гнучких автоматизованих систем управління в збройних силах нашої держави.

Виклад основного матеріалу дослідження

17 вересня 2021 року Указом Президента України № 473/2021 затверджено Стратегічний оборонний бюлетень України [10; 11], чим забезпечено продовження стійкого розвитку безпеки та обороноздатності нашої незалежної держави, у тому числі й з питань подальшого вдосконалення структури об'єднаного керівництва силами оборони та військового управління у Збройних Силах України, яка має здійснюватися відповідно до передового досвіду, принципів і стандартів Північноатлантичного блоку. По суті, на порядку денному залишилися завдання інноваційної, оптимальної та адаптованої до умов війни з рф розбудови гнучких автоматизованих систем управління, що використовують технологію C4ISR, та її варіації, і мобільних бездротових сенсорних мереж (сенсорних систем) [1]. Так, серед заходів означеного спрямування визначено:

побудова Об'єднаної мережі оборони, основу якої становитимуть електронна комунікаційна мережа та інформаційні системи Міністерства оборони України та Збройних Сил України;

створення та розвиток мереж операцій, побудованих на сучасних цифрових засобах, якими буде переоснащено польову систему зв'язку Збройних Сил України, розроблення нових (удосконалення існуючих) систем бойового управління;

стандартизація, оптимізація та взаємосумісність інформаційних систем сил оборони;

інтеграція існуючих систем спеціального зв'язку сил оборони в єдину захищену систему зв'язку сил оборони;

автоматизація процесів управління військами і зброєю, оборонними ресурсами, розвідкою, логістикою, медичним та іншими видами забезпечення. Упровадження електронного документообігу, цифровізація документів обліку особового складу;

оптимізація системи захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Силах України;

набуття спроможностей системою управління розвідкою Збройних Сил України у трирівневій вертикалі керівництва;

реалізація наявних та створення нових спроможностей військових частин (підрозділів) розвідки Збройних Сил України;

автоматизація процесів збору і обробки розвідувальних відомостей (даних) та управління силами і засобами розвідки з урахуванням принципів і стандартів НАТО;

забезпечення військових частин (підрозділів) розвідки Збройних Сил України новітніми (модернізованими) технічними засобами розвідки [10; 11].

Як можна пересвідчитися, практична ефективна і результативна реалізація вище перерахованих заходів безпосередньо та/або опосередковано залежить від технологічної якості побудови гнучких автоматизованих систем управління і мобільних бездротових сенсорних мереж та їх фахового оптимального, адаптованого й продуктивного застосування в середовищі бойових дій. За таких умов, варто зазначити, C4ISR – це система оперативного (бойового) управління, зв'язку, розвідки та спостереження, що діє за стандартами військового керування НАТО, яка дозволяє досягти інформаційної переваги над ворогом і трансформується в бойову могутність завдяки поєднанню роботи підрозділів й усіх розвідувальних спроможностей в єдиний цифровий дієвий простір. Фактично, це гнучка автоматизована система управління військами, що забезпечує:

управління військами (Command and Control);

належну роботу підрозділів зв'язку (Communications);

функціонування автоматизованої системи управління і зв'язку (Computers),

роботу служби розвідки (здобуття інформації; виконання всіх процесів, що супроводжують отримання, обробку і розповсюдження добутої інформації на командні пункти) (Intelligence);

спостереження (Surveillance),

рекогносцировку (військову розвідку) (Reconnaissance).

На сьогодні, через розширення різних викликів, спровокованих гібридними загрозами і провокативними кібератаками, ця система модернізована і, крім означеного, здатна додатково забезпечувати:

співпрацю між державним і приватним секторами (Combat systems);

оборонну кібербезпеку (Cyber);

співпрацю та оперативну сумісність з партнерами і союзниками (Collaboration).

Крім того, можуть застосовуватися додаткові фактори і засоби: узгодженість (Convergence), згуртованість (Cohesion), взаємодія (Combine), поєднання (Co-operation), координація (Coordination), постійність (Continuous), використання пов'язаних мереж (Connected networks) і мультихмарне середовище (Multi-clouds) [15, 14].

Сформовані за вимогами системи C4ISR, чи одного з її модифікованих варіантів, мережі (канали інфокомунікаційного зв'язку), збирають значні обсяги даних з безлічі датчиків, баз даних та інших джерел по всьому світу. Отримана таким чином інформація узагальнюється, обробляється і безпечно передається авторизованим користувачам. Отже на практиці, технологічною основою системи оперативного (бойового) управління, зв'язку, розвідки та спостереження або її модифікацій є реалізація доктрини, так званої, мережецентричної війни, а по суті, поєднання джерел інформації в одну прозору дигіталізовану систему. За таких умов, швидкість прийняття поінформованих і зважених рішень командирами під час бойових операціях зростає у рази. До того ж така система дозволяє зберігати керованість навіть у випадку знищення пунктів управління. Водночас, за оцінками військових аналітиків, запровадження доктрини мережецентричності та принципів цієї системи у війську, дає змогу зменшити видатки на артилерійські снаряди до 20 разів і, головне, зменшити втрати особового складу до 10 разів [12].

Отже, знання концепцій, форм і способів бойових дій у сучасних війнах, зокрема, з урахуванням досвіду відсічі й стримування збройної агресії рф в Україні, а також дослідження нових військових доктрин, свідчить про посилення значимості гнучкої автоматизації процесів управління в країнах світу з розвиненою воєнною сферою. В цьому контексті інформаційні війни набули стратегічного значення і перебувають в центрі уваги національних стратегій. Пріоритетом стає здобуття інформаційної переваги над противником, що втілюється через використання передових технологій для створення мобільних сенсорних систем спеціального призначення. Саме до таких систем слід віднести і БСМ, що виконують функцію отримання та надання розвідувальної інформації про противника, а також подання її органам військового управління і розподілу між засобами протидії та ураження [5]. Тому, на практиці, більшість уваги зосереджена на бездротових сенсорних мережах, що стають основою для побудови інноваційних гнучких автоматизованих систем управління у військовій сфері.

Сьогодні, БСМ становлять розподілену сенсорну систему, що самоорганізується та складається з великої кількості датчиків (сенсорів) і пристроїв виконання, об'єднаних між собою бездротовим зв'язком [2]. Покриття такої мережі

може охоплювати від кількох метрів до декількох кілометрів. Завдяки здатності до ретрансляції повідомлень між різними елементами, БСМ можуть застосовуватися військовими для виконання низки специфічних завдань, а саме: моніторинг розташування противника, його кількості та характеру дій; збір розвідувальної інформації на місцевості; використання в системах наведення інтелектуальних снарядів; визначення положення необхідних об'єктів (подій); забезпечення захисту своїх підрозділів; моніторинг державного кордону в будь-якій місцевості та за будь-яких умов [4].

Для всебічного огляду сучасного стану БСМ, варто розглянути передовий досвід розроблення, впровадження і застосування таких сенсорних систем, висвітлити їхні функціональні особливості, а також зробити висновки щодо їх ефективного впровадження в сфері військових технологій, особливо, під час побудови гнучких автоматизованих систем управління з метою забезпечення оперативного командування. Маємо констатувати, військовим керівництвом Збройних Сил (далі – ЗС) США здійснюється регулярне та послідовне переведення військових частин і органів управління на бригадну структуру з їх одночасним оснащенням перспективними системами озброєння, зв'язку, розвідки та управління. Зокрема, надається значна увага розвитку та впровадження БСМ. Наведемо окремі приклади такої конструктивної роботи.

Автономна підводна система нагляду на основі бездротових сенсорних мереж (Autonomous Underwater Surveillance Sensor Network (AUSSNet)) корпорації L3 Technologies Autonomous (США) [13], являє собою БСМ, що призначена для прямого розгортання в підводних зонах стратегічного значення. Мобільна сенсорна система може збирати, обробляти, зберігати та дискретно передавати дані підводного спостереження через супутникові та/або гідроакустичні телеметричні канали на землю, повітря, космос або об'єкти в морі для підвищення ситуативної обізнаності. Означена система швидко розгортається і забезпечує можливість постійного підводного спостереження протягом тривалого періоду в будь-якому водному регіоні. Вона застосовується під час операцій спеціального призначення, моніторингу стану елементів кораблів, для охорони гаваней, підтримки морських десантних (наступальних) операцій, протидії підводним човнам, захисту підводної та критичної інфраструктури, охорони державного кордону. AUSSNet, як автономна бездротова сенсорна мережа, має здатність до самовідновлення, самоорганізації і можливості багаторазового використання. Дані спостереження передаються на низьких частотах (менше 500 Гц) з множини підводних сейсмоакустичних модулів, розташованих на морському дні (рис. 1).

Усі отримані дані від підводного сейсмоакустичного модуля записуються локальною станцією, що є основною для певної зони сенсорної мережі. В задані інтервали часу (або за подією), локальна станція підіймає на морську поверхню прив'язаний буй-шлюз, що передає зібрані дані до надводної базової станції управління і контролю.

Тактико-технічні характеристики сенсорної системи AUSSNet:

підводний сейсмоакустичний модуль, вагою 0,4 кг – 3 шт.;

локальна станція з буєм-шлюзом – 1шт.;

надводна базова станція управління та контролю – 1шт;

діапазон частот – від 10 кГц до 250 кГц;

робоча температура – від – 30°С до + 65°С;

матеріал – Titan GR2/5, надійність відповідає вимогам стандартного тесту електронного обладнання для оцінки надійності (стандарт «Військове керівництво зі стандартного тесту електронного обладнання для оцінки надійності» (MIL-HDBK-217));

електромагнітна сумісність відповідає стандартним вимогам до інтерфейсу Міністерства оборони США для управління характеристиками електромагнітних завад підсистем і обладнання («Характеристики електромагнітних завад і вимоги до обладнання» (MIL-STD-461E));

маркування відповідає вимогам стандарту «Військове маркування MIL STD 129 для транспортування і зберігання», що використовується для однакового маркування військової техніки та предметів постачання, що перевозяться морськими суднами.

Рисунок 1 – Підводний вузол сенсорної системи AUSSNet

Також корпорацією L3 Technologies Autonomous розроблено сенсорну систему морських зон Vigilis (США) [13], що призначена для спостереження за навколишнім морським простором. Ця сенсорна система є спеціалізованою БСМ, що розгортається у морських і прибережних зонах й забезпечує безпеку та здійснює моніторинг

навколишнього середовища з метою захисту морських об'єктів і критичної наземної інфраструктури (порти, вантажні термінали, субмарини-розвідники й атомні станції). Крім того, сенсорна система Vigilis застосовується для управління трафіком суден, під час проведення операцій спеціального призначення, моніторингу стану елементів кораблів, охорони гаваней, підтримки морських десантних операцій, протидії підводним човнами, захисту підводних сил, охорони державного кордону, захисту критичної інфраструктури.

Зазвичай, означену сенсорну систему розгортають у центрі управління трафіку суден і морських районів стратегічного значення, забезпечуючи комплексний набір інструментів для збору, обробки, відображення та аналізу даних моніторингу. На спеціальному командному пункті (далі – КП), що обладнаний інструментами сенсорної системи Vigilis, оператор має можливість виконувати такі дії:

конфігурувати і переглядати загальний стан зон моніторингу, пристроїв, що розгорнуті в них та зв'язків між ними;

здійснювати моніторинг трафіку суден в межах певної області за допомогою відображення карти в режимі реального часу;

віддалено керувати пристроями сенсорної системи;

виявляти і класифікувати порушення;

обмінюватися даними з іншими КП та суднами;

виконувати системні заходи з адміністрування та обслуговування сенсорної системи.

Особливості основних складових сенсорної системи Vigilis наведено в таблиці 1.

Таблиця 1

Особливості складових сенсорної системи Vigilis

Складова	Характеристика
Системи автоматичної ідентифікації (AIS)	Суднові та берегові системи мовлення, що працюють у морській смузі ультракоротких хвиль (далі – УКХ).
Радари	Для виявлення малорозмірних цілей і спостереження за прибережними територіями. Для інтегрованого перегляду зон спостереження та уникнення «сліпих зон» використовується декілька радарів.
Системи зв'язку	Ідентифікація та трекінг на великих відстанях за допомогою використання супутникових систем.
Камери	Денні і нічного бачення, великої дальності, зі стабілізацією та без. Особливості: гнучкі операторські дисплеї та засоби керування для взаємодії кількох камер; взаємодія з продуктами різних постачальників; автоматичне відстеження цілей з найвищим пріоритетом.
Трекінг суден і активів	Судна, оснащені інструментами системи Vigilis надають дані про позицію судна, швидкість руху та напрямок.

Для збільшення рівня ситуативної обізнаності у морському середовищі, сенсорні системи Vigilis можна поєднувати з вже існуючими. Гнучка архітектура сенсорної системи дає змогу розподіляти функції управління мережею, а комплексний набір інструментів адаптується до різних типів даних та їх швидкості, передає дані вузлів, генерує тривоги/сповіщення, підтримує резервне копіювання і відтворення для ситуацій, що розвиваються, а також зберігає дані для аналізу наслідків інцидентів і реконструкції подій. Сенсорна система Vigilis забезпечує:

гнучку, відкриту архітектуру з використанням компонентів готових комерційних систем (Commercial Off-The-Shelf systems (COTS));

комплексне керування судноплавними шляхами;

обробку та узагальнення даних від різних типів датчиків і джерел;

автоматичну та ручну класифікацію подій;

відображення даних про стан судна в реальному часі через налаштовані фони графіків електронних навігаційних карт;

оповіщення користувача за відповідним алгоритмом про події у визначеному регіоні;

гнучке відображення кількох камер, керування ними та записами;

повну реєстрацію подій у службі відображення Google Earth™;

масштабовану архітектуру;

відображення електронних навігаційних карт за стандартом (Interactive S57/S63 Electronic Navigational Charts (Interactive S57/S63 ENCs));

можливість моделювання роботи за віртуальними морськими сценаріями для навчань.

У свою чергу, REM-Sense (США) є бездротовою сенсорною мережею, що забезпечує миттєвий обмін інформацією між пристроями виявлення руху, за принципом «Бачить один – знають всі» [10]. Ця мережа є набором тактичних, дистанційно керованих наземних сенсорів (Unattended Ground Sensors (далі – UGS)), що пасивно виявляють і класифікують живу силу й транспортні засоби противника у помірному діапазоні вдень і вночі. Універсальні компоненти REM-Sense є сумісними з багатьма військовими та комерційними сенсорними системами, а програмне забезпечення, що постійно оновлюється, може бути адаптоване для підтримки різних операцій. Означена сенсорна система перевірена в широкому спектрі тактичних операцій по всьому світу. В межах програми ЗС США Programs of Record, ці бездротові сенсорні мережі сумісні з іншими сенсорними системами та утворюють велику структуру для покращення

ситуаційної обізнаності та захисту військових підрозділів. Вони містять у собі:

системи запобігання вторгнень BAIS (Battlefield Anti-Intrusion System) (AN/PRS-9 та AN/PRS-9A);

сенсори поля бою з дистанційним моніторингом REMBASS-II (Remotely Monitored Battlefield Sensor System-II) (AN-GSR-8 (V);

компоненти множини автономних наземних сенсорів Unattended Ground Sensor Set (AN/GSQ-257), що входить до складу Тактичної дистанційної сенсорної системи (Tactical Remote Sensor System (далі – TRSS) морської піхоти США.

Сенсорна система виявлення вторгнень на полі бою (AN/PRS-9A Battlefield Anti-Intrusion System (далі – AN/PRS-9A BAIS)) (США) (рис. 2) [13].

Рисунок 2 – Сенсорна система виявлення вторгнень на полі бою AN/PRS-9A BAIS

Означена сенсорна система забезпечує більш якісне виявлення вторгнень і загроз та їх класифікацію. Вона призначена для використання тактичними підрозділами, з метою забезпечення охорони особового складу та оборонних позицій. Бездротова сенсорна мережа AN/PRS-9A BAIS застосовується під час операцій спеціального призначення, охорони державного кордону, операцій протидії незаконному обігу наркотиків. Вона складається з одного ручного монітору/передавача і базового набору з трьох сейсмоакустичних сенсорів, що забезпечують приймання / передавання радіосигналів, здійснюють локальне та дистанційне бездротове програмування (табл. 2).

Таблиця 2

Особливості складових сенсорної системи виявлення вторгнень на полі бою AN/PRS-9A BAIS

Складова	Характеристика
Сейсмоакустичний сенсор / приймач-передавач	Основний датчик з функцією інфрачервоного та магнітного виявлення. Надає інформацію про клас цілі, що забезпечує її класифікацію за алгоритмом на основі комбінованих сейсмічних і акустичних сигнатур. Налаштовується як радіо-ретранслятор.
Ручний монітор/ передавач	Відображає інформацію з сенсорів на LCD-дисплеї або виводить повідомлення на інші пристрої. Дає змогу програмувати сенсори бездротовим способом як локально, так і віддалено. Підтримка повідомлень сенсорних мереж: BAIS (SAS & S/T) (29-біт); TRSS (29-біт, 285-біт); REM/IREM/REM-II (29-bit, 101-bit); LKMD (детектор руху) сигналізації.

Слід розуміти, що кожен датчик означеної бездротової сенсорної мережі може бути налаштований як звичайний автономний вузол, радіо-ретранслятор або комбінований вузол-ретранслятор. Ця можливість дає змогу подолати радіочастотні завади в зоні дії, розширюючи діапазон радіочастот для забезпечення надійного та стійкого зв'язку. Вона має невеликий розмір, вагу (до 5 кг) і легко транспортується однією особою в спеціальному рюкзаку. Тактико-технічні характеристики сенсорної системи AN/PRS-9A BAIS:

три сейсмоакустичні сенсори розміром 19,3×10,6×5,3 см і вагою 0,6 кг;

один ручний монітор/передавач розміром 16,5×10,6×10,6 см і вагою 0,6 кг;

живлення забезпечується від акумуляторної батареї (далі – АКБ) з номінальною напругою 9В, або від зовнішнього джерела;

тривалість автономної роботи: сенсора – до 130 діб (за 1000 спрацювань на день), ручного монітора – до 19 діб;

кількість каналів – 599;

забезпечує підтримку до 255 сенсорів у мережі;

двосторонній радіозв'язок – SEIWG-005C, діапазон від 138 МГц до 153 МГц;

робоча температура – від – 40°С (– 20°С для монітору) до + 71°С;

стійка до вітру зі швидкостями 20 м/год (пил), 40 м/год (пісок).

Сенсорна система виявлення вторгнень на полі бою AN/PRS-9A BAIS має вбудований пристрій встановлення та запобігання помилок, програмне забезпечення, що оновлюється, стійка до зламу, може бути інтегрована до бездротових сенсорних мереж вищих рівнів. Додаткові можливості цієї сенсорної системи щодо виявлення цілей наведено в таблиці 4.

Водночас, інша модифікація цього типу бездротових сенсорних мереж BAIS-і (США) забезпечує якісніше встановлення нападу і загроз [13], їх класифікацію та характеризується більш низькою вартістю порівняно з попередньою версією (рис. 3).

Рисунок 3 – Сенсорна система виявлення вторгнень на полі бою BAIS-i

Вона розроблена для військових підрозділів з метою забезпечення охорони своїх сил, оборонних позицій та спостереження за державним кордоном. Фактично, сенсорна система BAIS-i застосовується під час операцій спеціального призначення, охорони державного кордону, операцій протидії незаконному обігу наркотиків. Означена сенсорна система складається з одного ручного монітора/передавача і базового набору невеликих сенсорів (табл. 3).

Таблиця 3

Особливості складових сенсорної системи виявлення вторгнень на полі бою BAIS-i

Складова	Характеристика
Сенсор	Має мініатюрний, маловартісний сейсмічний датчик, що забезпечує класифікацію цілі за алгоритмом на основі сейсмічних сигнатур. Налаштовується як радіо-ретранслятор.
Ручний монітор/ передавач	Відображає інформацію з сенсорів на LCD-дисплеї або виводить повідомлення на інші пристрої. Дає змогу програмувати сенсори бездротовим способом як локально, так і віддалено на відстані до 2 км. Підтримує повідомлення сенсорних мереж: BAIS (SAS & S/T) (29-біт); TRSS (29- біт, 285-біт); REM/IREM/REM-II (29-bit, 101-bit); LKMD (детектор руху) сигналізації.

Бездротова сенсорна мережа BAIS-i забезпечує двосторонній радіозв'язок. Вона компактна, має невелику вагу і не обтяжлива для транспортування. Кожен сенсор складається з сейсмічного датчика та антени УКХ. Ручний монітор дає змогу відображати інформацію від сенсорів на LCD-дисплей або виводити повідомлення через роз'єм RS-232 на додатковий персональний комп'ютер.

Тактико-технічні характеристики сенсорної системи BAIS-i:

сейсмічний сенсор розміром 7,6×6,3×3,9 см, вагою 0,2 кг;

ручний монітор розміром 16,5×10,6×10,6 см, вагою 0,6 кг;

тривалість автономної роботи: сенсорного вузла – до 200 діб (за 1000 спрацювань на день); ручного монітора – до 19 діб;

можливість програмувати тривалість операції;

можливість роботи від батареї та від зовнішнього живлення;

кількість каналів – 599 каналів;

забезпечує підтримку до 999 вузлів в мережі;

двосторонній радіозв'язок – SEIWG-005C,

діапазон частот – від 138 МГц до 153 МГц;

локальне та дистанційне бездротове програмування.

Крім того, ця система має вбудований пристрій, що гарантує низький рівень виявлення помилкових сигналів, а також програмне забезпечення, яке оновлюється, стійка до зламу, може бути інтегрована до систем вищих рівнів. Додаткові можливості системи виявлення вторгнень на полі бою BAIS-i, у порівнянні з AN/PRS-9A BAIS, наведено в таблиці 4.

Таблиця 4

Порівняння додаткових можливостей систем виявлення вторгнень на полі бою AN/PRS-9A BAIS та BAIS-i

Клас цілі	Радіус виявлення, м*	
	BAIS	BAIS-i
Гусенична техніка	0–450	0–550
Колісна техніка	0–350	0–400
Жива сила	0–75	0–100

*Радіус виявлення залежать від типу та стану ґрунту

На відміну від бездротових сенсорних мереж, проаналізованих вище, наземна сенсорна система для завдань розвідки Reconnaissance (ISR) UGS (США) пасивно виявляє, класифікує та визначає напрямок руху живої сили й транспортних засобів в будь-якому середовищі, вдень і вночі [13]. Вона застосовується під час операцій спеціального призначення, охорони державного кордону, заходів стосовно протидії незаконному обігу наркотиків, у процесі інших операцій із забезпечення національної безпеки та оборони (рис. 4).

Рисунок 4 – Наземна сенсорна система для завдань розвідки Reconnaissance (ISR) UGS

До її складу входить сенсор з базовим набором датчиків, ручний монітор і система обробки сигналів для досягнення високої точності моніторингу (таблиця 5).

Сейсмоакустичний датчик означеної системи може працювати в режимі ретранслятора з метою розширення цього діапазону на 6 км для кожного реле або по всьому світу за допомогою додаткової супутникової системи REM-Sense SATCOM або стільникового реле. Сенсорна система негабаритна, маловагома і зручно транспортується однією особою в спеціальному рюкзаку.

Тактико-технічні характеристики сенсорної системи Reconnaissance (ISR) UGS:

сейсмоакустичний датчик розміром 19,3×10,7×5,3 см, вагою 0,7 кг – 1 шт.;

інфрачервоний датчик (IRID-II), розміром 24,4×2,8×2,8, вагою 0,7 кг – 1 шт.;

магнітний датчик (MAGID-II) розміром 10,7×6,9×2,5 см, вагою 0,4 кг – 1 шт;

ручний монітор розміром 16,5×10,7×5,6 см, вагою 0,7 кг – 1 шт;

вбудована АКБ з номінальною напругою 9В;

тривалість автономної роботи – сенсорного вузла – до 200 діб (за 1000 спрацювань/день); ручного монітора – до 19 діб;

кількість каналів – 599;

забезпечує підтримку до 255 вузлів в мережі;

двосторонній радіозв'язок – SEIWG-005C;

діапазон частот – від 138 МГц до 153 МГц;

робоча температура – від – 40°С (– 20°С для ручного монітору) до +71°С;

стійка до вітру: 20 м/год (пил), 40 м/год (пісок), ударостійка;

електромагнітна сумісність відповідає стандартним вимогам MIL-STD-461E.

Таблиця 5

Складові наземної сенсорної системи для завдань розвідки Reconnaissance (ISR) UGS

Складова		Характеристика
Сенсор	Сейсмоакустичний датчик	Забезпечує класифікацію цілі за алгоритмом на основі сейсмічних сигнатур. Налаштовується як ретранслятор. Забезпечує живлення інфрачервоного та магнітного датчиків.
	Магнітний датчик II (MAGID-II)	Визначає напрямок і кількість цілей, різницю температур цілі і фон. Підключається до сейсмоакустичного датчика.
	Інфрачервоний датчик II (IRID-II)	Оцінює напрямок і кількість цілей. Пасивно виявляє зміни в магнітному полі, викликані рухом залізних матеріалів. Підключається до сейсмоакустичного датчика.
Ручний монітор		Забезпечує передачу інформації на LCD-дисплей; вивід повідомлень через роз'єм RS-232 на додатковий персональний комп'ютер; програмування параметрів роботи сенсорних вузлів локально і віддалено. Підтримує повідомлення сенсорних мереж: BAIS (29-біт); TRSS (285-біт); REM-II (29-bit, 101-bit)

Ця бездротова сенсорна мережа має вбудовану систему виявлення та запобігання помилок, програмне забезпечення, що регулярно оновлюється, а також здатність бути інтегрованоюа у платформи сенсорних систем вищого рівня. Додаткові можливості наземної сенсорної системи для завдань розвідки Reconnaissance (ISR) UGS наведено в таблиці 6.

Таблиця 6

Додаткові можливості наземної сенсорної системи для завдань розвідки Reconnaissance (ISR) UGS

Клас цілі/тип сенсора	Сейсмоакустичний*	Інфрачервоний**	Магнітний
	Радіус виявлення, м		
Гусенична техніка	0–450	3–50 (від 16 до 96 км/год)	3–50 (від 5 до 100 км/год)
Колісна техніка	0–350	3–50 (від 16 до 96 км/год)	3–30 (від 5 до 100 км/год)
Жива сила	0–75	3–20 (від 5 до 8 км/год)	1–5 (від 2 до 12 км/год)

*Радіус виявлення залежить від типу та стану ґрунту.

**Жива сила, озброєна АК-47.

Не зважаючи на тактико-технічні характеристики проаналізованих вище бездротових сенсорних мереж, що на нашу думку, доцільно застосовувати для побудови сучасних гнучких автоматизованих систем управління у військовій сфері, маємо визнати, що сенсорна система Pathfinder, яка виробляється «Асоціацією прикладних досліджень Північної Кароліни»

(Applied Research Associates of North Carolina (ARA)) (США) з метою моніторингу, виявлення та ідентифікації прихованих загроз, є лідером у цій сфері [13]. Означена система, під час тестування й оцінювання отримала схвальні відгуки від сертифікованих агентств, була прийнята на озброєння ЗС США та ефективно використовувалася в збройних конфліктах у багатьох регіонах світу (рис. 5).

Рисунок 5 – Вузли сенсорної системи Pathfinder

На практиці, Pathfinder, як головна складова структури керування безпеки та оборони, застосовується для моніторингу лінії зіткнення з ворогом, охорони місць розташування підрозділів, військових баз, доріг, маршрутів пересування та визначених критичних об’єктів, виявлення вибухових пристроїв, диверсійно-розвідувальних груп і снайперів. Ефективність системи, особливо у віддалених районах, забезпечується запатентованою системою зв'язку, що передає інформацію моніторингу на відстань до 8–10 км («точка-точка») та більш ніж до 25 км («земля-повітря»). Відкрита архітектура забезпечує інтеграцію з існуючими системами розвідки, спостереження і виявлення на місцевості (Intelligence, surveillance, reconnaissance (ISR)). Інформація про бездротову сенсорну мережу Pathfinder (статус вузлів, продуктивність, локація, характеристики подій, відстань до них) відображається на пристроях системи Android. Вузли означеної сенсорної системи, завдяки невеликим розмірам, швидко встановлюються однією людиною у визначеному місці розташування.

Тактико-технічні характеристики сенсорної системи Pathfinder:

mini сенсор розміром 6,6×5,6 см, вагою 0,2 кг з двома вбудованими літій-іонними АКБ номінальною напругою – 3,6 В. Тривалість автономної роботи до 6 місяців. Максимальна сила струму під час передачі становить 250 мА. Частота передачі – 916 МГц;

XL сенсор розміром 6,6×12 см, вагою 0,4 кг з вісьмома вбудованими літій-іонними АКБ напругою 3,6 В. Тривалість автономної роботи до 24 місяців. Максимальна сила струму під час передачі становить 250 мА. Частота передачі – 916 МГц;

приймач розміром – 5,3×18,3×21,3 см, вагою – 1,7 кг;

виготовлений з дотриманням стандарту США MIL-STD-810;

робоча температура – від – 32°С до + 49°С;

з'єднувачі – роз'єми MIL і RS-232 ;

кабель RJ-45 Ethernet;

антена TNC;

живлення напругою – від 100 до 240 VAC з частотою 47–63 Гц, або – 12 VDC;

використання алгоритмів штучного інтелекту;

низький рівень помилкових спрацювань.

Додаткові можливості сенсорної системи Pathfinder наведено в таблиці 7.

Таблиця 7

Додаткові можливості сенсорної системи Pathfinder

Клас цілі	Радіус виявлення, м
Жива сила	до 70
Колісна техніка	до 250
Гусенична техніка	до 350

Крім проаналізованої американської бездротової сенсорної мережі Pathfinder, ще одна сенсорна система Claw компанії General Atomics Aeronautical Systems (США) [13], є ефективною інтегрованою системою контролю та аналізу військової операції, що дає змогу проводити мульти-сенсорну розвідку, спостереження і забезпечує високу ситуативну обізнаність на полі бою.

На практиці означена система, як правило, застосовується під час проведення операцій спеціального призначення, охорони державного кордону, рятувально-пошукових операцій. Вона використовує відкриті стандарти і протоколи для забезпечення максимальної сумісності з існуючими воєнними системами (понад 50 типів) і дає змогу реалізовувати спільні операції та отримувати загальну картину моніторингу поля бою. Система широко застосовується у багатьох пілотованих і безпілотних платформах ЗС США, може бути поєднана із засобами різних типів, зокрема, відеомагнітофонами, радарами, радіолокаторами, радіостанціями тощо.

Поєднання модульної архітектури, відкритих стандартів і позитивного досвіду використання дає змогу швидко інтегрувати та модернізувати цикли роботи системи для задоволення потреб користувачів в умовах постійно змінюваних військових операцій.

Тактико-технічні характеристики сенсорної системи Claw:

електрооптичний сенсорний модуль;

інфрачервоний сенсорний модуль;

лазерний далекомір;

освітлювач;

вказівник;

радар;

автоматизована система ідентифікації;

автоматичне виявлення наземних і морських цілей;

інтеграція з технологіями, що проникають крізь перешкоди;

3D-проєкція та візуалізація даних моніторингу на карті;

позиціонування літального засобу та цілей;

діагностика стану сенсорних вузлів (температура, несправності);

тактичний канал передачі даних, супутникові комунікації з охопленням С-діапазону;

вбудовані шаблони звітування;

підтримка повідомлень Link-16 згідно «Спільного протоколу подання заявок на збільшення дальності дії» (Joint Range Extension Applications Protocol (JREAP));

декодування і транскодування відео кодеками стиснення H.264 і H.265;

сумісність з Windows 10 (64-біт);

відповідає численним інтерфейсам відкритих стандартів – STANAGS 4609, 4676, 4545, 4559, тощо;

одночасне відтворення декількох відео потоків HD, режим цифрового відеомагнітофону DVR.

Не менш ефективними серед достатньо широкого переліку американських бездротових сенсорних систем, що доцільно використовувати для побудови інноваційно-гнучких автоматизованих систем управління у військовій сфері, є сенсорні системи Forester Агентства оборонних науково-дослідних проєктів (DARPA) (США). Вони являють собою спеціалізовані системи розвідки і спостереження за цілями, зокрема, у лісистій місцевості, під час темряви, за несприятливих погодних умов [13]. Така сенсорна система може бути застосована для виявлення мінних полів, диверсійно-розвідувальних груп і снайперів завдяки використанню радіолокатора VHF/UHF діапазону. З висоти 5 км сенсорна система Forester охоплює зону 145 км2, забезпечує безперервне покриття в секторі 90° та має функції механічного й електронного керування антеною для кругового огляду (рис. 6).

Рисунок 6 – Розміщення сенсорної системи Forester на гелікоптері

Означена сенсорна система була розроблена для використання на БпЛА, літаках цивільної та військової авіації. Вона пройшла випробування в різних умовах з метою досягнення оптимальних показників функціонування. Бортові сенсори дають змогу отримати високу продуктивність зйомки і виявлення об'єктів в інтересах військової операції. Глибина проникнення таких сенсорних систем може сягати від 2 до 5 м, що дає змогу використовувати їх Forester в пошуково-рятувальних операціях, для виявлення військових цілей, мінних полів тощо. Крім того, сенсорна система Forester здатна виявляти низьколітаючі гвинтокрили та літаки на відстані до 75 км, забезпечуючи індикацію наземної (Ground Moving Target Indicator (GMTI)) та повітряної рухомої цілі (Air Moving Target Indicator (AMTI));

Тактико-технічні характеристики сенсорної системи Forester:

діапазон робочих частот – від 215 до 730 МГц;

потужність – до 1 кВт;

роздільна здатність – 66 см;

площа антени – 1 м2;

використовує властивості поглинання електромагнітної енергії різними поверхнями (Specific absorption rate (SAR));

вбудована GPS;

максимальна висота роботи над рівнем моря – до 7,5 км;

корпус із підвищеною міцністю (ударостійкий), водонепроникний.

Сенсорна система Forester достатньо проста в експлуатації, використовує алгоритми штучного інтелекту, дає змогу обробляти дані моніторингу в реальному часі, має низьку частоту помилкових спрацювань. Додаткові можливості сенсорної системи Forester наведено в таблиці 8.

Таблиця 8

Додаткові можливості сенсорної системи Forester

Клас цілі	Радіус виявлення, м
Жива сила	до 15000
Колісна техніка	до 20000
Гусенична техніка	до 30000

Аналогічними бортовими бездротовими сенсорними мережами подібного типу можна вважати сенсорні системи Mineseeker (Великобританія) і Carabas II (Швеція). Так, Британська сенсорна система призначена для виявлення мін з повітря зі швидкістю до 100м2/с (сапери виконують це завдання зі швидкістю до 40 м2/день). У свою чергу, сенсорна система Carabas-II забезпечує максимальне проникнення радіолокаційного сигналу під рослинний покрив і земну поверхню з роздільною здатністю в межах від 3,3 м до 15 м, оскільки працює в VHF діапазоні й використовує сигнал на частотах від 20 до 90 МГц з горизонтальною поляризацією.

Ще однією бездротовою сенсорною мережею американських виробників, що, на нашу думку, заслуговує бути використана для забезпечення ефективного функціонування гнучких автоматизованих систем управління в Збройних Силах України, є сенсорна система компанії Microflown Avisa (США) [13]. У свій час, вона була розроблена для ЗС США, працює як акустична парасолька для військового підрозділу, отримала назву Camel (рис. 7).

Рисунок 7 – Сенсорна система Camel

На практиці сенсорна система Camel є мобільною акустичною системою, що розміщується на військових транспортних засобах, і призначена для виявлення і локалізації таких загроз як артилерія та міномети, літальні апарати різних типів і стрілецьке озброєння тощо. Ця сенсорна система може бути застосована для захисту бойової машини та/або конвою, позицій військових підрозділів (з'єднань) і забезпечення загального спостереження. Означена бездротова сенсорна мережа використовує, так звані «мікропотоки», що дають змогу одночасно вимірювати амплітуду і визначати напрямок звукової хвилі, завдяки чому, один сенсор може виявляти та класифікувати акустичну подію. Вона функціонує у трьох режимах:

1. «Горб» – один вузол працює самостійно для виявлення і класифікації живої сили противника в межах сектору 2° з кутовою точністю до 5% від діапазону, виявлення і відстеження ударних гвинтокрилів, що низько літають.

2. «Верблюд» – два вузли працюють самостійно для поліпшення акустичних можливостей 1-го режиму, відокремлення вхідного і вихідного вогню на борту транспортного засобу.

3. «Караван» – мережа вузлів на декількох машинах виявляє і класифікує засоби артилерії та авіацію.

Тактико-технічні характеристики сенсорної системи Camel:

розмір – 14,0×31,5 см, вага – 4,1 кг (включно із системою кріплення);

потужність менше 2 Вт;

напруга живлення – від 12 В до 24 В;

скорегований рух декількох транспортних засобів (за запитом);

система захисту від РЕБ;

корпус із підвищеною міцністю (ударостійкий), водонепроникний;

інтеграція з операційними даними, доступними в транспортному засобі (геопосилання та вогневі позиції/мітки);

інтегрується з такими системами як RWS («Віддалена збройна станція»), EO («Електрооптичні»), BMS & C2 («Система управління бойовим процесом» і «Керування та контролю»).

Додаткові можливості сенсорної системи Camel наведено в таблиці 9.

Таблиця 9

Додаткові можливості сенсорної системи Camel

Клас цілі	Радіус виявлення, м
Жива сила	до 700
Колісна техніка	до 7000
Гусенична техніка	до 15000
Літаки та армійська авіація	до 30000
БпЛА	до 15000
Артилерія	до 20000
Міни	до 8000

На відміну від американських бездротових сенсорних мереж, сенсорна система Primrose компанії Elbit Systems (Ізраїль), розроблена для ЗС цієї країни з метою забезпечити ситуаційну обізнаність у реальному часі [13]. На практиці, установлені на поверхні землі, інтелектуальні сенсорні вузли цієї системи спільно виявляють і відстежують рухи живої сили противника, транспортних засобів та інших подій. За таких умов можуть застосуватися для захисту військ або операцій спеціального призначення, а також для моніторингу державного кордону. Сенсорна система Primrose забезпечує покриття необхідної зони та високу точність виявлення в режимі 24/7 з надзвичайно низькою кількістю помилкових спрацювань, навіть у складних місцевостях. Вона масштабована і гарантує підтримку значної кількості мініатюрних, просторово розподілених і двонаправлених дистанційно контрольованих вузлів, включаючи акустичні, радарні, сейсмічні, електрооптичні датчики, фотоапарати тощо (рис. 8). Варто усвідомлювати, що кілька таких мереж можуть бути об'єднані разом, заради покриття ще більшої зони. Сучасна енергозберігаюча технологія, що застосована у цій сенсорній системі, забезпечує економне споживання енергії та тривалий термін служби батарей для безперебійного функціонування її вузлів. Кожен пристрій герметичний, захищений від вологи, корозії, електромагнітних та інших впливів, що дає змогу вузлам сенсорної системи працювати протягом тривалого часу в складних погодних умовах й агресивному середовищі. Попри все, сенсорну систему Primrose можна швидко і легко розгорнути. Вона ідеально підходить для використання на горбистих місцевостях або в інших місцях, де пряма видимість неможлива.

Рисунок 8 – Вузли сенсорної системи Primrose

Тактико-технічні характеристики сенсорної системи Primrose:

сейсмоакустичний датчик (клас захищеності IP 68) з тривалістю автономної роботи до 5 років, розмірами 13,5×8,5×6,5 см, вагою – 0,65 кг;

камера (клас захищеності IP 67) забезпечує трансляцію в режимі реального часу 25 кадрів/с через радіоканал. Завдяки інфрачервоному режиму здійснює моніторинг цілодобово;

тривалість автономної роботи системи – до 6 місяців;

розмір – 18×14×6,5 см, вага – 0,65 кг;

працює в діапазоні частот ISM (Industrial scientific and medical («Індустріальні наукові та медичні»));

технології бездротових мереж multi-hop та ad-hoc роблять систему здатною до самоорганізації та самовідновлення.

Сенсорна система Primrose достатньо проста в експлуатації, сумісна з іншими системами моніторингу, має низьку частоту помилкових спрацювань, здатна проводити складний аналіз даних у фоновому режимі. Додаткові можливості сенсорної системи Primrose наведено в таблиці 10.

Таблиця 10

Додаткові можливості сенсорної системи Primrose

Клас цілі/сенсора	Сейсмоакустичний	Камера
	Радіус виявлення, м	
Жива сила	до 100	до 100
Колісна техніка	до 150	до 130
Гусенична техніка	до 200	до 150

Достатньо ефективною для побудови гнучких автоматизованих систем управління у військовій сфері є також сенсорна система Flexnet компанії Exensor Technology (Швеція). Вона являє собою набір унікальних, мініатюрних і відносно маловартісних вузлів, що призначені для цілодобового спостереження і цільового збору інформації (рис. 9) [13].

Рисунок 9 – Склад сенсорної системи Flexnet

Кожен вузол містить у собі геофон і мікрофон, що дають змогу виявляти та класифікувати живу силу й транспортні засоби противника у межах зони розгортання сенсорної мережі. Системи Flexnet застосовується для захисту військ, операцій спеціального призначення, моніторингу державного кордону та виконання інших операцій із забезпечення національної безпеки.

Вузли цієї сенсорної системи мають компактний розмір, малу вагу, прості у використанні, розгортанні та обслуговуванні й взаємодіють у самоорганізованій, самоконфігурованій мережі. Технологія ad-hoc такої сенсорної сітки передбачає роботу кожного вузла в режимі ретранслятора для збільшення радіуса поширення радіосигналу та підвищення надійності роботи системи загалом.

Тактико-технічні характеристики сенсорної системи Flexnet:

вузли, що визначають своє розташування, а їх положення автоматично відображається на графічному інтерфейсі;

інтерфейс UMRAwin C2 надає детальну інформацію про розгорнуту мережу на електронній карті;

розмір – 6,4×9,5×15 см, вага – 0,9 кг;

вбудована GPS;

підтримка технології ad-hoc;

робоча температура – від – 30°C до + 70°C;

тривалість автономної роботи – до 30 діб;

радіус прямої видимості становить 1 км для частот 868–870 МГц;

корпус із підвищеною міцністю (ударостійкий), водонепроникний, випробуваний за стандартом США, що регламентує рівень захисту обладнання від різних зовнішніх впливів (MIL-STD-810F).

Сенсорна система Flexnet швидко розгортається та проста в експлуатації, має змогу інтегруватися до інших сенсорних систем. Додаткові можливості сенсорної системи Flexnet наведено в таблиці 11.

Таблиця 11

Додаткові можливості сенсорної системи Flexnet

Клас цілі	Радіус виявлення, м	Примітка
Жива сила	до 50	Під час пішої ходи
Окопування	до 50	Під час окопування
Транспортні засоби	до 50	Цивільні/легкі
	до 200	Військові/важкі

Наведені в статті основні тактико-технічні характеристики бездротових сенсорних мереж спеціального призначення, їх конструктивні ознаки, особливості функціонування та сфери їх застосування, дають змогу виокремити низку унікальних рис, властивих таким сенсорним системам:

значна просторова та розгалужена геометрична розмірність, де кількість вузлів може сягати десятків, сотень і тисяч;

неоднорідність мережі, що характеризується наявністю стаціонарних і мобільних (рухомих) базових станцій та вузлів;

збір даних моніторингу в реальному часі;

висока динаміка зміни топології, що характеризується відмовами в роботі окремих

вузлів, їх знищенням або переміщенням, а також особливостями ведення бойових дій;

обмеженість окремих ресурсів у вузлів мережі, таких як доступна пам'ять, ємність батарей, продуктивність процесорів, потужність радіопередавачів тощо;

різні способи розташування вузлів для забезпечення покриття (детерміновано або випадково);

необхідність реалізації різних варіантів (бар'єрне, площинне, цільове) і типів (к-покриття, α-покриття) покриття для території бойового поля;

наявність декількох сенсорних модулів (датчиків) у вузлах, що призводить до різнорідного трафіку моніторингу (дані, відео) з різною інтенсивністю;

комбінування децентралізованого та централізованого підходів до управління;

наявність декількох цільових функцій управління мережею, що змінюються відповідно до бойової обстановки та наявних ресурсів;

обмежені дальність і пропускна здатність каналів радіозв'язку між вузлами.

Висновки й перспективи подальших досліджень

Проведене нами дослідження підтверджує той факт, що бездротові сенсорні мережі провідних країн світу (США, Великобританії, Ізраїлю, Швеції), з метою забезпечення ефективного виконання різних бойових завдань, активно застосовуються для побудови гнучких автоматизованих систем управління, зокрема C4ISR та її подальших модифікацій, у військовій сфері. На практиці, досвід російсько-української війни свідчить, що вчасне отримання повної та якісної інформації надає оперативну перевагу в боротьбі з агресором. За таких умов, впровадження інноваційних сенсорних систем у сектор безпеки та оборони нашої незалежної держави заради побудови дієвих гнучких автоматизованих систем управління, сприятиме ефективному досягненню заходів, завдань, стратегічних цілей і мети, що затверджені Стратегічним оборонним бюлетенем України. А також відповідатиме стандартам, доктринам і рекомендаціям НАТО, виступить певною гарантією інтеграції національних Збройних сил до гнучкої автоматизованої системи управління оборонними ресурсами держав-членів Північноатлантичного блоку.

У підсумку, наведені в статті тактико-технічні характеристики найбільш застосовуваних на практиці та інноваційно-адаптованих до бойових умов бездротових сенсорних мереж дали змогу запропонувати їх оптимальне та узагальнене призначення для побудови гнучких автоматизованих систем управління у військовій сфері. З огляду на це, маємо констатувати, що сучасна бездротова сенсорна мережа, з метою ведення розвідки, призначена для: функціонування в складному фізико-географічному середовищі, за несприятливого клімату, в різний час доби; цілодобового спостереження (моніторингу) у реальному часі; виявлення, ідентифікації, класифікації вторгнень і загроз у навколишньому просторі; цільового збору інформації, перетворення отриманих даних і зображень, їх обробки, зберігання та передачі через радіочастотні, супутникові (гідроакустичні) канали безпосередньо на командні пункти заради підвищення ситуативної обізнаності, оперативного контролю та своєчасного прийняття оперативних рішень.

Отже, на нашу думку, основними рекомендаціями стосовно подальшого впровадження і застосування бездротових сенсорних мереж, як однієї із головних складових для побудови гнучких автоматизованих систем в секторі безпеки та оборони України, слід зазначити такі.

Для моніторингу прибережних і морських територій сенсорні системи доцільно застосовувати під час: проведення операцій спеціального призначення; моніторингу стану елементів кораблів; для охорони гаваней і підтримки морських десантних (наступальних) операцій; протидії підводним човнам; захисту підводної інфраструктури та підводних сил; захисту критичної інфраструктури; охорони державного кордону; управління трафіком суден.

Для моніторингу суходолу сенсорні системи доцільно застосовувати з метою: охорони бойових машин, місць розташування військ (військових баз), оборонних позицій підрозділів (з'єднань), маршрутів пересування (конвоїв); моніторингу лінії зіткнення; виявлення мінних полів (вибухових пристроїв), диверсійно-розвідувальних груп і снайперів; моніторингу за логістикою, транспортною інфраструктурою (доріг, мостів, естакад, перехресть тощо); спостереження та охорони об'єктів критичної та енергетичної інфраструктури; забезпечення проведення операцій спеціального призначення; оперативного збору аудіо-відео інформації у важкодоступних і небезпечних районах, зокрема, в будівлях, підвалах; охорони державного кордону; проведення операцій з протидії незаконному обігу наркотиків.

Серед ключових рекомендацій стосовно подальшого інноваційного розвитку вітчизняних бездротових сенсорних мереж в секторі безпеки та оборони України, можна виділити:

створення національних стандартів щодо розробки бездротових сенсорних мереж і побудови на їх основі гнучких автоматизованих систем

управління у військовій сфері, гармонізованих та уніфікованих зі стандартами НАТО (особливе значення має опрацювання національних стандартів стосовно розроблення, впровадження та експлуатації бездротових сенсорних мереж для забезпечення їхньої сумісності та взаємодії з іншими сенсорними системами, а також гнучкими автоматизованими системами управління у військовій сфері);

розширення сфери застосування (у віддалених, важкодоступних чи небезпечних районах, лініях зіткнення бойових дій, охорони об'єктів інформаційної та критичної інфраструктури, для збору розвідувальної інформації);

розроблення інтегрованих рішень (бездротові сенсорні мережі, як інтегрована сенсорна система, можуть бути поєднані з іншими безпековими технологіями, зокрема, з елементами (вузлами) гнучкої автоматизованої системи управління військами згідно стандартів НАТО);

забезпечення безпеки даних (важливо удосконалювати систему передачі та зберігання даних у бездротових сенсорних мережах, наприклад, шляхом застосування сучасних протоколів шифрування);

удосконалення енергоефективності (актуальними є дослідження можливостей збільшення тривалості функціонування вузлів бездротової сенсорної мережі через вдосконалення систем живлення, використання енергоефективних технологій (протоколів) та альтернативних джерел енергії);

розроблення концептуальної моделі системи управління бездротовими сенсорними мережами, що функціонують із використанням штучного інтелекту, володіють здатністю до самоорганізації і можливістю планування послідовності дій та виконання визначених завдань.

Список бібліографічних посилань

1. Ефективні дії ЗСУ на великій війні спонукали НАТО до покращення командування й розвідки в Альянсі. 21.03.2023. URL: https://armyinform.com.ua/2023/03/21/efektyvni-diyi-zsu-na-velykij-vijni-sponukaly-nato-do-pokrashhennya-komanduvannya-j-rozvidky-v-alyansi/ (дата звернення: 23.06.2023). **2. Жук О. В.** Концептуальна модель побудови системи управління безпроводовими сенсорними мережами військового призначення. *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО*: доп. та тези доп. учасників XI науково-практичної конференції, м. Київ, 8-9 листопада, 2018 р. Київ : ВІТІ ім. Героїв Крут, 2018. С. 20–28. **3. Жук О. В., Міночкін А. І, Романюк В. А.** Перспективи розвитку тактичних сенсорних мереж. *Збірник наукових праць ВІТІ НТУУ «КПІ».* 2007. № 2. С. 112–119. **4. Жук О. В., Романюк В. А., Бовда Е. М.** Методологія синтезу автоматизованих систем управління телекомунікаційними системами військового призначення. *Збірник наукових праць ВІТІ.* 2017. № 1. С. 36–46. **5. Жук О. В., Романюк В. А., Бовда Е. М.** Управління перспективними неоднорідними безпровідними сенсорними мережами тактичної ланки управління військами: проблема і шляхи рішення. *Збірник наукових праць «Труди університету».* 2017. Вип. 1. С. 171–180. **6. Жук О. В., Романюк В. А., Сова О. Я.** Методологічні основи управління перспективними неоднорідними безпроводовими сенсорними мережами тактичної ланки управління військами. *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення* : тези доповідей та виступів учасників IX науково-практичної конференції, м. Київ, 2016 р. Київ : ВІТІ НТУУ «КПІ», 2016. С. 34–44. **7. Жук О. В., Романюк В. А., Сова О. Я.** Система управління тактичними сенсорними мережами. *Збірник наукових праць ВІТІ НТУУ «КПІ».* 2008. № 2. С. 88-96**. 8. Прищепа Т. О., Лисенко О. І.** Безпроводові сенсорні мережі із мобільними сенсорами. *Перспективи телекомунікацій* : зб. матер. Міжнар. наук.-техн. конф., м. Київ, 21–25 квітня 2015 року. Київ: НТУУ «КПІ», 2015. URL : http://conferenc.its.kpi.ua/proc/article/view/104177 (дата звернення: 23.06.2023). **9. Про рішення** Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 06.06.2016 № 240/2016. URL: https://www.president.gov.ua/documents/ 2402016-20137 (дата звернення: 23.06.2023). **10. Рішення** Ради національної безпеки і оборони «Про Стратегічний оборонний бюлетень України» від 20.08.2021 №n0063525-21 URL: https://zakon.rada.gov.ua/laws/show/n0063525-21 (дата звернення: 23.06.2023). **11. Указ Президента** України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17 вересня 2021 року № 473/2021 URL: https://zakon.rada.gov.ua/laws/show/ 473/2021#n17(дата звернення: 23.06.2023). **12. Що таке C4ISR?** Аеророзвідка. 20.09.2022. URL: https://www.facebook.com/aerorozvidka/ posts/ 5149553421834764/ (дата звернення: 23.06.2023). **13. Arora A., Dutta P., Bapat S., Kulathumani V., Zhang H., Naik V., Mittal V., Cao H., Demirbas M., Gouda M., Choi Y., Herman T ., Kulkarni S., Arumugam U., Nesterenko M., Vora A., Miyashita M.** A Line in the Sand: A Wireless Sensor Network for Target detection, classification, and tracking. Computer Networks. December 2004. Vol. 46, Is. 5. P. 605–634. URL: https://www.sciencedirect.com/science/article/abs/pii/S138912860400146X (дата звернення: 23.06.2023). **14. Militaries** moving from C4ISR and C5ISR to C6ISR. 2023. URL: https://idstch.com/technology/electronics/militaries-moving-from-c4isr-and-c5isr-to-c6isr/ (дата звернення: 23.06.2023). **15. Warfare** in the post-digital era. 2021. URL: https://wavellroom.com/2021/10/05/warfare-in-the-post-digital-era/ (дата звернення: 23.06.2023). **16. Zhuk O. V., Romaniuk V. A., Stepanenko E. A.** Method of collecting monitoring

information in wireless sensor networks with uav. *Інформаційно-телекомунікаційні технології та радіоелектроніка УкрМіКо'2018* : тези доповідей та виступів учасників Третьої IEEE Міжнародної конференції, м. Одеса, 10–14 вересня 2018 р. Одеса : ОНАЗ ім. О. С. Попова, 2018. С. 22–24.

CONCEPTUAL APPROACHES TO THE USE OF WIRELESS SENSOR NETWORKS BY THE ARMIES OF THE WORLD'S LEADING COUNTRIES

Mashtalir Vadym ***(Doctor of Historical Sciences, Professor)*** [1]
Zhuk Oleksandr ***(Doctor of Technical Sciences, Associate Professor)*** [1]
Minenko Liudmyla ***(PhD)*** [1]
Artyukh Sergiy [2]

[1] ***National Defence University of Ukraine, Kyiv, Ukraine***
[2] ***Military institute of telecommunications and information technologies named after Heroes of Kruty, Kyiv, Ukraine***

Russia's war against Ukraine has prompted an objective assessment of existing communication networks and command and control systems, which are configured according to the norms of the C4ISR concept, which stands for «Command and Control, Computers, Communications, Intelligence – Surveillance – Reconnaissance». It is an integrated approach to command and control and coordination of military operations in modern warfare. Today, due to cyber and other threats, this concept has expanded to include seven permanent components – «Command and Control, Computers, Communications, Intelligence - Surveillance - Reconnaissance, Combat systems, Cyber, Collaboration». The abbreviation C7ISR is used to refer to this type of system. In addition, the successful functioning of this system is ensured by additional possible factors and means of «Convergence, Cohesion, Combine, Co-operation, Coordination, Continuous, Connected networks, Multi-clouds». Therefore, the use of new technologies in the military sphere will continue to generate variations of such systems, their names and abbreviations. By their very nature, such communication networks and command and control systems must be able to respond immediately to massive cyber attacks, missile strikes and other threats. During the Russian-Ukrainian war, the use of advanced NATO technologies, in particular through the potential of C4ISR and its subsequent modifications, made it possible to reveal the build-up of enemy troops on the Ukrainian-russian-belarusian border and the aggressor's strongholds. It is flexible automated control systems that respond in a timely manner to the impact of various external factors that allow the Ukrainian military to quickly adapt to the changing situation on the battlefield. The C4ISR system, with the flexible use of additional factors and means (e.g. C5ISR, C6ISR, C7ISR) and its architecture, is optimally adapted to the environment and provides collection and analysis of multidimensional intelligence information on land, in the air and in the water, when there is a significant amount of different types of signals: electronic, electro-optical, infrared and satellite. This helps to improve the process of making operational decisions, ensures their immediate and effective communication to the executors, provides support capability, controls and, if necessary, regulates the implementation of assigned combat tasks. Mobile wireless sensor networks (sensor systems) are a key tool for obtaining, processing and transmitting data that ensure the proper functioning of C4ISR (C5ISR, C6ISR, C7ISR) systems. It should be noted that the russian-Ukrainian war has highlighted the importance of using sensor systems to obtain intelligence and its comprehensive analysis to ensure effective decision-making by commanders. Rapid deployment, self-organisation and fault tolerance are key features of wireless sensor networks that make them a reliable tool for efficiently performing operational tasks. The purpose of the article is to analyse the tactical and technical characteristics, peculiarities of operation and application of wireless sensor networks of the armies of the world's leading countries with a view to developing professional recommendations for their further implementation in the security and defence sector of Ukraine, and also to guarantee the innovation of development of domestic models of flexible automated control systems in the armed forces of our State. The methods of analysis, synthesis, and forecasting were used to provide a scientifically sound basis for the article. This methodological toolkit made it possible to conceptually characterise NATO's automated command and control systems (C4ISR and extended C7ISR), to reveal the tactical and technical characteristics of special (military) sensor systems, the peculiarities of their functioning, to summarise the purpose of mobile wireless sensor networks of the operational level, and to develop recommendations for the implementation of such systems in the national military sphere and their further innovative development. The article analyses the Strategic Defence Bulletin of Ukraine in terms of the need for total digitalisation of the Ministry of Defence and the General Staff of the Armed Forces of Ukraine and the use of wireless sensor networks for the development of flexible automated control systems in the military sphere. A conceptual description of the NATO military command and control standard is given. An analysis of leading scientific research and publications on the tasks of control using sensor systems, the current state of mobile wireless sensor networks, as well as the prospects for their development and the feasibility of using them to build innovative automated control systems in the Armed Forces of Ukraine is carried out. The article highlights the tactical and technical characteristics, describes the design features and highlights the peculiarities of functioning of sensor systems for special (military) purposes. In particular, the following sensor systems are considered:

AUSSNet, Vigilis, REM-Sense, AN/PRS-9A BAIS, BAIS-i, UGS Reconnaissance (ISR), Pathfinder, Claw, Forester, Camel (USA), Mineseeker (UK), Carabas II, Flexnet (Sweden), Primrose (Israel). It was found that acoustic, electro-optical, infrared, magnetic, temperature, accelerometric and seismic sensors are used as part of the sensor systems. The purpose and areas of application are summarised and recommendations for the use of wireless sensor networks in the military sphere of Ukraine, in particular, for the construction of flexible automated control systems for the armed forces, are formulated. The analyses contribute to the deepening of scientific knowledge about the technological, architectural, and design features of individual components (modules) of sensor systems in order to improve them and effectively implement them in the military sphere, which is formed on the basis of the principles and standards of NATO member states. The applied use of mobile wireless sensor networks qualitatively improves the characteristics of the C4ISR automated system and its further modifications, and ensures its optimally adapted integration into automated systems for managing domestic defence resources.

Keywords: *Strategic Defence Bulletin, flexible automated control system, C4ISR, sensor systems, wireless sensor networks, tactical and technical characteristics, advanced technologies for creating sensor systems.*

References

1. ArmyInform, (June 23, 2023). Effective Actions of the Ukrainian Armed Forces during a Large-Scale War Prompted NATO to Improve Command and Intelligence within the Alliance [online]. Available at: https://armyinform.com.ua/2023/03/21/efektyvni-diyi-zsu-na-velykij-vijni-sponukaly-nato-do-pokrashhennya-komanduvannya-j-rozvidky-v-alyansi/ [Accessed : 23 June 2023]. **2. Zhuk, O. V.,** (2018). Conceptual Model for Constructing Management Systems of Military Wireless Sensor Networks. In Priority Directions of Development of Telecommunication Systems and Networks of Special Purpose, 20–28. Kyiv: VITI named after Heroes of Krut..**3. Zhuk, O. V., Minochkin, A. I., & Romaniuk, V. A.,** (2007). Prospects for the Development of Tactical Sensor Networks. Collection of Scientific Works of VITI NTUU «KPI», (2), 112–119. **4. Zhuk, O. V., Romaniuk, V. A., & Bovda, E. M.,** (2017). Methodology for Synthesizing Automated Management Systems for Military Telecommunication Systems. Collection of Scientific Works of VITI, (1), 36–46. **5. Zhuk, O. V., Romaniuk, V. A., & Bovda, E. M.,** (2017). Management of Prospective Heterogeneous Wireless Sensor Networks of Tactical Control Units: Problem and Solutions. Collection of Scientific Works «Trudi universiteta», 1, 171–180. **6. Zhuk, O. V., Romaniuk, V. A., & Sova, O. Y.,** (2016). Methodological Foundations for Managing Prospective Heterogeneous Wireless Sensor Networks of Tactical Control Units. In Priority Directions of Development of Telecommunication Systems and Networks of Special Purpose, 34–44. Kyiv: VITI NTUU «KPI». **7. Zhuk, O. V., Romaniuk, V. A., & Sova, O. Y.,** (2008). Tactical Sensor Network Management System. Collection of Scientific Works of VITI NTUU «KPI», 2, 88–96. **8. Prishchepa, T. O., & Lysenko, O. I.,** (2015). Wireless Sensor Networks with Mobile Sensors. In Perspectives of Telecommunications, 104177. Kyiv: NTUU «KPI» [online]. Available at: http://conferenc.its.kpi.ua/proc/article/view/104177 [Accessed : 23 June 2023]. **9. President** of Ukraine, (2016). Decision of the National Security and Defense Council of Ukraine dated May 20, 2016, «On the Strategic Defense Bulletin of Ukraine». Decree No. 240/2016 [online]. Available at: https://www.president.gov.ua/documents/2402016-20137 [Accessed : 23 June 2023]. **10. National** Security and Defense Council, (2021). Decision on the Strategic Defense Bulletin of Ukraine. Decision No. n0063525-21 [online]. Available at: https://zakon.rada.gov.ua/laws/show/n0063525-21 [Accessed : 23 June 2023]. **11. President** of Ukraine, (2021). Decree on the Decision of the National Security and Defense Council of Ukraine dated August 20, 2021, «On the Strategic Defense Bulletin of Ukraine». Decree No. 473/2021 [online]. Available at: https://zakon.rada.gov.ua/laws/show/473/2021#n17 [Accessed : 23 June 2023]. **12. Aerial** Reconnaissance, (2022). What is C4ISR? [online]. Available at: https://www.facebook.com/aerorozvidka/posts/5149553421834764/ [Accessed : 23 June 2023]. **13. Arora, A., Dutta, P., Bapat, S., Kulathumani, V., Zhang, H., Naik, V., Mittal, V., Cao, H., Demirbas, M., Gouda, M., Choi, Y., Herman, T ., Kulkarni, S., Arumugam, U., Nesterenko, M., Vora, A., Miyashita, M.,** (2004). A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking. Computer Networks, 46(5), 605–634 [online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S138912860400146X [Accessed : 23 June 2023]. **14. IDSTCH,** (2023). Militaries moving from C4ISR and C5ISR to C6ISR [online]. Available at: https://idstch.com/technology/electronics/militaries-moving-from-c4isr-and-c5isr-to-c6isr/ [Accessed : 23 June 2023]. **15. Wavell Room,** (2021). Warfare in the Post-Digital Era [online]. Available at: https://wavellroom.com/2021/10/05/warfare-in-the-post-digital-era/ [Accessed : 23 June 2023]. **16. Zhuk, O. V., Romaniuk, V. A., & Stepanenko, E. A.,** (2018). Method of Collecting Monitoring Information in Wireless Sensor Networks with UAV. In Information and Telecommunication Technologies and Radio Electronics UkrMiCo'2018, 22–24. Odessa: ONAZ named after O. S. Popov.

DOI:**10.33099/2311-7249/2023-47-2-113-118**

УДК 519.682

Ільїн Дмитро Володимирович
Старинський Іван Михайлович *(кандидат технічних наук)*

Національний університет оборони України, Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ З ВИКОРИСТАННЯМ НЕЙРОННОЇ МЕРЕЖІ НА ОСНОВІ АВТОЕНКОДЕРІВ

Інформаційно-телекомунікаційна мережа військового призначення має великий обсяг наборів даних, а забезпечення захищеності такої мережі від кібератак, є працеємним процесом. Дані мережевого трафіку мають складні нелінійні зв'язки, що змінюються в часі. Існуючі моделі забезпечення кіберзахищеності базуються на моделях кореляції даних про трафік і вимагають значних обчислювальних витрат та не дають змоги здійснювати обробку мережевого трафіку в реальному часі. Крім того, вони не враховують просторово-часові кореляції даних. Метою статті є розроблення математичної моделі системи виявлення вторгнень на основі мережі автоенкодерів для забезпечення кіберзахищеності інформаційно-телекомунікаційної мережі військового призначення. Запропоновано розроблену математичну модель системи виявлення вторгнень на основі нейронної мережі, яка базується на поєднанні багатошарової згорткової нейронної мережі на основі автоенкодерів з використанням довгострокової короткочасної пам'яті. Розроблена модель системи виявлення вторгнень спочатку використовує багатошарову згорткову нейронну мережу на основі автоенкодерів для аналізу просторових особливостей набору даних, які потім обробляються автоенкодерами з використанням довгострокової короткочасної пам'яті для виявлення аномалій у мережевому трафіку. Для підвищення точності виявлення вторгнень запропоновано застосовувати два алгоритми Isolation Forest, що виправляють помилки, виявляють хибнопозитивні та хибнонегативні результати. Тренування моделі системи виявлення вторгнень на основі нейронної мережі проводилось з використанням набору даних NSL-KDD та показало високу точність реконструкції даних та її працездатність.

Ключові слова: *інформаційно-телекомунікаційна мережа, кіберзахищеність, нейронна мережа, система виявлення вторгнень, автоенкодер.*

Вступ

Постановка проблеми. За умов стрімкого зростання кіберризиків і кіберзагроз важливим є питання забезпечення кіберзахисту інформаційно-телекомунікаційних мереж (далі – ІТМ) військового призначення (далі – ВП). Особливої уваги потребують DoS-атаки, які є найбільш небезпечними, простими в організації та найдешевшими за вартістю кіберзагрозами. Так, наприклад, в Україні такі кібератаки здійснювалися на сайти органів державної влади, а саме, Президента України, Кабінету Міністрів України, Міністерства оборони України, Служби безпеки України, Міністерства внутрішніх справ України тощо. Водночас було встановлено більше 5 тисяч кібератак. Ці кібератаки показали низький рівень кіберзахищеності ІТМ від такого типу запланованих кібератак, та відсутність досить ефективних засобів захисту, таких як системи виявлення вторгнень [1]. У зв'язку з цим, розроблення методів і моделей, що дають змогу формалізувати процеси виявлення вторгнень є актуальним науковим завданням.

Аналіз останніх досліджень та публікацій. Аналіз літератури з кібербезпеки свідчить, що для забезпечення кіберзахищеності ІТМ створюються системи виявлення вторгнень (далі – СВВ) на основі нейронних мереж (далі – НМ). Наприклад, у роботах [2–4] пропонується СВВ нейронної мережі з неконтрольованим навчанням, що базується на напівконтрольованій нечіткій C-Mean кластеризації з одношаровими НМ прямого зв'язку (далі – ПЗ), також відомою як Extreme Learning Machine (далі – ELM) для виявлення вторгнень у режимі реального часу.

Сьогодні використовуються методи неконтрольованого глибинного навчання, такі як мережа глибоких переконань (Deep Belief Network) (далі – DBN), самоорганізуючі карти та автоенкодери. У роботі [5] запропоновано модель СВВ нейронної мережі на основі самоорганізованої карти, яка покращує виявлення вторгнень. А в роботах [6] та [7] запропоновано СВВ нейронної мережі з неконтрольованим глибинним навчанням DBN для виявлення вторгнень. Крім того, у значній кількості досліджень вивчалося застосування глибокої мережі переконань у проєктуванні СВВ НМ [8; 9].

Разом із тим, досвід побудови СВВ НМ свідчить, що перспективним напрямом дослідження є побудова ефективних СВВ НМ із

використанням автоенкодерів (далі – АЕ), оскільки вони прості у реалізації та маловартісні. У низці досліджень була спроба розробити варіанти АЕ з покращеними характеристиками щодо виявлення вторгнень. Разом із тим, стає очевидним, що, незважаючи на значний приріст продуктивності, досягнутий із застосуванням СВВ з неконтрольованим навчанням, має місце їх достаньо низька ефективність стосовно виявлення прихованих кібератак. Таким чином, дослідження проблеми забезпечення кіберзихищеності інформаційно-телекомунікаційних системи від кібератак на основі СВВ НМ з неконтрольованим навчанням на основі автоенкодера є актуальним.

Метою статті є розроблення математичної моделі системи виявлення вторгнень з використанням нейронної мережі на основі автоенкодерів для забезпечення кіберзахищенності інформаційно-телекомунікаційної мережі військового призначення.

Виклад основного матеріалу дослідження

Для забезпечення кіберзахищеності ІТМ доцільно використовувати СВВ на основі автоенкодерів, що є одним із типів НМ прямого зв'язку з неконтрольованим навчанням (без вчителя) та застосовується для реконструкції вхідних даних. Нейронна мережа на основі АЕ намагається під час аналізу трафіку в ІТМ визначити оптимальний підпростір, де нормальні та аномальні дані відрізняються.

Для побудови математичної моделі АЕ припустимо, що нормальний тренувальний набір є множиною $X=\{x_1,x_2,x_3,...,x_n\}$, у якій кожен елемент є d розмірний вектор $(x_i \in R^d)$, а після навчання на виході АЕ отриманий результат описується множиною $\{x_1',x_2',...,x_n'\}$. Тоді помилка реконструкції визначається як:

$$\varepsilon(x_i,x_i')=\sum_{j=1}^{d}(x_i-x_i')^2 \qquad (1)$$

Принцип виявлення вторгнень на основі АЕ полягає в тому, що звичайні дані в тестовому наборі даних відповідають нормальному профілю і відповідна помилка реконструкції є меншою, тоді як аномальні дані матимуть відносно вищу помилку реконструкції. Тому встановивши порогове значення помилки реконструкції, можна легко класифікувати аномальні дані:

$$c(x_i)=\begin{cases} normal \varepsilon_i < \theta) \\ anomalous \varepsilon_i > \theta \end{cases} \qquad (2)$$

Архітектура АЕ складається з кодера та декодера. Кодер і декодер складаються з вхідного шару нейронів, вихідного шару нейронів та одного або кількох прихованих шарів нейронів. Автоенкодлер має симетричну структуру – вихідний шар декодера дорівнює вхідному шару кодера. Математично, кодер із вхідними векторами $(x_i \in R^d)$ та вихідний шар розміру m (прихований шар) можна описати за виразом:

$$h_i=f_\theta(x_i)=s(\sum_{j=1}^{n} w_{ij}^{ex}x_j+b_i^{ex}), \qquad (3)$$

де $f_\theta(x_i)$ – функція активації вхідного шару;

x_i – вхідний вектор, $i=\overline{1,n}$;

$W^{ex}=\|w_{ij}^{ex}\|$ – матриця ваг кодера, $i,j=\overline{1,n}$;

w_{ij}^{ex} – ваги j-го елементу i-го набору даних матриці ваг кодера W^{ex}, $i,j=\overline{1,n}$;

$b^{ex}=\{b_i^{ex}\}$ – вектор зміщення, $i=\overline{1,n}$.

b_i^{ex} – зміщення у i-му елементі кодера, $i=\overline{1,n}$.

Відповідно до виразу (3) вхідний вектор x_i кодується у вектор меншої розмірності.

Отримане представлення h_i потім декодується назад до вихідного простору R^d за допомогою декодера, який описується наступною функцією:

$$x_i'=g_{\theta'}(h_i)=s(\sum_{j=1}^{n} w_{ij}^{вих}h_j+b_i^{вих}), \qquad (4)$$

де $g_{\theta'}(h_i)$ – функція активації вихідного шару;

x_i' – вихідний вектор, $i=\overline{1,n}$;

θ' – множина параметрів вихідного шару $\{W^{вих},b^{вих}\}$;

$W^{вих}=\|w_{ij}^{вих}\|$ – матриця ваг декодера;

$w_{ij}^{вих}$ – ваги j-го елементу i-го набору даних матриці ваг декодера $W^{вих}$, $i,j=\overline{1,n}$;

$b^{вих}=\{b_i^{вих}\}$ – вектор зміщення.

$b_i^{вих}$ – зміщення у i-му елементі декодера, $i=\overline{1,n}$.

Для мінімізації середньої помилки реконструкції будуємо наступну цільову функцію $F_{\theta',\theta''}(x_i,x_i')$ АЕ відносно параметрів θ та θ′

$$F_{\theta^*,\theta'^*}(x_i,x_i')=\underset{\theta,\theta'}{arg\,min}\frac{1}{n}\sum_{i=1}^{n}\varepsilon(x_i,x_i')= \\ =\underset{\theta,\theta'}{arg\,min}\frac{1}{n}\sum_{i=1}^{n}\varepsilon(x_i,g_{\theta'}(f_\theta(x_i))) \qquad (5)$$

де ε – функція помилка реконструкції.

Таким чином, аномальні дані можна визначити за допомогою виразу (3), але для цього потрібно визначити функції активації f та g, які мають бути нелінійними функціями, щоб виявити нелінійну кореляцію між вхідними характеристиками.

Для цього застосуємо такий метод машинного навчання без вчителя як метод ізольованого лісу [7], який може виявляти вторгнення шляхом випадкового розділення точок даних. Метод ізоляційного лісу передбачає, що дані, які не знаходяться в області їх обробки, є аномаліями. Область обробки даних формується як двійкові дерева ізоляції та ансамблі iTrees шляхом випадкової вибірки для заданого набору даних. Ключова роль дерева ізоляції полягає у виявленні аномалії для виявлення вторгнення.

Метод ізольованого лісу має декілька переваг. Спершу, для створення iTrees виконується

випадковий вибір підмножини з навчального набору. По-друге, у методі iForest не використовується вимірювання відстані чи щільності для виявлення аномалії, що зменшує витрати на обчислення порівняно з вимірюваннями відстані, задіяними в кластеризації. По-третє, метод iForest вимагає невеликої кількості пам'яті та використовує ідею ансамблю, і не залежить від того, що деякі дерева не дають ефективних результатів, оскільки алгоритми ансамблю перетворюють слабкі дерева в ефективні. Завдяки всім цим перевагам доцільно використати метод iForest для виявлення аномалій у трафіку ІТМ.

Запропонована математична модель (5) формалізує процес функціонування системи виявлення вторгнень на основі нейронної мережі, яка базується на поєднанні багатошарової згорткової нейронної мережі на основі автоенкодерів (далі – БШЗНМ МАЕ) та мережі автоенкодерів довгострокової короткочасної пам'яті (далі – МАЕ ДКП). Модель СВВ НМ обчислює показники аномалій на основі помилки реконструкції даних трафіку, що дає можливість ідентифікувати зловмисний трафік, тобто кібератаку. Ця модель виявляє вторгнення за двома послідовними діями. Тестовий набір даних надходить до БШЗНМ МАЕ, що виявляє вторгнення на основі порогового значення та розділяє вхідні дані на два набори – трафік з ознаками атаки (вторгнення) та звичайний мережевий трафік. Потім МАЕ ДКП за допомогою методу iForest визначає аномальні точки даних, тобто виявляє вторгнення.

Процес функціонування СВВ НМ доцільно розділити на такі етапи:

1. Попередня обробка даних (стандартизація та нормалізація).

2. Ідентифікація атрибутів даних мережевого трафіку на основі БШЗНМ МАЕ;

3. Розподіл мережевого трафіку на основі НМ МАЕ ДКП;

4. Виявлення вторгнення.

На першому етапі здійснюється попередня обробка даних, що можуть бути символічними та безперервними для перетворення їх в один числовий тип. Крім того, оскільки атрибути даних розподілені нерівномірно, то вони масштабуються за одним з найпоширеніших методів кодування символьних значень, що кодує числові значення на основі рівномірного розподілення в інтервалі [0–1]. Для цього використовується метод мінімально-максимальної нормалізації даних:

$$x_i' = \frac{x_i - min(x_i)}{max(x_i) - min(x_i)} \qquad (7)$$

де $\max(x_i)$ та $min(x_i)$ – максимальне і мінімальне значення вектора атрибутів x_i;

x_i' – нормалізоване значення функції між [0–1].

На другому етапі здійснюється ідентифікація атрибутів даних мережевого трафіку на основі багатошарової згорткової нейронної мережі на основі автоенкодерів. Оскільки мережевий трафік – це багатовимірний набір даних, який неможливо ідентифікувати лише за кількома окремими ознаками, то архітектуру БШЗНМ МАЕ налаштовано та трансформовано для виконання цього завдання.

Згортковий автоенкодер (далі – ЗАЕ) [10] – це особливий вид автоенкодера, який не передбачає повне підключення нейронів між собою. Модель ЗАЕ складається із конволюційних (згорткових) і деконволюційних шарів архітектури згорткової нейронної мережі (далі – ЗНМ). ЗАЕ використовує згортковий шар нейронів у частині кодера та деконволюційний шар нейронів у частині декодера. За таких умов, згортковий шар нейронів зменшує розмірність атрибутів даних, тоді як шар нейронів деконволюції збільшує розмірність цих ознак. Тобто, у ЗАЕ згортковий шар нейронів бере на себе роль кодера для виконання зменшення розмірності, тоді як шар нейронів деконволюції застосовується для реконструкції даних. Згортковий автоенкодер використовує переваги згорткового та деконволюційного шарів. Тому, порівняно зі звичайним автоенкодером, ЗАЕ має меншу кількість параметрів, тому час навчання ЗАЕ набагато менший.

Багатошарова згорткова нейронна мережа на основі автоенкодерів має кілька вузлів згортки різного розміру для отримання кількох наборів локальних функцій для досягнення точної ідентифікації. Структура БШЗНМ МАЕ базується на трьох багатошарових згортках. Багатошарові згортки обробляють набори даних за допомогою згорток розмірності 1×1, 2×2 та 3×3 для виявлення зв'язку між базовими атрибутами даних мережевого трафіку. Кодер та декодер АЕ мають вхідний шар та шар згортки, шар об'єднання, повно зв'язну нейронну мережу та вихідний шар, що має таку ж розмірність, як і вхідний шар. Для побудови математичної моделі БШЗНМ МАЕ припустимо, що $X \in \Re^{N_x \times N_y}$ і $K^f \in \Re^{a \times b}$ є вхідним вектором для ЗНМ і фільтром відповідно.

Операція згортки між вхідним вектором X і N_f фільтрами визначається таким чином:

$$Y_{i,j} = \sum_{f=1}^{N_f} \sum_{p=1}^{a} \sum_{q=1}^{b} K_{p,q}^{f} X_{i+p-1, j+q-1} \qquad (8)$$

де $Y_{i,j}$ – компоненти відфільтрованого вхідного вектору.

Розмір Y визначається його рядком Y_x і стовпцем Y_y за виразами:

$$Y_x = \frac{N_x - a + 2P}{S_x} + 1 \qquad (9)$$

$$Y_y = \frac{N_y - a + 2P}{S_y} + 1 \qquad (10)$$

де S_X і S_y – кроки в рядку та стовпці відповідно, які керують зміщенням фільтра на вхідних даних;

P – відступ, який контролює кількість нулів навколо X. Відступ використовується для зміни

розміру виходу ЗНМ без шкоди для результату згортки.

Припускаючи $d = N_x \times N_y$, можна відобразити будь-яку точку даних x_k до точки $x_{i,j}$ у двовимірному масиві (який виглядає як $N_x \times N_y$ матриця). Тобто

$$x_k \equiv X_{i,j},$$

$$k = \overline{1,d},\ i = \overline{1,N}_x \text{ та } j = \overline{1,N}_y;$$

де
$$h_l = \sigma\left(\sum_{k=1}^{d'} w'_{lk} x_{\phi(k)} + b_l\right) \quad (11)$$

$$d' = Y_x \times Y_y;$$

$$w'_{lk} = \sum_{k=1}^{N_f} \sum_{p=1}^{a} \sum_{q=1}^{b} K^{f}_{p,q} w_{lk} \quad (12)$$

та

$$x_{\phi k} \equiv X_{i+p-1, j+q-1}$$

де $\phi(k) = (i+p-1),\ \ j+q-1$;

$w'_{ik}(\forall l,k)$ – нові латентні просторові ознаки, які є вхідними даними до МАЕ ДКП.

На третьому етапі здійснюється розподіл мережевого трафіку з використанням НМ на основіф автоенкодерів довгострокової короткочасної пам'яті. Автоенкодер в МАЕ ДКП складається з кодера та декодера. Завданням кодера є вивчення основних характеристик і створення закодованої версії вхідного зразка, а декодер – реконструкція вхідних даних.

Функцією кодера архітектури МАЕ ДКП є перетворення послідовності латентних просторових ознак, що були витягнуті з мережевого трафіку за допомогою БШЗНМ МАЕ в фіксований вектор нових ознак (латентний простір), який, в свою чергу, декодером перетворюється на вихідну послідовність. Така конфігурація АЕ здатна виявляти короткі та довгі залежності в послідовності базових ознак.

МАЕ ДКП може запам'ятовувати довготривалі залежності у ДКП-комірках – c_i. Комірки c_i оновлюються за допомогою чотирьох внутрішніх активаційних шарів (гейтів), які є нейронними шарами сигмоїдної нейронної мережі, із виконанням покомпонентної операції над ними.

Кожен гейт призначений для виконання окремої функції:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (13)$$

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (14)$$

$$\widetilde{C}_t = \tanh(W_C[h_{t-1}, x_t] + b_C) \quad (15)$$

$$O_t = \sigma(W_O[h_{t-1}, x_t] + b_O) \quad (16)$$

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C}_t \quad (17)$$

$$h_t = O_t * \tanh(C_t) \quad (18)$$

де W_f, W_i, W_C, W_O – лінійні перетворення;

C_t та h_t – пам'ять комірки та вихідне значення відповідно в момент часу t.

На виході МАЕ ДКП маємо послідовність трафіку $X(n) = [x^{(1)}, x^{(2)}, \ldots, x^{(W)}]$ довжиною W, де n - індекс звичайного тренувального прикладу.

Кодер АЕ ДКП генерує синтезований вихідний вектор (y^W) з попередньо визначеною розмірністю $r \times 1$ на основі рівнянь (13)-(18):

$$y^W = \psi[x^{(1)}, x^{(2)}, \ldots, x^{(W)}] \quad (19)$$

де ψ – нелінійна функціюя кодера архітектури ДКП.

Вектор (y^W) є новими латентними просторовими ознаками, які виражають компактне представлення поведінки у часі базових ознак. Вектор (y^W) використовується декодером для відновлення вхідного зразка відповідно до виразу (19):

$$\hat{X}(n) = \Phi[y^{(1)}, y^{(2)}, \ldots, y^{(r)}] \quad (20)$$

де Ф – функція декодера МАЕ ДКП.

Метою декодера є відновлення вхідної послідовності з мінімальною втратою, що може бути обчислена з урахуванням середньоквадратичної помилки відповідно до (1).

Четвертий етап передбачає виявлення вторгнення. Оскільки АЕ навчається тільки на «нормальних» даних, тому втрати реконструкції для даних атаки є набагато вищими, ніж для «нормальних» даних, тобто:

$$Y_i = ((Y_P^{/}), (Y_q^{/})) \quad (21)$$

де $(Y_P^{/})$ – вектор «нормального» пакету даних, у яких помилка реконструкції менша, ніж граничне значення;

$(Y_q^{/})$ – вектор даних з вищою помилкою реконструкції, які вважаються «атаками».

Оскільки результат АЕ не є стовідсотково точним, як $(Y_P^{/})$, так і $(Y_q^{/})$ містять як дані про атаку, так і нормальні дані відповідно.

Для досягнення більшої точності, тобто виявлення більшої кількості вторгнень, ці два набори подаються на вхід двох модулів *iForest*. Перший модуль *iForest-1* отримує результати «атак» від АЕ і шукає нормальні точки даних. Другий модуль *iForest-2* бере вихід «нормальних» даних від АЕ і шукає атаковані точки даних. Дані атаки у наборі «нормальних» і нормальні дані у наборі «атак» є ніщо інше, як викиди або аномалії.

Модуль *iForest-2* бере «нормальний» набір $(Y_P^{/})$ і шукає дані про атаку. Оскільки АЕ вже ідентифікував більшість нормальних і атакованих пакетів на першому етапі, набір $(Y_P^{/})$ містить меншу кількість атакованих пакетів.

Набір $(Y_q^{/})$, що містить «атаковані» дані, подається на вхід *iForest-1*. $(Y_q^{/})$ також містить

деякі фактичні нормальні дані. *iForest-1* шукає ці «викиди» у $(Y_q^{'})$, тобто

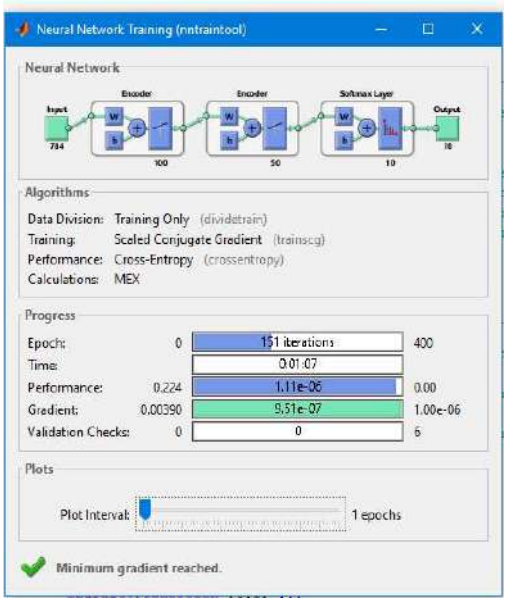
$$Y_P, O_q \leftarrow iForest - 1((Y_P^{'})) \quad (22)$$

$$Y_q, O_p \leftarrow iForest - 2((Y_q^{'})) \quad (23)$$

У кінцевому підсумку, (Y_P, O_q) і (Y_q, O_p) є остаточними наборами нормальних і шкідливих пакетів мережевого трафіку.

Toolbox програмного середовища MATLAB та натреновано з використанням набору даних UNSW-NB15. Результати тренування наведено на рисунку 1.

Математичну модель СВВ НМ було побудовано за допомогою пакету програм Neural Network.



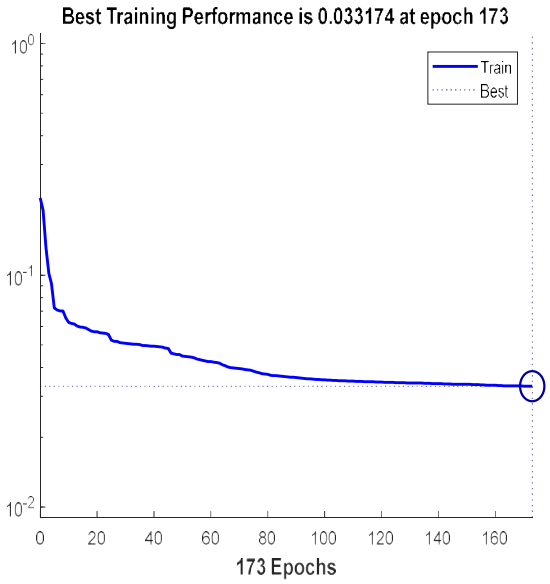


Рисунок 1 – Модель СВВ НМ та результати її тренування

Висновки й перспективи подальших досліджень

У цій статті представлено розроблену математичну модель системи виявлення вторгнення з використанням нейронної мережі на основі автоенкодерів, яка формалізує процес виявлення вторгнень у інформаційно-телекомунікаційних мережах військового призначення шляхом виявлення взаємозалежності між базовими атрибутами мережевого трафіку.

Системи виявлення вторгнень нейронних мереж поєднує в собі багатошарову згорткову нейронну мережу на основі автоенкодерів та мережу автоенкодерів з використанням довгострокової короткочасної пам'яті для виявлення просторово-часової залежності в даних мережевого трафіку. Продуктивність запропонованого підходу було оцінено з використанням набору даних UNSW-NB15.

Напрямом подальших досліджень є розроблення математичної моделі виявлення вторгнень на основі автокомпенсаційного принципу з використанням запропонованої в цій статті математичної моделі системи виявлення вторгнень на основі автоенкодерів.

Список бібліографічних посилань

1. Ahmad M., Basheri M. J. Iqbal, Rahim A. Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection, *IEEE Access*. 2018. № 6. 33789–33795. doi:10.1109/ACCESS.2018.2841987. **2. Auskalnis J., Paulauskas N., Baskys A.**, Application of local outlier factor algorithm to detect anomalies in computer network. *Elektronika ir Elektrotechnika*. 2018. №24(3). С. 96–99, cited By :2. **3. Rathore S., Park J. H.** Semi-supervised learning based distributed attack detection framework for iot, *Applied Soft Computing Journal*. 2018. № 72. С. 79–89, cited By :80. **4. Aliakbarisani R., Ghasemi A., Felix Wu S.** A data-driven metric learningbased scheme for unsupervised network anomaly detection. *Computers and Electrical Engineering*. 2019. №73. С. 71–83, cited By :7. **5. Karami A.,** An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities, *Expert Systems with Applications*. 2018. № 108. С. 36–60, cited By :28. **6. Alom M. Z., Bontupalli V., Taha T. M.** Intrusion detection using deep belief networks, in: 2015 *National Aerospace and Electronics Conference* (NAECON), 2015, pp. 339–344. doi:10.1109/NAECON.2015. 7443094. **7. Kang M.-J., Kang J.-W.** Intrusion detection system using deep neural network for in-vehicle network security. *PloS one*. 2016. № 11 (6). e0155781. **8. Gao N., Gao L., Gao Q., Wang H.** An Intrusion detection model based on deep belief networks, in: 2014 *Second International Conference on Advanced Cloud and Big Data, IEEE*. 2014. P. 247–252. **9. Zhang X., Chen J.** Deep learning based intelligent intrusion detection, in: 2017 IEEE 9th International

Conference on Communication Software and Networks (ICCSN), IEEE. 2017. P. 1133–1137. **10. Yu Y., Long J., Cai Z.** Network intrusion detection through stacking dilated convolutional autoencoders, Security and Communication Networks 2017.

MATHEMATICAL MODEL OF AN AUTOENCODER FOR ENSURING CYBERSECURITY OF MILITARY INFORMATION AND TELECOMMUNICATIONS NETWORK

Ilin Dmytro
Starinskyi Ivan ***(Candidate of technical sciences, senior researcher)***

National Defence University of Ukraine, Kyiv, Ukraine

The article demonstrates that the traffic of military-purpose Information and Telecommunication Networks (ITN) encompasses a substantial volume of data sets. Ensuring the security of military ITN against cyberattacks is a highly labor-intensive and error-prone process. In this context, network traffic data exhibit intricate nonlinear relationships that evolve over time. Existing cybersecurity models are based on data correlation models for traffic. These models often demand significant computational resources and do not permit real-time network traffic processing, neglecting spatiotemporal correlations within the data. To address this issue, a unified autoencoder, named Multi-Scale Convolutional Neural Network-Long Short-Term Memory Autoencoder (MSCNN-LSTM-AE), is proposed for anomaly detection in network traffic. The model initially employs a multi-scale convolutional neural network autoencoder (MSCNN-AE) to analyze the spatial features of the data set. Subsequently, the latent space features obtained from the MSCNN-AE are utilized in an autoencoder network based on Long Short-Term Memory (LSTM) for anomaly detection in network traffic. The model also employs two Isolation Forest algorithms as error correction mechanisms to address false positives and false negatives, thus enhancing detection accuracy. The evaluation of the NSL-KDD and UNSW-NB15 models on the CICDDoS2019 dataset indicates that the proposed mathematical model significantly outperforms existing mathematical models.

Keywords: *cybersecurity, cyberattack, cyber incidents, cyber threats, information security, cybersecurity strategy.*

References

1. Ahmad, M., Basheri, M. J. Iqbal, Rahim, A., (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection, IEEE Access 6 33789–33795. doi:10.1109/ACCESS.2018.2841987. **2. Auskalnis, J., Paulauskas, N., Baskys, A.,** (2018). Application of local outlier factor algorithm to detect anomalies in computer network. *Elektronika ir Elektrotechnika,* 24 (3), 96–99, cited By: 2. **3. Rathore S., Park J. H.,** (2018). Semi-supervised learning based distributed attack detection framework for IoT, *Applied Soft Computing Journal,* 72, 79–89, cited By: 80. **4. Aliakbarisani, R., Ghasemi, A., Felix Wu, S.,** (2019). A data-driven metric learning-based scheme for unsupervised network anomaly detection. *Computers and Electrical Engineering*, 73, 71–83, cited By: 7. **5. Karami, A.,** (2018). An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications* 108 36–60, cited By: 28. **6. Alom, M. Z., Bontupalli, V., Taha, T. M.,** (2015). Intrusion detection using deep belief networks. In: 2015 *National Aerospace and Electronics Conference (NAECON),* 339–344. doi:10.1109/NAECON.2015.7443094. **7. Kang M.-J., Kang J.-W.,** (2016). Intrusion detection system using deep neural network for in-vehicle network security. *PloS one,* 11(6), e0155781. **8. Gao, N., Gao, L., Gao, Q., Wang, H.,** (2014). An intrusion detection model based on deep belief networks. In: 2014 *Second International Conference on Advanced Cloud and Big Data, IEEE*, 247–252. **9. Zhang, X., Chen, J.,** (2017). Deep learning based intelligent intrusion detection. In: 2017 IEEE *9th International Conference on Communication Software and Networks (ICCSN), IEEE*, 1133–1137. **10. Yu, Y., Long, J., Cai, Z.** Network intrusion detection through stacking dilated convolutional autoencoders. *Security and Communication Networks*, 2017.

DOI: **10.33099/2311-7249/2023-47-2-119-124**

УДК 621.396

Марченко Андрій Олександрович *(кандидат технічних наук)* [1]
Войтко Віталій Віталійович *(кандидат технічних наук, старший дослідник)* [2]
Кузьменко Віталій Володимирович [3]

[1] ***Національний університет оборони України, Київ, Україна***
[2] ***Воєнна академія імені Євгенія Березняка, Київ, Україна***
[3] ***Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна***

РЕКОМЕНДАЦІЇ ЩОДО РОЗВИТКУ АНТЕННИХ СИСТЕМ ЗАСОБІВ РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ

У засобах радіорелейного зв'язку використовуються параболічні антени, що мають вузьку діаграму спрямованості, а також логоперіодичні та рефлекторні антени, які мають широкий промінь діаграми спрямованості. Але зазначені антени мають суттєвий недолік, оскільки мають лінійну поляризацію. Поширення електро-магнітних хвиль уздовж земної поверхні призводить до змінення виду поляризації внаслідок рефракції, при цьому енергетика сигналів зменшується. Тому під час передачі інформації існує проблемна ситуація, що обумовлена потребою забезпечення зв'язку в умовах поширення електро-магнітних хвиль над землею та забезпечення енергетичної доступності сигналів в умовах складної завадової обстановки. Метою статті є розроблення рекомендацій щодо розвитку антенних систем засобів радіорелейного зв'язку для усунення поляризаційної неузгодженості сигналів та антенних систем. Під час написання статті застосовано теоретичні методи, а саме аналіз досліджень і публікацій за антенною тематикою, аналіз побудови антенних систем радіорелейних станцій, їх узагальнення, пояснення виразу, що визначає дальність поширення електромагнітних хвиль у вільному просторі. Зазначений методологічний підхід дає змогу порівняти основні технічні характеристики, визначити переваги і недоліки конструкцій антен для досягнення мети статті. У роботі проведено аналіз конструктивних особливостей і технічних характеристик антенних систем засобів радіорелейного зв'язку, що формують діаграми спрямованості різної ширини та форми в заданих діапазонах робочих частот. Наведено основні переваги та недоліки цих антен. Зокрема зазначено, що загальним недоліком антенних систем засобів радіорелейного зв'язку є використання опромінювачів з лінійною поляризацією, що призводить до втрат потужності сигналів під час поширення електромагнітних хвиль уздовж земної поверхні. Для усунення такого негативного ефекту запропоновано використовувати адаптивні, за поляризацією, антенні решітки на основі поляризаційно-голографічних антен. Вплив поляризаційної неузгодженості засобів радіорелейного зв'язку розглянуто на основі аналізу залежності дальності від коефіцієнту поляризації. Крім того, показано, що для збільшення пропускної здатності цифрових радіорелейних станцій використовується технологія «Множинний вхід – множинний вихід», реалізувати яку можна за допомогою багатошарових поляризаційно-голографічних антен. Наведено основні переваги адаптивних антен. Розроблено рекомендації щодо напрямів подальшого розвитку антенних систем засобів радіорелейного зв'язку.

Ключові слова: *радіорелейний зв'язок, антенна система, електромагнітна хвиля, діаграма спрямованості, адаптивна антенна решітка, поляризація, поляризаційно-голографічна антена.*

Вступ

Постановка проблеми. Сьогодні основу системи радіозв'язку становлять засоби радіорелейного зв'язку (далі – РРЗ) різних типів, принципом роботи яких є ретрансляція (приймання, перетворення, підсилення та передавання) сигналу через ланцюг радіорелейних станцій (далі – РРС), розташованих у зоні прямої видимості.

Важливою складовою частиною кожної РРС є антенна система (далі – АС). У сучасних РРС використовуються дзеркальні антени, що характеризуються великим коефіцієнтом підсилення, вузькою діаграмою спрямованості (далі – ДС) та, як правило, лінійною поляризацією сигналів. Особливістю організації РРЗ є те, що електромагнітні хвилі (далі – ЕМХ) поширюються уздовж земної поверхні, водночас, поляризація випромінюваних сигналів може змінюватись, а рівень потужності прийнятих сигналів суттєво зменшуватись, що негативно впливає на стійкість та завадозахищеність зв'язку.

Разом із тим, у більшості РРС використовуються логоперіодичні та рефлекторні антени, що мають широкий промінь ДС і меншу ступінь завадозахищеності, порівняно з дзеркальними антенами, та потребують збільшення вихідної потужності передавальних систем для

забезпечення потрібної дальності радіорелейного зв'язку. Таким чином, під час організації РРЗ спостерігається проблемна ситуація, що обумовлюється потребою забезпечити стійкий та завадозахищений зв'язок в умовах сигнально-завадової обстановки, що постійно змінюється та ускладняються, а також – швидкої зміни місця розташування РРС для забезпечення реалізації усіх вимог, які висуваються до системи управління. Отже, питання, що пов'язані із забезпеченням стійкості та завадозахищеності зв'язку, реалізацією адаптивних методів приймання та обробки сигналів в умовах функціонування засобів РРЗ є важливими та першочерговими.

Звідси постає актуальне наукове та практичне завдання щодо побудови адаптивних АС, які відповідають вимогам завадозахищеності, швидкої та своєчасної зміни напрямку передавання інформації. Разом із тим, потрібно забезпечити стійке передавання інформації вздовж земної поверхні шляхом усунення поляризаційної неузгодженості сигналів та АС засобів РРЗ.

Аналіз останніх досліджень та публікацій. У роботі [1] розглянуто передумови забезпечення стійкого РРЗ та основні напрями його розвитку, наведено загальні відомості про новітні цифрові засоби радіорелейного зв'язку. Проте у статті не розглядаються антено-фідерні пристрої засобу РРЗ, як складова, від якої суттєво залежить якість передачі інформації, але зазначено, що перспективним напрямом розвитку є застосування адаптивної обробки сигналів.

Основні принципи побудови цифрових радіорелейних і тропосферних ліній зв'язку, а також напрямів їх розвитку викладені в [2]. Також наведено порядок розрахунку таких ліній та енергетичні співвідношення. Показано, що на завмирання сигналів впливають ДС антен, які обумовлені варіаціями кутів виходу і приходу ЕМХ, викликаними випадковими змінами рефракції. Водночас не зазначено як цей ефект можна усунути.

Аналіз каналу зв'язку проведений у [3], де описані джерела послаблення сигналів, втрати потужності прийнятих сигналів у трактах залежно від частоти тощо, але не зазначено як на потужність сигналів впливає неузгодженість поляризації.

У статті [4] проведено розрахунки очікуваної граничної дальності зв'язку для цифрових радіо-радіорелейних засобів при різних швидкостях передачі інформації, але втрати потужності за рахунок рельєфу прийнято рівними 0.

У [5] наголошено, що застосування перспективних адаптивних АС дає змогу формувати максимум ДС антени засобів РРЗ у потрібному напрямку та придушувати сигнали в напрямку дії завад шляхом формування провалів ДС, а також швидко переналаштовувати ДС для забезпечення роботи декількох РРС. Як висновок, запропоновано для підвищення стійкості та завадозахищеності засобів РРЗ використовувати адаптивні за поляризацією АС. Такі властивості мають поляризаційно-голографічні антени (далі – ПГА), за рахунок спірофазного ефекту [6]. Використання таких адаптивних антенних решіток дає змогу уникнути поляризаційної неузгодженості сигналів, що поширюються вздовж земної поверхні. Крім того, багатошарові поляризаційно-голографічні антени забезпечують одночасне передавання та приймання сигналів на різних робочих частотах [7].

Результати аналізу джерел свідчить, що для виконання поставленого наукового завдання постала потреба у проведенні аналізу конструкцій антенних систем РРС, порівнянні їх основних технічних характеристик, визначенні переваг і недоліків конструкцій антен, а також – розробленні рекомендацій щодо напрямів розвитку антенних систем засобів РРЗ.

Метою статті є розроблення рекомендацій щодо розвитку антенних систем засобів радіорелейного зв'язку на основі результатів аналізу конструктивних особливостей і тактико-технічних характеристик радіорелейних станцій для усунення поляризаційної неузгодженості сигналів та антенних систем засобів радіорелейного зв'язку.

Виклад основного матеріалу дослідження

Сьогодні для організації РРЗ застосовуються цифрові РРС різних типів, а саме: Р-414 МУ, Р-425С3, Р-450, Р-402 [1].

Антенна система РРС Р-414МУ складається з параболічної антени ANT2 0,6 15 HP з лінійним розміром 0,6 м і двох параболічних антен ANT2 1,2 6HPX з лінійним розміром 1,2 м [1; 9].

Перевагою антенної системи Р-414МУ є використання гостронаправлених параболічних антен з великим коефіцієнтом підсиленням, що забезпечує потрібну дальність передачі інформації при невеликих потужностях передавальних пристроїв. Недоліком АС є використання лінійно-поляризованих опромінювачів, які формують ЕМХ з вертикальною або горизонтальною поляризацію, що призводить до втрат енергетики сигналів під час їх поширення вздовж земної поверхні. Цей ефект частково усувається використанням поляризаційного селектора, який дає змогу приймати лінійно-поляризовані ЕМХ, але при цьому використовується додаткова приймально-передавальна апаратура.

Конструкція антени РРС Р-425С3 ідентична параболічній антені ANT2 1,2 6HPX, що використовується в РРС Р414МУ [9].

Антенна РРС Р-450 [10] є рефлекторною логоперіодичною, що забезпечує приймання і передачу радіосигналу з вертикальною або горизонтальною поляризацією. Поляризація антени визначається по розташуванню відбивачів рефлектора. Встановлення площини поляризації здійснюється шляхом відповідного приєднання антени до щогли під час розгортання РРС.

Конструкція антени РРС Р-450 є достатньо простою, але за рахунок невеликих лінійних розмірів формує широкий промінь діаграми спрямованості, тому потрібно збільшувати потужність передавальної системи для забезпечення впевненого приймання сигналів. Крім того, це підвищує можливості стосовно виявлення таких станцій і постановки радіозавад противником.

Антенна система РРС Р-402 складається з [8]:

гостронаправленої антени, яка призначена для концентрації радіосигналу у вузький промінь та використовується для побудови радіорелейних інтервалів довжиною до 35 км (режим роботи точка–точка).

секторної антени, що формує ДС з шириною $\Theta_E = 90°$ і використовується для побудови радіомережі з географічно-широкою зоною покриття. При цьому забезпечується робота віддалених станцій у кількості більше однієї (режим роботи точка–багатоточка).

всенаправленої антени, що має кругову ДС ($\Theta_E = 360°$) і призначена для створення покриття простору в районі розташування станції Р-402. У такому режимі станція Р-402 виконує роль точки доступу для абонентів та може підтримувати передачу інформації за технологією множинний вхід – множинний вихід (Multiple Input – Multiple Output) (далі – MIMO).

Основним недоліком антенної системи РРС Р-402 є використання секторної та всенаправленої антени, що формують секторну та кругову ДС відповідно. У цих антенах потужність радіосигналів розподіляється в широкому промені, що також призводить до зменшення дальності зв'язку або передачі інформації в небажаному напрямку зі зниженням ступеня завадозахищеності засобу радіозв'язку.

Результати аналізу конструктивних особливостей АС свідчать, що у РРС (Р-414 МУ, Р-425С3, Р-402) використовуються направлені АС, побудовані на основі дзеркальних параболічних антен, які мають властивість концентрації потужності радіосигналів у вузькому промені з шириною ДС $\Theta = 3–5°$ у потрібному напрямку (режим точка–точка) [1; 8; 9].

Загальним недоліком розглянутих антенних систем РРС є використання опромінювачів з лінійною (горизонтальною та/або вертикальною) поляризацією, що визначається напрямком орієнтації вектора електричної складової ЕМХ. Оскільки під час поширення ЕМХ уздовж нерівної поверхні землі, напрямок поляризації може суттєво змінюватись, то в таких умовах замість лінійно-поляризованих хвиль поширюються ЕМХ з довільною (невідомою) орієнтацією площини поляризації відносно горизонту, що призводить до зменшення рівня прийнятого сигналу і, як наслідок, дальність зв'язку може зменшуватися.

Такий ефект доцільно розглянути на основі аналізу виразу, що визначає дальність поширення ЕМХ у вільному просторі [11]:

$$D_p = \lambda/4\pi \sqrt{\frac{P_a G_a G_p}{n P_{\min}} \gamma_{\text{п}} a_p}\,, \qquad (1)$$

де λ – робоча довжина хвилі РРС;

Pa – потужність, що випромінюється РРС;

a_p – коефіцієнт передачі потужності сигналу в антено-фідерного пристрою приймальної РРС;

G_a – коефіцієнт підсилення антени передавальної РРС;

G_p – коефіцієнт підсилення антени приймальної РРС;

P_{min}– чутливість приймального пристрою РРС;

n – коефіцієнт перевищення потужності сигналу над чутливістю приймального пристрою РРС;

$\gamma_{\text{п}}$ – коефіцієнт узгодженості поляризації антен радіорелейних станцій. Як правило, під час розрахунків його вважають за величину 0,5 [11].

Слід зазначити, що у виразі (1) не враховано поглинання ЕМХ в атмосфері. У цьому виразі найбільший інтерес викликає вплив коефіцієнту узгодженості поляризації антен $\gamma_{\text{п}}$ на дальність D_p.

Характеристики АС засобів РРЗ, що використовувались як ввідні дані для розрахунку залежностей дальності зв'язку від коефіцієнту узгодженості поляризації антен радіорелейних станцій наведений у таблиці 1.

Аналіз наведених графічних залежностей (рис. 1) свідчить, що на дальність поширення ЕМХ може суттєво впливати поляризаційні характеристики АС засобів РРЗ. Вплив поляризаційної неузгодженості засобів РРЗ на рівень сигналів доцільно зменшувати використанням гостронаправлених АС, що забезпечують приймання сигналів незалежно від напрямку вектора електричної складової ЕМХ [13].

Таблиця 1

Ввідні дані для розрахунку залежностей дальності зв'язку від коефіцієнту узгодженості

Тип РРС		Характеристика антенної системи						
		Тип антени	Поляризація	Ширина ДС, град	Коефіцієнт підсилення антени, дБі	Довжина хвилі, м	Потужність передавача, дБм	Чутливість приймача, Вт
Р-402	Р-402.01	параболічна	лінійна	$\Theta_E = \Theta_H$=5	28	0,052	до 29	10×10^{-13}
	Р-402.02	секторна	лінійна	Θ_E = 90 (120)	20 (16)	0,055	до 27	10×10^{-13}
	Р-402.04	всенаправлена	лінійна	Θ_E =360	13	0,055	до 27	10×10^{-13}

Продовження таблиці 1

Тип РРС		Характеристика антенної системи						
		Тип антени	Поляризація	Ширина ДС, град	Коефіцієнт підсилення антени, дБі	Довжина хвилі, м	Потужність передавача, дБм	Чутливість приймача, Вт
Р-414 МУ	ВО-15	параболічна Ø0,6 м	лінійна	$\Theta_E = \Theta_H \approx 3$	30	0,201	28±1	10×10^{-13}
	ВО-6С	параболічна Ø 1,2 м	лінійна (горизонтальна та вертикальна)	$\Theta_E = \Theta_H = 3,3$	35	0,044	30	10^{-6}
Р-425СЗ		параболічна Ø 1,2 м	лінійна	$\Theta_E = \Theta_H = 3,3$	35	0,044	30	10^{-6}
Р-450		рефлекторна логоперіодична	лінійна (вертикальна/ горизонтальна)	$\Theta_E = \Theta_H = 5$	20	0.15	35	10×10^{-13}

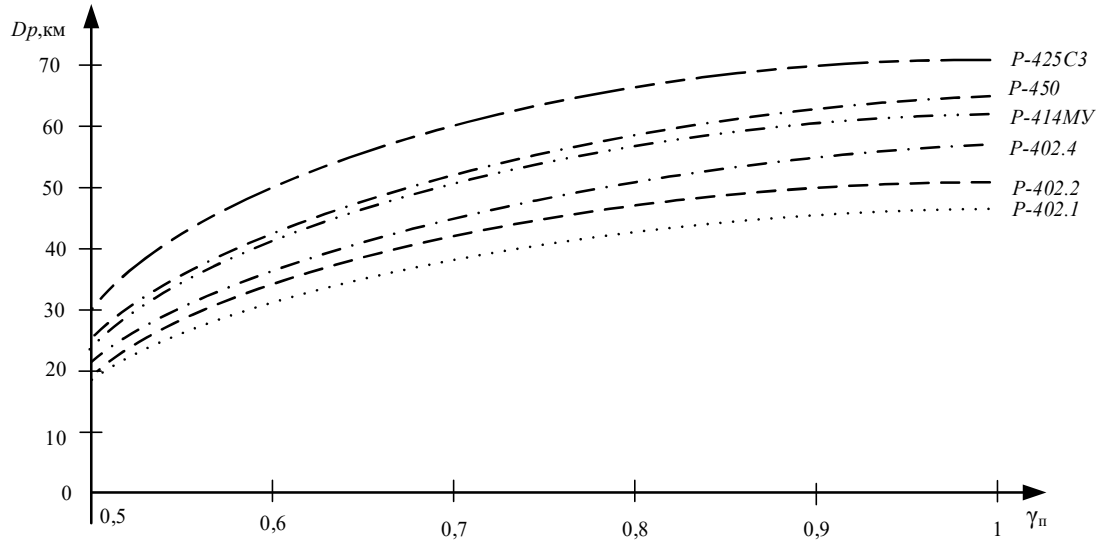


Рисунок 1 – Залежність дальності зв'язку від коефіцієнту узгодженості поляризації антен РРС

Крім того, до засобів РРЗ висувається ряд вимог щодо високої бойової готовності, пропускної здатності, стійкості, мобільності, доступності, завадозахищеності, а також можливості забезпечення швидкої та своєчасної зміни напрямку передачі інформації в разі втрати зв'язку з абонентом або під час зміни місця розташування приймальної станції [1].

Сьогодні, для збільшення пропускної здатності цифрових РРС достатньо часто використовуються технологія MIMO, що реалізує передачу інформації декількома рознесеними передавальними і приймальними антенами (рис. 2) [13].

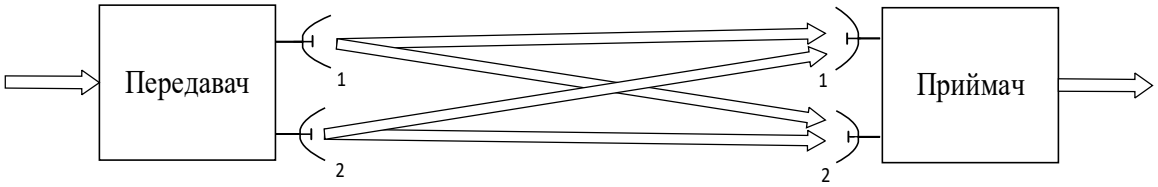


Рисунок 2 – Передача інформації за технологією MIMO

Недоліком технології MIMO є те, що для забезпечення зв'язку використовуються додаткові передавальна та приймальна антени, що, зі свого боку, призводить до збільшення кількості антен у радіорелейній лінії. Усунення наведених недоліків АС, забезпечення вимог щодо завадозахищеності засобів РРЗ і швидкої зміни напрямку передачі інформації, а також оптимізація кількості антен у РРС потребує нових підходів до побудови АС засобів РРЗ.

Перспективним напрямом розроблення нових і удосконалення існуючих РРС може бути побудова адаптивних систем передавання (приймання) та обробки сигналів. Процес адаптації залежить від певних факторів, а саме: реалізованих методів адаптації, типу пристрою формування (обробки) сигналів, принципів побудови адаптивної антени та її елементів.

До переваг адаптивних антен слід віднести: усунення ефекту багатопроменевості, розширення

зони обслуговування однієї РРЗ, оперативне регулювання потужністю випромінювання, збільшення кількості одночасно працюючих абонентів, підвищити пропускну здатність каналів управління та передачі, усунути вплив внутрішніх і міжсистемних завад, що діють у смузі частот корисного сигналу, вирівняння потужності від абонентів, розташованих на різних відстанях, розв'язання задачі визначення місцеположення тощо. Такі можливості можна реалізовувати через настроювання адаптивних антенних решіток (далі – АР) на ефективне приймання корисного сигналу і придушення завад.

Крім того, в сучасних цифрових системах зв'язку для підвищення пропускної здатності та спектральної ефективності отримала розвиток технологія Massive (широкомасштабний) MIMO, яка дає змогу використовувати набагато меншу кількість терміналів користувачів, чим кількість антен. Massive MIMO реалізується використанням багатоелементних цифрових АР, в яких адаптація здійснюється ваговою обробкою цифрових масивів напруг.

Основними рекомендованими напрямами подальшого розвитку АС для створення (проєктування) нових, удосконалення (модернізації) існуючих РРС, що входять до складу мереж РРЗ чи комплексів зв'язку, слід вважати:

заміну антен з широким променем ДС (Р-450) на гостронаправлені (дзеркальні) з одночасним використанням систем автоматичного повороту (юстирування) АС за азимутом і кутом місця, що дасть змогу зменшити потужність передавальних систем під час забезпечення потрібної дальності передачі інформації;

використання плоских (планарних) АС (для РРС Р-402, Р-414МУ, Р-425 тощо), наприклад, на основі поляризаційно-голографічних антен, які дають змогу обробляти сигнали як з лінійною, так і з коловою (еліптичною) поляризацією, що забезпечує впевнене приймання при заданій дальності передачі інформації [12];

розроблення (конструктивний синтез) багатошарових поляризаційно-голографічних антен [7] для забезпечення передачі інформації за технологією MIMO;

конструктивний синтез адаптивних АР, зокрема цифрових, для побудови адаптивних мереж РРЗ [13]. Використання адаптивних АР дає змогу змінювати напрямок і потужність випромінювання сигналів, підвищити завадозахищеність засобів РРЗ та оптимізувати кількість антен цих засобів.

Висновки й перспективи подальших досліджень

Використання поляризаційно-голографічних антен, які за своїми властивостями відповідають дзеркальним антенам, дає змогу уникнути поляризаційної неузгодженості електромагнітної хвилі, що поширюються вздовж земної поверхні та приймальних антен засобів радіорелейного зв'язку. Також багатошарові поляризаційно-голографічні транспаранти (відбивачі) можуть забезпечити передачу інформації декількома каналами на різних робочих частотах.

Застосування адаптивних антенних решіток дає змогу формувати максимум діаграми спрямованості антени засобів радіорелейного зв'язку в потрібному напрямку передачі інформації та подавляти сигнали в напрямку дії завад шляхом формування провалів у характеристиках спрямованості антен, а також здійснювати швидке переналаштування (сканування) діаграми спрямованості для забезпечення роботи декількох радіорелейних станцій.

Основними напрямами подальшого розвитку антенних систем є створення (проєктування) нових, удосконалення (модернізації) існуючих антенних систем радіорелейних станцій, що входять до складу мереж (комплексів) радіорелейного зв'язку.

Список бібліографічних посилань

1. Кушнір О. І., Васюта К. С., Озеров С. В., Литвин А. В., Северілов А. В. Основні тенденції та перспективи розвитку військового радіорелейного зв'язку. *Збірник наукових праць Харківського університету Повітряних Сил.* Харків: ХНУПС, 2017. № 4. С. 7–11. **2. Наритник Т. М., Почерняєв В. М., Повхліб В. С.** Цифрові радіорелейні та тропосферні лінії зв'язку. Одеса : ОНАЗ ім. О. С. Попова, 2019. С. 27–32. **3. Sklar B., Harris F. J.** Digital Communications: Fundamentals and Applications. 3-ed ed. Chicago, USA : Pearson, 2021. 2287 p. **4. Гурський Т. Г., Степаненко Є. О., Шишацький А. В.** Оцінка граничної дальності зв'язку на сучасних радіо- та радіорелейних лініях. *Збірник наукових праць ВІТІ.* Київ, 2019. Вип. 1. С 6–17. **5. Марченко А. О., Войтко В. В., Буяло О. В., Семібаламут К. М.** Шляхи підвищення стійкості та завадозахищеності радіорелейного зв'язку. Тези Міжнародної науково-практичної конференції «Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану». (24 листопада 2022 року). Хмельницький : НАДПСУ, 2023. С. 891–893. **6. Замятин В. И., Гусак Ю. А.** Поляризационно-голографические антенны: методы расчета и возможные конструкции. *Радиоэлектроника*, 1996. № 10. С. 19–26. **7. Марченко А. О., Гусак Ю. А., Войтко В. В.** Багатошарова поляризаційно-голографічна антена : пат. 142499 Україна : H01Q 15/24. № u 2019 11692 ; заявл. 06.06.2019 ; опубл. 10.06.2020, Бюл. № 11. 8 с. **8. Вакуленко О. В., Ніколаєнко Б. А.** Станція радіорелейна широкосмугова СРШ-5000 (станція радіорелейна Р-402). Навч. посіб. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2019. 85 с. **9. Нестерук.** Радіорелейна станція Р-425С3. Посібник з експлуатування. Харків: ХНУПС, 2015. 69 с. **10. Краснер Є. Ю.** Станція радіорелейна Р-450. Посібник з експлуатації. Харків: ХУПС, 2007. 56 с. **11. Смирнов Ю. А.** Радиотехническая разведка. Москва : Воениздат, 2001. 456 с. **12. Гусак Ю. А., Марченко А. О.** Застосування поляризаційної голографії при побудові антен в системах радіозв'язку. *Збірник наукових праць ВІТІ НТУУ «КПІ».* Київ, 2011. Вип. 3. С 23–27. **13. Sathish Ch.** Adaptive antenna arrays : trends and applications / editor Ch. Sathish. New York : Springer-Verlag Berlin, 2004. 661 p. URL: file:///C:/Users/НДВ/Downloads/vdoc.pub_adaptive-antenna-arrays-trends-and-applications.pdf (дата звернення: 29.05.2023).

RECOMMENDATIONS FOR THE DEVELOPMENT OF ANTENNA SYSTEMS FOR RADIO RELAY COMMUNICATION MEANS

Marchenko Andrii, *(Candidate of technical sciences)* [1]
Voytko Vitalii, *(Candidate of technical sciences, senior researcher)* [2]
Kuzmenko Vitalii [3]

[1] *National Defence University of Ukraine, Kyiv, Ukraine*
[2] *Yevgeny Berezniak Military Academy, Kyiv, Ukraine*
[3] *Institute of special communication and information protection National Technical University of Ukraine «Ihor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine*

In radio relay communications, parabolic antennas with a narrow radiation pattern are used, as well as log-periodic and reflector antennas with a wide beam pattern. However, these antennas have a significant drawback, as they have linear polarization. The propagation of electromagnetic waves along the earth's surface leads to a change in the type of polarization due to refraction, while the energy of the signals decreases. Therefore, during the transmission of information, there is a problematic situation due to the need to ensure communication in the conditions of propagation of electromagnetic waves over the ground and to ensure the energy availability of signals in a complex interference environment. The purpose of the article is to develop recommendations for the development of antenna systems for radio relay communication to eliminate the polarization mismatch of signals and antenna systems. In writing the article, theoretical methods were used, namely, analysis of research and publications on the antenna subject, analysis of the construction of antenna systems of radio relay stations, their generalization, and explanation of the expression that determines the range of propagation of electromagnetic waves in free space. This methodological approach makes it possible to compare the main technical characteristics, determine the advantages and disadvantages of antenna designs to achieve the goal of the article. The paper analyzes the design features and technical characteristics of antenna systems of radio relay communication means that form radiation patterns of various widths and shapes in the specified operating frequency ranges. The main advantages and disadvantages of these antennas are presented. In particular, it is noted that a common disadvantage of antenna systems for radio relay communication is the use of linearly polarized irradiators, which leads to signal power losses during the propagation of electromagnetic waves along the earth's surface. To eliminate this negative effect, it is proposed to use adaptive polarization-based antenna arrays based on polarization-holographic antennas. The influence of polarization inconsistency of radio relay communication means is considered on the basis of the analysis of the dependence of the range on the polarization coefficient. In addition, it is shown that to increase the throughput of digital radio relay stations, the multiple input-multiple output technology is used, which can be realized using multilayer polarization-holographic antennas. The main advantages of adaptive antennas are presented. Recommendations on the directions of further development of antenna systems for radio relay communication are developed.

Keywords: *radio relay communication, antenna system, electromagnetic wave, directional pattern, adaptive antenna array, polarization, polarization-holographic antenna.*

References

1. Kushnir, O. I., Vasyuta, K. S., Ozerov, S. V., Lytvyn, A. V., Severilov, A. V., (2017). The main trends and prospects for the development of military radio relay communication, *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*. Kharkiv : KhNUPS, 4, 7–11. **2. Narytnyk, T. M., Pochernyayev, V. M., Povkhlib, V. S.,** (2019). Digital radio relay and tropospheric communication lines. Odesa : ONAZ im. O. S. Popova, 27–32. **3. Sklar, B., Harris, F. J.,** (2021). *Digital Communications: Fundamentals and Applications*. 3-ed ed. Chicago, USA : Pearson, 2287. **4. Hurskyi, T. G, Stepanenko, E. O, Shishatskyi, A. V.,** (2019). Evaluation of boundary communication range of modern radio and radio relay links. *Zbirnyk naukovykh prats VITI*. Kyiv : VITI, 1, 6–17. **5. Marchenko, A. O., Voytko, V. V., Buialo, O. V., Semibalamut, K. M.,** (2023). Ways of increasing the stability and immunity of radio relay communication. *Tezy Mizhnarodnoi naukovo-praktychnoi konferentsii «Sektor bezpeky i oborony Ukrainy na zakhysti natsionalnykh interesiv: aktualni problemy ta zavdannia v umovakh voiennoho stanu»*. Khmelnytskyi : NADPSU (24 November 2022), 891–893. **6. Zamyatin, V. I. Gusak, YU. A.,** (1996). Polarization-holographic antennas: calculation methods and possible designs. *Radioelektronyka*. 10, 19–26. **7. Marchenko, A. O. Husak, Yu. A., Voytko, V. V.,** (2020). Bahatosharova polyaryzatsiyno-holohrafichna antena: *pat* 142499 Ukraina : H01Q 15/24, № u 2019 11692, zaiavl. 06.06.2019, opubl. 10.06.2020, 11, 8. **8. Vakulenko, O. V., Nikolaienko, B. A.,** (2019). Broadband radio relay station SRS-5000 (radio relay station R-402). Navch. posib. Kyiv : ISZZI KPI im. Ihoria Sikorskoho, 85 . **9. Nesteruk,** (2015). Radio relay station R-425C3. *Posibnyk z ekspluatuvannia*. Kharkiv : KhNUPS, 69. **10. Krasner, E. Yu.,** (2007). Radio relay station R-450. *Posibnyk z ekspluatatsiyi*. Kharkiv : KHUPS. 56. **11. Smyrnov, Yu. A.,** (2001). Radyotekhnycheskaia razvedka. Moskva : Voenyzdat, 456. **12. Husak, Yu. A., Marchenko, A. O.,** (2011). The use of polarization holography in the construction of antennas in radio communication systems. *Zbirnyk naukovykh prats VITI NTUU «KPI»*. Kyiv : VITI NTUU «KPI», 3, 23–27. **13. Sathish, Ch.,** (2004). Adaptive antenna arrays : trends and applications / editor Ch. Sathish. New York : Springer-Verlag Berlin, 661. URL: file:///C:/Users/НДВ/Downloads/vdoc.pub_adaptive-antenna-arrays-trends-and-applications.pdf (дата звернення: 29.05.2023).

DOI:**10.33099/2311-7249/2023-47-2-125-132**

УДК 355.1: 351.86

Артамощенко Вадим Станіславович *(кандидат військових наук, доцент)*

Національний університет оборони України, Київ, Україна

МОДЕЛЬ СИСТЕМИ ВІЙСЬКОВОЇ ОСВІТИ НА ОСНОВІ ЛАНЦЮГА МАРКОВА

Підготовка військових кадрів сил оборони з використанням уроків здобутих під час відсічі збройній агресії російської федерації, методики підготовки, принципів і стандартів НАТО є одним із завдань розвитку військової освіти. Розвиток системи військової освіти передбачає системні зміни та управління змінами. Прогнозування можливих ефектів, отриманих внаслідок впровадження змін, вимагає побудови моделі системи військової освіти. Метою статті є розроблення моделі системи військової освіти для прогнозування ефектів, отриманих внаслідок впровадження змін у процесах її розвитку. У статті застосовано метод оцінювання спільних спроможностей системи військової освіти. Процес формування спроможностей системи військової освіти подано абстрактною моделлю, що відображає сукупність елементів системи та складників її спроможностей. Складові системи військової освіти розподілені за трьома рівнями ієрархії: державний, відомчий та інституційний. Автор пропонує стратегічну мету та окремі цілі розвитку системи військової освіти здійснити за таксономічною моделлю «дерева цілей». Також, за підходами прийнятими у теорії ймовірності та рівномірної шкали оцінювання ймовірності настання випадкової події, запропоновано «модель ABCD» для опису критеріїв визначення рівня відповідності складових спроможностей системи військової освіти. Для оцінювання стану елементів спроможності системи використано ланцюг Маркова з дискретним станом та дискретним часом. Описано матрицю вектору переходу елементу спроможності на кожному кроці зміни з урахуванням імовірностей переходу елементу спроможностей з одного стану в інший через впровадження певної зміни. Модель дає змогу прогнозувати отримані ефекти внаслідок запроваджених змін та стан елемента спроможності у процесах розвитку системи військової освіти.

Ключові слова: *модель, спроможності, система військової освіти, ланцюг Маркова.*

Вступ

Розвиток сектору безпеки і оборони та нарощування спроможностей сил оборони за нормами, принципами й стандартами НАТО, що були закріплені рішеннями Ради національної безпеки і оборони України [1; 2] набули більшої актуальності під час відсічі збройній агресії російської федерації.

Системи протиповітряної оборони, авіаційні, ракетні та артилерійські системи, бойові броньовані машини й інше озброєння у поєднанні з автоматизацією процесів розвідки та ураження противника, змінюють тактику дій, процеси і процедури планування, стратегію досягнення цілей у протистоянні з агресором, визначають об'єктивну необхідність оновлення процедур ухвалення військових рішень, розвідки, об'єднаної вогневої підтримки, логістики та інших сфер діяльності відповідно до стандартів НАТО. Це все обумовлює потребу розвитку системи підготовки військових кадрів в інтересах сил оборони.

Підготовка військових кадрів для сил оборони здійснюється в системі військової освіти, яка з одного боку, є складником системи освіти держави, з іншого – перебуває на шляху професіоналізації, приведення її структури і змісту до стандартів, підходів та принципів, що впроваджені у країнах – членах НАТО. Такий напрям закріплено в Концепції трансформації системи військової освіти [3].

Постановка проблеми. Система військової освіти (далі – СВО) є складником спеціалізованої освіти військового профілю, призначена для підготовки військових кадрів сектору безпеки і оборони та являє собою сукупність рівнів і ступенів освіти, кваліфікацій, освітніх програм, стандартів освіти, ліцензійних умов, військових закладів освіти та інших суб'єктів освітньої діяльності, учасників освітнього процесу, державних органів та органів військового управління сектору безпеки і оборони, а також нормативно-правових актів, що регулюють відносини між ними [4].

Система військової освіти охоплює різні складові, розподілені за рівнями. Елементи СВО об'єднані зв'язками та залежні один від одного. СВО становить єдність закономірно розташованих і взаємопов'язаних складових елементів, компонентів та підсистем, що дає можливість стверджувати, що вона є складною системою.

Завдання розвитку СВО орієнтовані на отримання кінцевого продукту, а саме вмотивованого та професійного персоналу сил оборони. Для досягнення цього відбуватимуться організаційні та системні зміни СВО.

Реалізація концептуальних засад розвитку СВО тісно пов'язана з управлінням змінами, що є сукупністю процесів впливу керуючої системи на організацію через зміни у внутрішньому та зовнішньому середовищі, корегуванням діяльності,

оновлення структур, пошуком нових можливостей відповідно до вимог та запитів [5]. Водночас СВО виконує завдання підготовки військових кадрів відповідно до сучасних вимог, адже зміни та результати таких змін мають відповідати стратегічній меті розвитку СВО. Отже, для чіткого розуміння побудови СВО та подальшого оцінювання результатів її розвитку необхідно усвідомити систему в цілому, виділити її елементи і зв'язки між ними. Це дає можливість прогнозувати заплановані зміни та очікувані ефекти (наслідки) впровадження змін. Таке усвідомлення є можливим завдяки побудові моделі СВО.

Відомо, що моделювання, як метод наукового пізнання, дає змогу відтворити об'єкт дослідження. Воно широко використовується в дослідженні систем різної природи, але особливого значення набуває в межах методології системного підходу.

Аналіз останніх досліджень і публікацій. Проведемо аналіз наукових праць, що були присвячені моделюванню у сфері військової освіти, зокрема у СВО.

Моделюванню у сфері підготовки військових кадрів присвячено монографію авторського колективу під керівництвом І. С. Романченка [6]. В монографії представлено розроблений математичний апарат дослідження проблем кадрового менеджменту у військовій сфері, основними складовими якого є математичні моделі процесів кадрового менеджменту (переміщення, підготовки, накопичення тощо). Автори описують процес проходження військової служби математичною моделлю на основі однорідного марковського ланцюга з постійною функцією поповнення станів та безперервним часом. Математична модель процесу підготовки осіб офіцерського складу включає в себе марковську модель без поповнення станів і безперервним часом та стохастичну багатоперіодну оптимізаційну модель. В моделі використовується три рівня підготовки офіцерів: оперативно-стратегічний, оперативно-тактичний і тактичний. За результатами моделювання автори обґрунтовують обсяги державного замовлення на підготовку осіб офіцерського складу для Збройних сил України (далі – ЗС України) з урахуванням термінів їх підготовки за трьома рівнями військової освіти. Отже, основне призначення моделі підготовки – обґрунтувати порядок формування державного замовлення на підготовку офіцерів у системі кадрового менеджменту у військовій сфері.

У монографії авторського колективу під керівництвом В. Телелима та Д. Вітера [7] до СВО входять три функціональні складові: вища освіта, професійна військова освіта та підвищення кваліфікації. Виходячи з цього, автори формують візуальну модель СВО та підготовки офіцерського складу за складовими підготовки офіцерів. Інші складові підготовки у СВО, у тому числі допризовна підготовка, а також підготовка осіб рядового складу, сержантського (старшинського) складу авторами монографії не розглядається. Тому, така модель не дає змогу оцінити СВО.

Науковець М. Нещадим висвітлює модель СВО, як об'єкт управління [8]. У цій моделі визначено входи до системи, виходи з неї, її зовнішнє середовище. Входами до системи автор вважає ресурсне забезпечення функціонування системи, що включає людські, фінансово-матеріальні, інтелектуальні, духовні та часові ресурси. До виходів із системи автор відносить результати функціонування системи, що забезпечує перетворення витрачених ресурсів на кінцевий продукт, а саме кадровий, матеріальний, інтелектуальний, духовний, нормативно-правовий потенціали збройних сил. Зовнішнє середовище, яке впливає на СВО, вчений поділяє на дві частини: прямого і непрямого впливу. Середовищем прямого впливу він називає: концептуальні акти, нормативно-правову база, органи управління Міністерства оборони України (далі – МО України) і Міністерства освіти і науки України (далі – МОН України), економіку держави. Середовищем непрямого впливу – світову науку і систему освіти, соціокультурне середовище, військово-політичну обстановку тощо.

Крім цього, М. Нещадим описує методологічну модель аналізу стану і розвитку СВО на основі аналізу графа відносин між елементами системи на засадах аналізу ієрархій. Автор відокремлює суб'єкти управління СВО (органи влади, органи управління, керівництво закладами освіти) та об'єкти управління (заклади освіти, науково-педагогічні працівники, слухачі, курсанти, тощо) та описує відносини управління (процес стійких взаємозв'язків, що формується у процесі взаємодії суб'єкта та об'єкта управління. Сама система розглядається як об'єкт управління.

В основу проєктування СВО покладено системний підхід. На стадії проєктування СВО використовується функціональне моделювання на основі інформаційної технології моделювання складних систем, особливістю якого є поступове введення дедалі більших рівнів декомпозиції. Складовими у процесах моделювання СВО розглядаються заклади освіти, нормативно-правова база, органи управління, а також зв'язки між внутрішніми та зовнішніми елементами середовища.

Досягнення М. Нещадима у розробленні методологічних засад створення СВО не викликає сумніву. Його дослідження є науковим супроводженням процесів, які відбувались у СВО України на початку XXI ст. та не можуть бути повною мірою застосовані в сучасних умовах.

Науковець С. Полторак [9] обґрунтовує евристичну модель уніфікації механізмів державного управління професійною підготовкою кадрів у системі вищої військової освіти. Ефективність державного регулювання такою системою визначається на основі критеріїв, узагальнених підкритеріїв та показників ефективності, які розташовані за підпорядкованістю на різних рівнях ієрархії. У дослідженні діяльність системи вищої військової освіти представлено одночасно як об'єкта, так і

суб'єкта реформування сил оборони, а якість підготовки військових кадрів вважається умовою ефективності оборонної реформи.

Науковець О. Устименко досліджує СВО, як суб'єкт державного управління на основі моделі державного управління, яка побудована за рівнями ієрархії [10]. Вищий рівень ієрархії – суб'єкти державного управління СВО: Президент України, Верховна Рада України, Кабінет Міністрів України, МОН України, МО України, Генеральний штаб ЗС України. Наступною групою суб'єктів управління є органи військового управління та Департамент військової освіти і науки МО України. До об'єктів управління автор відносить вищі військові навчальні заклади, військові навчальні підрозділи закладів освіти та наукові установи. Модель наведена О. Устименком відображає підпорядкованість у СВО за трьома рівнями ієрархії, що може бути використано у подальшому дослідженні.

У монографії [5] автори наводять концептуальну модель управління змінами у СВО, як комплексний опис сукупності структурних компонентів управлінського циклу щодо впровадження змін у СВО в умовах впливу чинників зовнішнього і внутрішнього середовищ. Водночас вона не дає можливості прогнозувати результати змін.

Питання моделювання у сфері військової освіти розглядається ще у кількох наукових працях. Водночас у своїй більшості мова йде про моделі підготовки військових кадрів. Так, у науковій праці [11] автори розробляють адаптивну модель розвитку професійної військової освіти на основі принципу «outcome-based», що у подальшому стає підґрунтям для формування кваліфікаційних вимог професійної підготовки офіцерів та військових фахівців. Статтю авторського колективу [12] присвячено формуванню моделі професійної військової освіти. Автори описують модель підготовки офіцерського складу за відповідними рівнями та формують професійні компетентності. Однак, крім освітніх програм підготовки офіцерів, інші елементи СВО не розглядаються. У наукових статтях [13; 14] автори досліджують застосування ланцюгів Маркова для оцінки їх результативності окремих проєктів, у тому числі, для відображення ступеня досконалості організаційно-технічних систем у сфері освіти. Аналогічний підхід може бути застосованим для моделювання у сфері СВО.

Таким чином, результати аналізу наукових робіт та публікацій свідчать про те, що переважна більшість науковців моделюють процес підготовки фахівців сектору безпеки і оборони держави. Крім того, СВО розглядається як об'єкт та суб'єкт управління, а моделювання процесів розвитку залишалося поза увагою науковців. Водночас, сьогодні існує ряд нових умов функціонування та складових СВО, які не відображались у попередніх моделях. Зокрема, це діяльність СВО під час відсічі збройній агресії та євроатлантична інтеграція України. Отже, проблемним залишається питання моделювання змін СВО у процесах її розвитку та прогнозування ефектів, отриманих внаслідок впровадження змін.

Метою статті є розроблення моделі системи військової освіти на основі ланцюгів Маркова для прогнозування ефектів, отриманих внаслідок впровадження змін у процесах її розвитку.

Виклад основного матеріалу дослідження

Функціонування СВО у цілому орієнтоване на формування сукупного продукту – підготовленого персоналу. Водночас вимірювання та оцінювання її окремих елементів (освітні програми, заклади освіти, тощо) не дає уявлення про стан системи у цілому, тому СВО оцінюватиметься за її спроможностями, які полягатимуть у здатності до підготовки персоналу в інтересах сектору безпеки і оборони України.

Спроможності СВО формуватимуться спільно всіма елементами, а оцінюватимуться за складниками DOTMLPFI (doctrine – доктрини, organization – організація, training – підготовка, materiel – забезпечення, leadership – керівництво, personnel – персонал, facilities – інфраструктура, interoperability –сумісність), який застосовується в багатьох країнах-членах НАТО [15].

Процес формування спроможностей СВО може бути представлено абстрактною моделлю, яка у цілому відображатиме сукупність елементів СВО та складників її спроможностей (рис. 1).

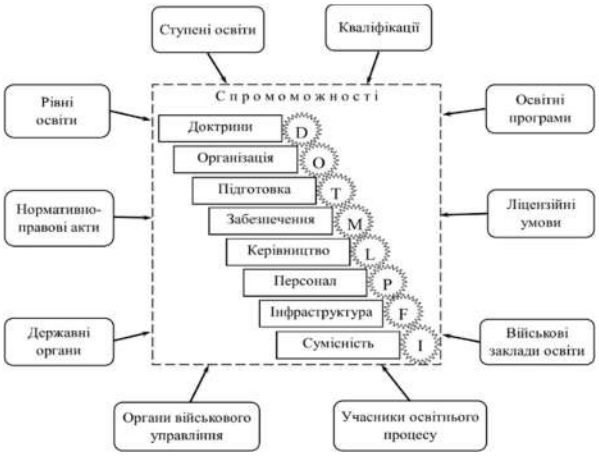


Рисунок 1 – Абстрактна модель формування спроможностей системи військової освіти

Висновки з аналізу умов функціонування та результати вивчення досліджень у сфері військової освіти свідчать про те, що СВО є багаторівневою. На кожному рівні розташовуватимуться її складові елементи, що вказуватимуть на зв'язки та залежності між ними.

Декомпозиція складових СВО на три рівні ієрархії (державний, відомчий та інституційний) дозволятиме відобразити місце, де формуватиметься зміна та місце, де така зміна надаватиме новий ефект (результат), прогноз впливу цього ефекту й висновок щодо доцільності такої зміни, зокрема, чи буде це пов'язано із набуттям нових спроможностей, а саме, з процесом розвитку СВО.

Відомо, що реалізація концепцій, в яких поєднуються цільові, системні та інтегральні підходи діяльності організацій пов'язана зі стратегічним управлінням [16]. Стратегічне управління є багаторівневим управлінським процесом, який сприяє формуванню та реалізації стратегій і концепцій. Отже, реалізацію концепції розвитку СВО слід розглядати через призму стратегічного управління. Запровадження такого управління до процесу управління розвитком СВО потребує узагальнення основних управлінських процесів, зокрема стратегічного аналізу, визначення мети і цілей, формування стратегії й концепції, впровадження змін та їх моніторинг [16; 17].

Оскільки досягнення стратегічної мети розвитку СВО є складним, багатоаспектним завданням, доцільно здійснити її декомпозицію. Тобто розподілити на кілька цілей та конкретизувати бажані ефекти впровадження змін та сукупний ефект. Такий метод, що отримав назву «дерево цілей», широко застосовують в практиці управління державних та економічних структур. За допомогою «дерева цілей» описують їх впорядковану ієрархію та послідовну декомпозицію стратегічної мети на часткові цілі з дотриманням певних принципів [18]:

під час декомпозиції стратегічної мети враховується, що реалізація цілей нижчого рівня є умовою досягнення цілей вищого рівня;

формулювання цілей описується через бажані результати, а не способи їх досягнення;

формулювання цілей здійснюється із врахуванням реальних ресурсів;

цілі одного рівня не мають бути взаємозалежними і перетинатися;

на найнижчому рівні «дерева цілей» описується завдання конкретних виконавців, забезпечених необхідними ресурсами, що можуть бути виконані в установлені терміни з необхідним результатом.

З іншого боку, СВО розглядається, як складна багатовимірна ієрархічна система. Тому, модель формування дерева цілей розвитку СВО за складниками спроможностей та рівнями ієрархії (державний, відомчий, інституційний) є таксономічною моделлю, адже описує розміщення цілей розвитку за певними рівнями, принципами та правилами (рис. 2).

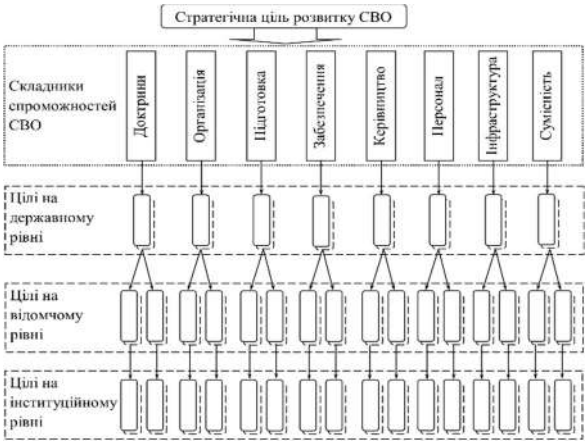


Рисунок 2 – Таксономічна модель «дерева цілей» розвитку системи військової освіти

Варто відзначити, що досконало побудоване «дерево цілей» у подальшому трансформуватиметься у програми та проєкти, визначені цілі мають відповідати вищезазначеним критеріям SMART (specific – конкретна, measurable – вимірна, achievable – досяжна, relevant – значуща, time-bounded – обмежена у часі). Наступним кроком є моделювання стану елементів СВО у процесі впровадження змін для досягнення бажаних ефектів розвитку СВО.

Формування критеріїв визначення рівня відповідності здійснено за параметрами можливості чіткого окреслення його стану і відповіді «так» чи «ні» і відповідності таких критеріїв загальним підходам щодо ознак випадкових подій, прийнятих у теорії ймовірності та рівномірної шкали оцінювання ймовірності настання події (табл. 1).

Таблиця 1

Критерії визначення рівня відповідності складових спроможностей системи військової освіти

Ймовірність події	Стислий опис відповідності вимогам	Характеристика стану елементу спроможності СВО	Рівень відповідності
0,01…0,24	точно «ні»	Стан елементу не відповідає визначеним вимогам, виявлені недоліки (невідповідності) мають фундаментальний характер та не можуть бути усунені протягом одного року	D
0,25…0,49	радше «ні»	Стан елементу не відповідає визначеним вимогам, виявлені недоліки (невідповідності) можуть бути усунені протягом одного року	C
0,50…0,74	радше «так»	Стан елементу відповідає визначеним вимогам, однак виявлені не суттєві недоліки (невідповідності)	B
0,75…1,00	точно «так»	Стан елементу повністю відповідає визначеним вимогам є ознаки (перспективи) розвитку	A

Критерії визначення рівня відповідності складових спроможностей СВО є підґрунтям створення моделі стану елементів спроможності СВО за рівнями відповідності A, B, C, D. Діяльності СВО розглядатимемо, як випадковий процес, у якому складники СВО та її спроможності залежать від випадкових подій, адже кількісно-якісне співвідношення підготовленого персоналу є випадковим явищем, що залежить від багатьох випадкових подій.

Стан відповідності і-го складника спроможностей Q_i в загальному уявленні можна позначити, як відношення його фактичного стану (q_i) до бажаного або нормативного (q_n):

$$Q_i = \frac{q_i}{q_n}, \quad (1)$$

де n – індекс станів елементів i = 1, 2…N.

Вважатимемо, що всі складники спроможностей СВО є рівноважливими, адже через наявність зв'язків та взаємного впливу одного складника на інший встановити їх пріоритетність є достатньо складним завданням зі значною кількістю невідомих та випадкових даних. Тоді, загальну оцінку стану якості елементів спроможностей СВО Q представимо через сукупність паралельних випадкових процесів для яких:

$$Q = 1 - \sum_{i=1}^{I} (1 - Q_i)_I, \quad (2)$$

Стан кожного складника спроможностей є змінюваним у часі. Водночас виміряти цей стан можливо лише за певним результатом реалізації спроможності (завершення навчального року, завершення терміну курсу навчання, отримання відгуків від випускників тощо). Отже час є дискретним. За таких міркувань можна вважати, що у фіксований момент часу (*t*):

$$Q_i = \{p_1(t_1), p_2(t_2), ...p_j(t_j)\}, \quad (3)$$

де $p_j(t)$ – імовірність перебування елементу у стані j, j = 1,2, … J.

За умов встановлення фіксованих критеріїв стану елемента спроможності (A, B, C, D), максимальне значення J = 4. Водночас слід ще встановити інтервал фіксації часу, або той момент часу, коли здійснюватиметься вимірювання стану елементу.

Вважатимемо, що процес розвитку СВО пов'язаний із виконанням певних змін і заходів. Зміни можуть створювати як негативний, так і позитивний ефект. Для моделювання встановлюємо, що результатом зміни є ефект, за якого елемент спроможності перейшов з одного стану у інший. Висновок стосовно доцільності зміни здійснюватиметься на підставі оцінювання до якого рівня (вищого чи нижчого) перейшов елемент спроможностей. Інтервалом фіксації часу коли здійснюватиметься вимірювання стану якості елемента є крок (k) під яким розумітимемо комплекс впроваджених змін, ефектом яких є зміна показника стану Q.

Відомо, що випадковий процес, який відбувається в системі, вважається Марковським, якщо для будь-якого моменту часу t_0, ймовірнісні характеристики процесу в майбутньому, залежать лише від його стану в даний момент t_0 і не залежать від того, коли і як система прийшла до цього стану [19]. Отже, оцінювання стану окремого елементу спроможностей СВО після здійснення кроку k не пов'язане з оцінюванням його попереднього стану, тобто процес зміни стану елементів спроможностей СВО вважатимемо однорідним марковським процесом з дискретним станом та дискретним часом.

За допомогою методу ймовірності станів опишемо однорідний ланцюг Маркова з дискретним станом для станів A, B, C, D і дискретним часом, що змінюється покроково та обчислюється.

Припустимо, у момент часу t (після кроку k) елемент спроможностей перебуватиме в одному зі станів: $Q = \{Q_D, Q_C, Q_B, Q_A\}$, тобто здійсниться одне з повної групи несумісних подій: Q_D (k), Q_C (k), Q_B (k), Q_A (k). У такому випадку показник Q може змінюватись на кожному кроці k:

$$Q_i(k) = \{P_D(k), P_C(k), P_B(k), P_A(k)\}. \quad (4)$$

Позначимо ймовірність того, що елемент спроможності перебуває у станах j…J на моменти завершення кроків k (k = 1, 2, …, K). Ймовірності $P_D(k)$, $P_C(k)$, $P_B(k)$, $P_A(k)$ є ймовірністю стану однорідного марковського ланцюга, в якому перехідні ймовірності не залежать від номеру кроку. З огляду на властивість ймовірності несумісних дій, що утворюють повну групу, для кожного кроку k:

$$P_D(k) + P_C(k) + P_B(k) + P_A(k) = 1. \quad (5)$$

Такий підхід дозволяє моделювати результати впровадження змін у СВО впливом на окремі елементи спроможностей СВО через оцінювання досягнення позитивного (перехід у вищий стан) або негативного (перехід у нижчий стан) ефекту зміни.

Описаний випадковий процес подамо через ланцюг Маркова, як переміщення точки (показник Q_i) по графу станів випадковим чином з переходом з одного стану у інший за кроками t_1, t_2,….t_k.

Варто зазначити, що не кожна зміна (крок) обов'язково призводить до переходу Q_i до іншого стану. В певний проміж часу, він може перебувати у попередньому стані, тому для будь-якого кроку (моменту часу) існуватимуть різні ймовірності переходу показника в інший стан або затримання його у сталому положенні.

Водночас, стан елементу, що повністю відповідає визначеним вимогам (стан «A»), вважатимемо поглинальним станом, через те, що впровадження зміни, яке призвело до переходу елементу спроможності у найвищий стан відповідності свідчитиме, що зміна є прийнятною, а ефект її впровадження є таким, що відповідає меті або визначеному завданню.

Прогнозування на підставі за рівнями відповідності A, B, C, D дозволятиме здійснити оцінювання таких змін, за яких елемент перейде у стан повної відповідності вимогам, тому подальше моделювання буде не потрібним.

Особливістю поглинального стану є те, що зі збільшенням кількості кроків (змін), які відповідають меті ($k \to \infty$) ймовірність того, що елемент досягнене поглинального стану наближатиметься до 1. Для опису такого процесу скористаємося графом станів елементів спроможностей СВО, який є сукупністю вершин, що зображають можливі стани елемента Q_i з імовірністю P_i,. Вектори, що відображають можливі варіанти його переходу з одного стану в інший та імовірності того, що елемент перейде з одного стану в інший – перехідні імовірності π_{jJ} (рис. 3).

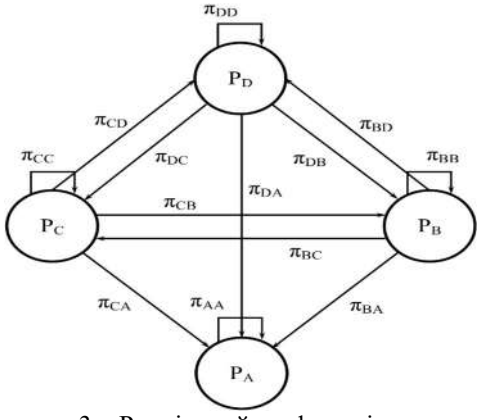


Рисунок 3 – Розмічений граф станів елементів спроможностей СВО

Умови переходу з одного стану в інший ймовірності перебування елементу спроможностей в різних станах залежно від її поточного стану у загальному вигляді можуть бути подані системою диференціальних рівнянь Чепмена-Колмогорова [19]:

$$\begin{aligned}
\frac{dP_D(t)}{dt} &= P_C(t)\pi_{CD} + P_B(t)\pi_{BD} - P_D(t)\pi_{DC} - P_D(t)\pi_{DB} - P_D(t)\pi_{DA} \\
\frac{dP_C(t)}{dt} &= P_D(t)\pi_{DC} + P_B(t)\pi_{BC} - P_C(t)\pi_{CD} - P_C(t)\pi_{CB} - P_C(t)\pi_{CA} \\
\frac{dP_B(t)}{dt} &= P_D(t)\pi_{DB} + P_C(t)\pi_{CB} - P_B(t)\pi_{BD} - P_B(t)\pi_{BC} - P_B(t)\pi_{BA} \\
\frac{dP_A(t)}{dt} &= P_D(t)\pi_{DA} + P_C(t)\pi_{CA} + P_B(t)\pi_{BA}
\end{aligned} \quad (6)$$

З огляду на те, що кожен крок є фіксованим у часі, тобто ми маємо однорідний марковський ланцюг з дискретним часом, диференціальні рівняння записуємо лінійними рівняннями для кожного зі станів:

$$\begin{cases}
P_D\pi_{DC} + P_D\pi_{DB} + P_D\pi_{DA} = P_C\pi_{CD} + P_B\pi_{BD} \\
P_C\pi_{CD} + P_C\pi_{CB} + P_C\pi_{CA} = P_D\pi_{DC} + P_B\pi_{BC} \\
P_B\pi_{BD} + P_B\pi_{BC} + P_B\pi_{BA} = P_D\pi_{DB} + P_C\pi_{CB} \\
P_A = P_D\pi_{DA} + P_C\pi_{CA} + P_B\pi_{BA}
\end{cases} \quad (7)$$

або

$$\begin{cases}
P_D(\pi_{DC} + \pi_{DB} + \pi_{DA}) = P_C\pi_{CD} + P_B\pi_{BD} \\
P_C(\pi_{CD} + \pi_{CB} + \pi_{CA}) = P_D\pi_{DC} + P_B\pi_{BC} \\
P_B(\pi_{BD} + \pi_{BC} + \pi_{BA}) = P_D\pi_{DB} + P_C\pi_{CB} \\
P_A = P_D\pi_{DA} + P_C\pi_{CA} + P_B\pi_{BA}
\end{cases} \quad (8)$$

У системі рівнянь (8), ліворуч розташовані ймовірності перебування у певному стані, які помножені на сумарну перехідну ймовірність з цього стану в інший, праворуч – сума добутків усіх перехідних ймовірностей на ймовірність тих станів з яких здійснюється перехід. Тоді, якщо ліву частину рівняння позначити через вектор переходу з певного стану в інший:

$$\vec{Q} = \left\{\vec{Q}_D; \vec{Q}_C; \vec{Q}_B; \vec{Q}_A\right\}, \quad (9)$$

отримаємо

$$\begin{cases}
\vec{Q}_D = P_C\pi_{CD} + P_B\pi_{BD} + P_A\pi_{AD} \\
\vec{Q}_C = P_D\pi_{DC} + P_B\pi_{BC} + P_A\pi_{AC} \\
\vec{Q}_B = P_D\pi_{DB} + P_C\pi_{CB} + P_A\pi_{AB} \\
\vec{Q}_A = P_D\pi_{DA} + P_C\pi_{CA} + P_B\pi_{BA}
\end{cases} \quad (10)$$

Ймовірність залишення у незмінному положенні π_{jj} доповнюватиме суму перехідних ймовірностей до одиниці. Наприклад, для стану Q_D справедливим буде твердження $\pi_{DD} = 1 - (\pi_{CD} + \pi_{BD} + \pi_{AD})$. З урахуванням цього, перехідні ймовірності з одного стану в інший описуватиме матриця:

$$\pi_{jJ} = \begin{vmatrix}
\pi_{DD} & \pi_{DC} & \pi_{DB} & \pi_{DA} \\
\pi_{CD} & \pi_{CC} & \pi_{CB} & \pi_{CA} \\
\pi_{BD} & \pi_{BC} & \pi_{BB} & \pi_{BA} \\
\pi_{DA} & \pi_{CA} & \pi_{BA} & \pi_{AA}
\end{vmatrix} \quad (11)$$

Зводимо лінійні рівняння (10) у матрицю:

$$\begin{vmatrix}
\vec{Q}_D \\ \vec{Q}_C \\ \vec{Q}_B \\ \vec{Q}_A
\end{vmatrix} = \begin{vmatrix}
P_D \\ P_C \\ P_B \\ P_A
\end{vmatrix} \cdot \begin{vmatrix}
\pi_{DD} & \pi_{DC} & \pi_{DB} & \pi_{DA} \\
\pi_{CD} & \pi_{CC} & \pi_{CB} & \pi_{CA} \\
\pi_{BD} & \pi_{BC} & \pi_{BB} & \pi_{BA} \\
\pi_{DA} & \pi_{CA} & \pi_{BA} & \pi_{AA}
\end{vmatrix} \quad (12)$$

На основі матриці перехідних станів, за умови, що початковий стан показника відомий, можна знайти ймовірності станів $P_D(k)$, $P_C(k)$, $P_B(k)$, $P_A(k)$ після кожного k-го кроку впроваджених змін, які сприяли ефекту переходу елемента спроможності від нижчого стану до вищого. Водночас, можна вважати, що початковим станом є стан Q_D тоді $P_D(0) = 1$. Перехідні ймовірності за кроками можна записати матрицею:

$$\pi_{jJ} = \begin{vmatrix}
\pi_{D(1)} & \pi_{C(1)} & \pi_{B(1)} & \pi_{A(1)} \\
\pi_{D(2)} & \pi_{C(2)} & \pi_{B(2)} & \pi_{A(2)} \\
\dots & \dots & \dots & \dots \\
\pi_{D(K)} & \pi_{C(K)} & \pi_{B(K)} & \pi_{A(K)}
\end{vmatrix} \quad (13)$$

Ймовірність станів після першого кроку визначатиметься за допомогою перехідних ймовірностей першого рядка матриці, для другого і наступних кроків за виразом:

$$\pi_{i(k)} = \sum_{j=1}^{J} P_{i(k-1)}\pi_{ij}. \quad (14)$$

Тоді з урахуванням перехідних ймовірностей вектор переходу елементу спроможності ($\vec{Q}$) на кожному наступному кроці (k+1) можна записати:

$$\vec{Q}_J^{(k+1)} = \vec{Q}_j^k P_j^k \pi_{jJ} = \begin{vmatrix}
P_D \\ P_C \\ P_B \\ P_A
\end{vmatrix} \cdot \begin{vmatrix}
\pi_{DD} & \pi_{DC} & \pi_{DB} & \pi_{DA} \\
\pi_{CD} & \pi_{CC} & \pi_{CB} & \pi_{CA} \\
\pi_{BD} & \pi_{BC} & \pi_{BB} & \pi_{BA} \\
\pi_{DA} & \pi_{CA} & \pi_{BA} & \pi_{AA}
\end{vmatrix} \cdot \begin{vmatrix}
\pi_{D(1)} & \pi_{C(1)} & \pi_{B(1)} & \pi_{A(1)} \\
\pi_{D(2)} & \pi_{C(2)} & \pi_{B(2)} & \pi_{A(2)} \\
\dots & \dots & \dots & \dots \\
\pi_{D(K)} & \pi_{C(K)} & \pi_{B(K)} & \pi_{A(K)}
\end{vmatrix} \quad (15)$$

Перехідні ймовірності стану елементу спроможності можуть бути отримані за даними статистичних досліджень, експертними методами досліджень або їх поєднанням, коли на певному етапі змін ми матимемо статистичні дані, а на подальших етапах узгоджену думку експертів. Отже, на етапі планування зміни, група експертів визначатиме значення перехідної ймовірності, у подальшому здійснюватиметься моделювання та оцінювання доцільності запланованої зміни.

Управління змінами у процесах розвитку СВО здійснюватиметься на підґрунті моделювання процесу формування спроможностей СВО, моделювання цілей розвитку на основі моделі дерева цілей та моделювання стану елементів спроможностей СВО за результатами прогнозованих ефектів, отриманих від запланованих змін. Ланцюг Маркова дозволяє моделювати стан елементу спроможності СВО залежно від впроваджених змін та прогнозованих ефектів від їх впровадження.

Висновки й перспективи подальших досліджень

Таким чином, абстрактна модель системи військової освіти (рис. 1) дає уявлення про зв'язок між її елементами та складниками спроможностей. Таксономічна модель дерева цілей (рис. 2) відображає впорядковану ієрархію та послідовну декомпозицію стратегічної мети розвитку системи військової освіти на часткові цілі на трьох рівнях ієрархії. Модель стану елементів спроможностей ґрунтується на однорідному ланцюзі Маркова з дискретним станом, дискретним часом та поглинальним станом «А», що дозволяє встановити стан елемента спроможності та прогнозувати отримані ефекти внаслідок запроваджених змін у процесах розвитку системи військової освіти.

Модель є підґрунтям для подальшого розроблення інструменту (методу, методики, механізму) оцінювання елементів спроможностей та системи військової освіти у цілому.

Список бібліографічних посилань

1. Про рішення Ради національної безпеки і оборони України від 25.03.2021 "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.2021 № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n2 (дата звернення: 05.06.2023). **2. Про рішення Ради** національної безпеки і оборони України від 20.08.2021 "Про Стратегічний оборонний бюлетень України": Указ Президента України від 17.09.2021 № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/473/2021#n2 (дата звернення: 05.06.2023). **3. Про трансформацію** системи військової освіти: Постанова Кабінету Міністрів України від 15.12.1997 № 1410. URL: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text (дата звернення: 05.06.2023). **4. Сальнікова О. Ф., Артамощенко В. С.** Теоретичні аспекти державного управління системою військової освіти. *Інвестиції: практика та досвід*. 2021. № 12. С. 67–71. URL: https://doi.org/10.32702/2306-6814.2021.12.67.

5. Зельницький А. М., Заболотний О. А., Васильєв О. М., Шабатіна Н. О. Теоретико-методологічні засади управління змінами в системі військової освіти: монографія. Київ : НУОУ, 2022. 312 с. **6. Математичні** основи кадрового менеджменту у військовій сфері: монографія. / Ю. А. Гусак, А. М. Сиротенко, П. І. Шуляк, О. В. Бобрун , В. М. Пасічник під заг. ред. д. військ. н. І. С. Романченка. Київ: ЦНДІ ЗС України, 2019. 250 с. **7. Професійна** військова освіта в Україні у сучасному безпековому середовищі: монографія. / І. Руснак, В. Мірненко, В. Оліферук та ін.; за заг. ред. д. філос. наук Д. Вітера та д. військ. н. В. Телелима. Київ: НУОУ, 2021. 277 с. **8. Нещадим М.І.** Військова освіта України: історія, теорія, методологія, практика: монографія. Київ: Видавничо-поліграфічний центр "Київський університет", 2003. 852 с. **9. Полторак С. Т.** Уніфікація механізмів державного управління реформуванням Збройних сил України в умовах трансформаційного суспільства: дис. доктора наук з державного управління: 25.00.02. Харків : НУ ЦЗУ, 2018. 450 с. **10. Устименко О. В.** Механізми державного управління системою військової освіти України: автореф. дис. кандидата наук з державного управління: 25.00.02. Київ : НА ДУ при ПУ, 2012. 23 с. **11. Оліферук В., Вітер Д. Шабатіна Н.** Моделювання процесу розвитку військової освіти в Україні: принципи та підходи до стандартизації. *Військова освіта: Збірник наукових праць НУОУ*. 2020. № 2 (42). С. 215–221. URL: https://doi.org/10.33099/2617-1783/2020-2/215-221. **12. Мітягін О., Вітер Д., Карпенко В.** Формування моделі професійної військової освіти в Україні з урахуванням процедур оперативного планування НАТО. *Військова освіта: Збірник наукових праць НУОУ*. 2021. № 1 (43). С. 64–78. URL: https://doi.org/10.33099/2617-1783/2021-43/64-78.

13. Олех Т. М., Гогунський В. Д., Барчанова Ю. С., Дмитренко К. М. Дослідження поглинаючих станів системи за допомогою марківських ланцюгів та фундаментальної матриці. *Вісник НТУ «ХПІ»*. 2016. № 2 (1174). С. 17–21. URL: https://doi.org/10.20998/2413-3000.2016.1174.4. **14. Колесніков О. Є.** Управління проектами у сфері освіти з використанням марковської моделі оцінки діяльності. *Управління розвитком складних систем*. 2017. № 29. С. 160–167. URL: http://urss.knuba.edu.ua/files/zbirnyk-29/23.pdf (дата звернення: 05.06.2023). **15. Оборонна** реформа: системний підхід до оборонного менеджменту: монографія. / А. Павліковський, В. Фролов, Ф. Саганюк та ін.; за заг. ред. д. військ. н. А. Сиротенка. Київ: НУОУ, 2020. 274 с. URL: https://nuou.org.ua/assets/documents/mono-obo-ref-2020.pdf (дата звернення: 05.06.2023). **16. Шершньова З. Є.** Стратегічне управління: підручник. Київ: КНЕУ, 2004. 699 с. **17. Bertalanffy L. von, Braziller G.** General systems theory. Foundations, Development, Applications. Inc. New York. 1969. 289 p. URL: https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf (дата звернення: 05.06.2023). **18. Коваль М. В., Пунда Ю. В., Артамощенко В. С.** Методологічні аспекти формування стратегії розвитку вищого військового навчального закладу. *Наука і оборона*. 2022. № 3/4. С. 37–46. URL: https://doi.org/10.33099/2618-1614-2022-20-3-4-37-46. **19. Імовірність,** процеси, статистика: навчальний посібник / О. І. Клесов, Є. О. Лєбєдєв, М. І. Портенко. Київ: Видавничо-поліграфічний центр «Київський університет», 2008. 494 с.

THE MODEL OF MILITARY EDUCATION SYSTEM BASED ON MARKIV CHAIN

***Artamoshchenko Vadym** (Candidate of Military Sciences, Associate Professor)*

National Defence University of Ukraine, Kyiv, Ukraine

Training military personnel of the defense forces using lessons learned during the repulsion of armed aggression by the russian federation, as well as incorporating NATO methodologies, training methods, principles, and standards, is one of the objectives of military education development. The development of the military education system entails systemic changes and change management. Forecasting the possible effects resulting from the implementation of these changes requires the construction of a military education system model. The purpose of the article is to develop a model of the military education system for predicting the effects obtained through the implementation of changes in its developmental processes. The article employs a method for assessing the joint capabilities of the military education system. The process of forming the capabilities of the military education system represented by abstract model that reflects the totality of system elements and components of its capabilities. The components of the military education system divided into three levels of hierarchy: state, departmental and institutional. The author proposes to implement the strategic goal and individual goals of the development of the military education system according to the «goal tree» taxonomic model. The author, based on the approaches adopted in probability theory and the uniform scale of probability assessment for the occurrence of a random event, proposes the «ABCD model» to describe the criteria for determining the level of conformity of the components' military education system capabilities. A discrete-time, discrete-state Markov chain has been developed to assess the state of system capability elements. The matrix of the transition vector for each step of change is described, considering the probabilities of transitioning the capability elements from one state to another due to the implementation of a specific change. This model enables the prediction of the effects obtained from implemented changes and the state of the capability elements in the developmental processes of the military education system.

***Key words**: model, capabilities, system of military education, Markov chain.*

References

1. On the decision of the National Security and Defense Council of Ukraine of 03/25/2021 «On the Military Security Strategy of Ukraine» [online], (2021). Decree of the President of Ukraine № 121/2021, 25 March. Available at: https://zakon.rada.gov.ua/laws/show/121/2021#n2 [Accessed 05 June 2023]. **2. On the decision** of the National Security and Defense Council of Ukraine of 20.08.2021 «On the Strategic Defense Bulletin of Ukraine» [online], (2021). Decree of the President of Ukraine № 473/2021, 17 September. Available at: https://zakon.rada.gov.ua/laws/show/473/2021#n2 [Accessed : 05 June 2023]. **3. On the transformation** of the military education system [online], (1997). Resolution of the Cabinet of Ministers of Ukraine № 1410. 15 December. Available at: https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text [Accessed : 05 June 2023]. **4. Salnikova, O., Artamoshchenko, V.,** (2021). Theoretical aspects of public administration of the military education system. *Investments: practice and experience.* 12, 67-71. DOI: https://doi.org/10.32702/2306-6814.2021.12.67.

5. Zelnytskyi, A., Zabolotnyi, O., Vasyliev, O., Shabatina, N., (2022). *Theoretical and methodological principles of change management in the system of military education*: a monograph. Kyiv: NUOU. **6. Husak, Y., Syrotenko, A., Shulyak, P., Bobrun, O., Pasichnyk, V.,** (2019). *Mathematical foundations of personnel management in the military sphere*: monograph / edited by Doctor of Military Sciences I. Romanchenko. Kyiv: Central Research Institute of the Armed Forces of Ukraine. **7. Rusnak, I., Mirnenko, V., Oliferuk, V. and others,** (2021). *Professional military education in Ukraine in the modern security environment*: a monograph / edited by Doctor of Philosophy D. Viter and Doctor of Military Sciences V. Telelym. Kyiv: NUOU. **8. Neshchadym, M. I.,** (2003). *Military Education of Ukraine: History, Theory, Methodology, Practice*: a monograph. Kyiv: Kyiv University Publishing and Printing Center. **9. Poltorak, S. T.,** (2018). *Unification of mechanisms of public administration of the reform of the Armed Forces of Ukraine in the conditions of a transformational society.* Doctor of Science in Public Administration. 25.00.02. Kharkiv, National University of Civil Protection of Ukraine. **10. Ustymenko, O. V.,** (2012). *Mechanisms of public administration of the system of military education of Ukraine*. Avtoref. Dys…PhD in Public Administration. 25.00.02. Kyiv, National Academy for Public Administration under the President of Ukraine. **11. Oliferuk, V., Viter, D., Shabatina, N.,** (2020). Modeling the process of development of military education in Ukraine: principles and approaches to standardization. *Military education: Collection of scientific works of the NOU*. 2 (42), 215-221. DOI: https://doi.org/10.33099/2617-1783/2020-2/215-221. **12. Mitiahin, O., Viter, D., Karpenko, V.,** (2021). Formation of a model of professional military education in Ukraine taking into account NATO operational planning procedures. *Military Education: Collection of scientific papers of NGOs*. 1 (43), 64-78. DOI: https://doi.org/10.33099/2617-1783/2021-43/64-78.

13. Olekh, T. M., Gogunsky, V. D., Barchanova, Y. S., Dmitrenko, K. M., (2016). Investigation of absorbing states of the system by means of Markov chains and fundamental matrix. *Bulletin of NTU «KhPI».* 2 (1174), 17-21. DOI: https://doi.org/10.20998/2413-3000.2016.1174.4.

14. Kolesnikov, O. E., (2017). *Project management in the field of education using the Markov model of activity evaluation.* Management of the development of complex systems. 29, 160-167 [online]. Available at: http://urss.knuba.edu.ua/files/zbirnyk-29/23.pdf [Accessed : 05 June 2023]. **15. Syrotenko, A., Pavlikovskyi, A., Frolov, V. & oth's,** (2020). *Defense reform: a systematic approach to defense management*: a monograph. Kyiv : NUOU [online]. Available at: https://nuou.org.ua/assets/documents/mono-obo-ref-2020.pdf [Accessed : 05 June 2023]. **16. Shershnova, Z. Ie.,** (2004). *Strategic management*: a textbook. Kyiv: KNEU. **17. Bertalanffy, L. von, Braziller, G.,** (1969). *General systems theory. Foundations, Development, Applications*. Inc. New York [online]. Available at: https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_ Theory_1968.pdf [Accessed : 05 June 2023]. **18. Koval, M. V., Punda, Y. V., Artamoshchenko, V. S.,** (2022). Methodological aspects of forming a development strategy for a higher military educational institution. *Science and Defense*. 3/4, 37-46. DOI: https://doi.org/10.33099/2618-1614-2022-20-3-4-37-46. **19. Klesov, O. I., Liebiediev, Ye. O., Portenko, M. I.,** (2008). Probability, processes, statistics: a textbook. Kyiv: Kyiv University Publishing and Printing Center.

DOI:**10.33099/2311-7249/2023-47-2-133-138**

УДК 355.3: 355.4

Шевчук Віталій Вікторович *(кандидат військових наук)*
Кривошеєв Віталій Валерійович *(кандидат військових наук, доцент)*
Швець Микола Миколайович

Національний університет оборони України, Київ, Україна

ВИМОГИ ДО СИСТЕМИ БОРОТЬБИ З БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

У статті окреслено низку питань, що актуалізують наявні проблеми у вимогах до системи боротьби з безпілотними літальними апаратами противника. Метою статті є узагальнення вимог до системи боротьби з безпілотними літальними апаратами на основі досвіду боротьби з такими апаратами противника під час відбиття збройної агресії російської федерації проти України та розкриття способів боротьби з ними. Під час написання статті застосовано метод аналізу досвіду боротьби з безпілотними літальними апаратами противника, отриманого під час відбиття збройної агресії російської федерації проти України у 2014–2023 роках, а саме аналіз функціонування елементів системи боротьби з безпілотними літальними апаратами. Це дає змогу визначити вимоги до системи боротьби з безпілотними літальними апаратами в цілому та до її складових, зокрема. Конкретизація таких вимог відповідає головному завданню – зниженню ефективності застосування противником безпілотних літальних апаратів по критичній інфраструктурі держави, військових об'єктах, а також цивільному населенню. Такий підхід дає змогу у подальшому виробити єдині погляди на тактику дій підрозділів Збройних сил України стосовно боротьби з безпілотними літальними апаратами та удосконалювати технічну складову системи боротьби з такими апаратами противника.

Ключові слова*: безпілотні літальні апарати, система боротьби, управління.*

Вступ

Під час збройної агресії російської федерації проти України ворог активно застосовував безпілотні літальні апарати (далі – БпЛА) різних класів. Тому постало питання протидії таким засобам, що в свою чергу підкреслює потребу постійного розроблення та удосконалення методів та способів боротьби з ними. Це зумовлює актуальність цієї статті.

Постановка проблеми. Досвід проведення операції Об'єднаних сил свідчить, що керівництво Збройних сил України (далі – ЗС України) здійснює пошук нових напрямів боротьби з БпЛА та проводить роботи з удосконалення існуючих способів протидії таким літальним апаратам [1]. Крім того, через застосування противником різних засобів повітряного нападу тенденція щодо підвищення ефективності застосування засобів ураження повітряних об'єктів збільшується. Слід зазначити, що для боротьби з БпЛА використовуються засоби ураження усіх складових сил оборони держави. Тому пошук шляхів щодо захисту військових та цивільних об'єктів від ударів БпЛА є актуальною проблемою в сучасних умовах бойового використання ЗС України.

Аналіз останніх досліджень і публікацій [2; 4; 5; 6], в яких окреслено низку питань щодо застосування та боротьби з БпЛА противника, а саме:

проведено порівняльний аналіз сучасних засобів протидії БпЛА та зроблені висновки щодо можливості їх застосування у ЗС України [2];

розкриті деякі питання протидії БпЛА щодо захисту, знищення та захоплення [5];

визначені перспективи подальшого розвитку застосування БпЛА при веденні операцій, як одних з елементів повітряної компоненти систем розвідки, зв'язку, навігації та ударних систем [4; 6].

Всі ці дослідження свідчать про те, що в сучасних збройних конфліктах активно застосовуються БпЛА. Водночас, крім виконання розвідувальних завдань БпЛА мають тенденцію до перетворення в основний засіб для нанесення ураження об'єктам критичної інфраструктури держави та військовим об'єктам на великих відстанях. Науковий підхід до обґрунтування шляхів боротьби з БПЛА противника дасть змогу не тільки удосконалювати шляхи підвищення ефективності застосування «протидронових» засобів, а й здійснювати пошук нових способів боротьби з БпЛА противника.

Метою статті є узагальнення вимог до системи боротьби з безпілотними літальними апаратами на основі досвіду боротьби з БпЛА противника під час відбиття збройної агресії російської федерації проти України та розкриття способів боротьби з ними.

Виклад основного матеріалу дослідження

За результатами вивчення досвіду застосування противником БпЛА визначено, що найбільш частіше використовувались такі БпЛА, як

«Форпост», «Орлан», «Герань-2». Шляхом поступового накопичення досвіду боротьби із зазначеними БпЛА було визначено їх тактико-технічні характеристики, способи їх застосування, а відтак і способи боротьби з ними невогневими засобами.

Багатофункціональний безпілотний комплекс (далі – БпК) *«Форпост»*, вироблений ВАТ «Уральський завод цивільної авіації» (м. Єкатеринбург), призначений для пошуку, виявлення та ідентифікації наземних об'єктів.

БпК «Форпост»:

здійснює дистанційно керований з землі політ в автономному режимі або за попередньо заданою програмою, а також здійснює навігацію за підтримки наземної станції управління і диференційної системи глобального позиціювання;

виконує передачу даних про параметри польоту і стан корисного навантаження на наземну станцію управління;

підтримує постійний зв'язок з наземною станцією управління по дубльованим каналам в дуплексному режимі передачі інформації

дає змогу встановлювати модульне оптико-електронне навантаження..

Багатофункціональні безпілотні авіаційні комплекси серії «Орлан» («Орлан-1», «Орлан-3», «Орлан-10», «Орлан-30») (далі – БпАК) розроблені ВАТ «Спеціальний технологічний центр» (м. Санкт-Петербург). Саме БпАК цього виробника обрано керівництвом збройних сил для озброєння підрозділів сухопутних військ. Підприємство розробило серію БпАК у чотирьох основних класах, кожен з яких призначений для оснащення військ у відповідній ланці системи управління військами. Основними зразками БпАК серії «Орлан» є:

«Орлан-1» (мікро, відділення – взвод – рота);

«Орлан-3М» (міні, рота – батальйон);

«Орлан-10» (тактичний, батальйон – полк/ бригада);

«Орлан-30» (оперативно-тактичний, полк/ бригада – дивізія).

Безпілотний авіаційний комплекс «Орлан-3М» призначений для виконання панорамної і планової фото- та відео зйомки місцевості.

Безпілотний авіаційний комплекс «Орлан-10» призначений для контролю об'єктів у важкодоступній місцевості, може використовуватися для пошуково-рятувальних робіт.

На БпЛА «Орлан-10» може бути встановлені декілька типів корисного навантаження (фото- і відеокамера, тепловізор та ретранслятор каналу управління тощо).

Варіанти змінного корисного навантаження БпАК «Орлан-10»:

фотокамери планові:

Canon EOS 650D; Canon EOS 500D; Canon EOS 50D; Canon EOS 5D;

відеокамери:

планові (Flir Photon 320, Flir Photon 640, BHV-558 EX);

курсові (Flir Photon 320, Flir Photon 640, BHV-558 EX);

поворотні (Flir Photon 320, Flir Photon 640);

гіростабілізованого типу (Controp D-STAMP, U-STAMP);

тепловізори: Flir Quark; Flir Tau 2; Flir Photon 320; Flir Photon 640.

На БпАК встановлений модуль системи навігації та позиціонування з приймачами Ublox LEA-6H та МНП-М7. Модуль приймає сигнали глобальних супутникових систем навігації і позиціювання NAVSTAR GPS та GLONASS.

Безпілотний літальний апарат «Орлан-30» є удосконаленою версією БпЛА «Орлан-10». Система автоматичного керування забезпечує упевнене пілотування та реєстрацію польотної інформації в реальному масштабі часу на пункті керування.

На БпЛА встановлюється фотокамера, відеокамера, тепловізор і гіростабілізована телевізійна камера.

З одного наземного пункту керування забезпечується одночасне керування до чотирьох БпЛА. Будь-який БпЛА може бути ретранслятором для інших.

Основні тактико-технічні характеристики (далі – ТТХ) БпЛА наведено у табл. 1.

Таблиця 1

Характеристики безпілотних літальних апаратів [3; 7]

Назва характеристики	Форпост	Орлан-3М	Орлан-10	Орлан-30
Тип двигуна	Поршневий, чотирьохтактний Jabiru 2200	Поршневий, двотактний 3w-55i (метанол)	Поршневий, чотирьохтактний Saito FG-40 40 (АІ-95)	Внутрішнього згоряння (метанол)
Маса, кг	325	7	14/18	30 – 35
Маса корисного навантаження, кг	100	до 1,8	до 5	до 8
Довжина, м	5,85	1,2	1.8	1,8
Розмах крила, м	8,55	2	3,1	3,1
Робоча швидкість польоту, км/год	126 – 148	70 – 150	75 – 170	90 – 150
Макс. тривалість польоту, год	17,5	2	16 год	18
Гранична висота, м	5797	7000	5000 – 6000	5000
Максимальна дальність дії, км.	250	100	600	>120
Частоти управління БпАК	1000-1800 МГц	863-870 МГц	902-922 МГц	865-922 МГц
Частоти передачі інформації з цільового навантаження та телеметрії	1070-1370 МГц	960-1215 МГц	2300-2700 МГц	3300-3800 МГц

Аналіз наведених у таблиці 1 ТТХ дає змогу запропонувати узагальнені вимоги до системи боротьби з БпЛА.

В*имоги до системи боротьби з БпЛА невогневими засобами.* Система боротьби з БПЛА противника невогневими засобами призначена для прикриття бойових порядків військ в бою та на марші від пілотованих та безпілотних повітряних цілей, з ефективною поверхнею розсіяння (далі – ЕПР) більше 0,01 м^2, що діють на швидкостях до 200 м/с, на висотах 10...6000 м і відстанях 500...7000 м в умовах застосування пасивних та активних перешкод середньої інтенсивності, вдень і вночі у будь яких метеорологічних умовах у всіх кліматичних зонах території країни.

Основою невогневого ураження системи є комплекси радіоелектронної боротьби (далі – РЕБ), призначенням якого є порушення управління БпЛА з наземних та повітряних пунктів управління, зниження ефективності його бойового застосування, обмеження можливостей добування інформації за допомогою радіоелектронних засобів (далі – РЕЗ), які розміщенні на БпЛА.

До складу системи боротьби з БпЛА за невогневого ураження мають входити підсистеми:

1. Виявлення у складі засобів:

оптичного виявлення БпЛА;

акустичного виявлення БпЛА;

виявлення власного радіовипромінювання БПЛА;

радіолокаційного виявлення БпЛА.

2. Невогневого ураження БпЛА.

3. Управління.

Засоби оптичного виявлення БпЛА призначені для розвідки повітряного простору та виявлення БпЛА із використанням тепловізійного та оптичного каналу. Дальність виявлення та визначення дальності до цілі може становити до 25 км.

До складу засобів оптичного виявлення БпЛА зазвичай входять:

засоби виявлення БпЛА в оптичному діапазоні;

засоби виявлення інфрачервоного (теплового) випромінювання БпЛА;

лазерний далекомір;

засоби оптичного підсвічення цілі.

Засоби оптичного виявлення БпЛА мають містити систему стабілізації у просторі з поворотно-нахильним механізмом.

Засоби акустичного виявлення БпЛА призначені для розвідки повітряного простору та виявлення БпЛА. Дальність виявлення шуму двигуна має становити до 15 км. Засоби акустичного виявлення БпЛА мають містити систему стабілізації у просторі з можливістю визначення напрямку на джерело шуму.

Засоби виявлення власного радіовипромінювання БпЛА призначені для проведення радіомоніторингу у польових умовах, виявлення та пеленгації мініатюрних радіопередавачів у діапазоні частот від 20 МГц до 6 ГГц. Ці засоби мають бути оснащені системою стабілізації у просторі з можливістю пеленгу в вертикальній та горизонтальній площині.

Засоби радіолокаційного виявлення БпЛА призначені для здобування первинної радіоелектронної інформації (далі – РЛІ) про повітряну обстановку, її обробку та видачу в систему управління системи боротьби з БпЛА, на командні пункти та взаємодіючі пункти управління (далі – ПУ).

До засобів радіолокаційного виявлення БпЛА відносяться:

первинні засоби радіолокаційної інформації (далі – ЗРЛІ);

вторинні ЗРЛІ тактичного рівня.

Первинними ЗРЛІ є радіолокаційні засоби виявлення повітряних цілей та пересувні радіовисотоміри (далі – ПРВ).

До вторинних ЗРЛІ тактичного рівня відносяться:

засоби мультирадарної обробки РЛІ, що надходить від інших первинних ЗРЛІ;

командні пункти (далі – КП) окремих радіолокаційних рот і радіотехнічних батальйонів.

Первинні та вторинні ЗРЛІ мають бути автоматизованими. Всі первинні ЗРЛІ мають забезпечувати автоматичне знімання і видачу інформації про повітряну обстановку з можливістю коригування оператором інформації про траєкторії руху цілей.

Підсистема управління боротьбою з БпЛА противника має складатися з таких елементів:

пункт управління;

засоби управління.

Зазначена підсистема управління системи боротьбою з БпЛА має забезпечувати автоматизований обмін інформації з автоматизованої системою управління (далі – АСУ) Повітряних Сил ЗС України тактичного рівня – ланка управління з'єднань, частин, підрозділів родів військ та прирівняних до них.

Засоби первинної радіолокації мають видавати:

трасову інформацію по виявлених повітряних об'єктах (далі – ПО);

навігаційну інформацію – координати точки місцеперебування ПО на момент їхньої локації;

Трасова інформація по виявлених ПО має містити:

номер ПО (машинний);

згладжені значення координат ПО у сферичній, полярній або прямокутній системі координат з екстраполяцією на момент видачі;

поточний час доби;

згладжені значення кутових координат постановника активних завад (далі – ПАЗ) з екстраполяцією на момент видачі (пеленги на ПАЗ) – за наявності вбудованих пеленгаційних каналів;

Координатна інформація по виявлених ПО повинна містити:

виміряні в момент локації значення координат ПО у прямокутній системі координат;

час локації ПО;

виміряні в момент локації значення кутових координат ПАЗ (пеленги на ПАЗ) за наявності вбудованих пеленгаційних каналів;

інформація впізнавання ПО;

польотна інформація, яка отримана за допомогою спряжених або збудованих засобів вторинної радіолокації.

Має бути передбаченою можливість одержання інформації, формування та передачі на пункти управління ознак державного впізнавання. Вторинні ЗРЛІ тактичного рівня мають видавати таку інформацію:

траси цілей, що супроводжуються (площинні координати цілі Х, У);

номер ПО машинний або в єдиній системі нумерації;

обчислені параметри руху кожної з цілей;

висота локаційна або барометрична;

інформація державного впізнавання;

кількісний склад групової цілі;

ознака постановки перешкод та вид перешкод.

Підсистема невогневого ураження БпЛА заснована на засобах РЕБ та їх застосуванні. Об'єктами впливу РЕБ є безпілотні літальні апарати, наземні та повітряні пункти управління ними.

Цілями радіоелектронного придушення (далі – РЕП) мають бути:

мережі управління та передачі даних БпЛА;

засоби радіонавігації;

засоби радіо-, радіотехнічної та оптико-електронної розвідки;

радіолокаційні системи БпЛА;

короткохвильовий (далі – КХ), ультракороткохвильовий (далі – УКХ) радіозв'язок та супутникові лінії радіозв'язку наземних та повітряних ПУ БпЛА.

До складу системи невогневого ураження БпЛА мають входити:

пункт управління засобами постановки завад;

засоби постановки завад мережам радіозв'язку та передачі даних БпЛА;

засоби постановки завад сигналам радіонавігації;

засоби постановки завад бортовим радіолокаційним станціям БпЛА;

засоби постановки завад радіозв'язку та супутниковим лініям радіозв'язку.

Пункт управління (далі – ПУ) засобами постановки завад системи невогневого ураження мають забезпечувати:

централізоване управління засобами постановки завад;

контроль радіоелектронної обстановки;

обмін інформацією з вищим органом військового управління;

накопичування та обробку інформації, що надходить від засобів радіотехнічної та радіолокаційної розвідки;

автоматизований та ручний розподіл цілей РЕП між засобами постановки завад, формування для них команд (завдання частот, видів випромінювання, часових параметрів випромінювання, частотних піддіапазонів роботи), призначення пріоритетів об'єктів придушення;

визначення заборонених частот;

протоколювання результатів роботи засобів постановки завад.

Засоби постановки завад мережам радіозв'язку та передачі даних БпЛА призначені для РЕП ліній радіозв'язку та передачі даних, що працюють на фіксованих радіочастотах із традиційними сигналами, сигналами з псевдовипадковою перебудовою робочої частоти та шумоподібними сигналами.

Засоби постановки завад сигналам радіонавігації призначені для РЕП навігаційного обладнання БпЛА, які використовують сигнали супутникових навігаційних систем з метою зриву визначення місцеположення БпЛА.

Засоби постановки завад бортовим радіолокаційним станціям (далі – БРЛС) призначені для прикриття військ (сил) та об'єктів шляхом РЕП, що встановлені на БПЛА.

Засоби постановки завад радіозв'язку та супутниковим лініям радіозв'язку наземних та повітряних ПУ БпЛА призначені для РЕП мереж управління базових станцій та ускладнення отримання розвідувальної інформації ними з БпЛА.

До складу системи невогневого ураження БпЛА може входити рухомий засіб електромагнітної зброї оснащений надпотужним генератором надвисокочастотного діапазону для ураження радіоелектронної апаратури БпЛА.

Вимоги до підсистеми невогневого ураження БпЛА. Під час прикриття точкових і лінійних об'єктів від ударних БпЛА засоби РЕБ, що складають підсистему невогневого ураження, на нашу думку, мають забезпечувати імовірність збереження об'єктів не нижче 0,5 за умови нанесення удару противником за допомогою БпЛА з імовірністю знищення об'єктив не менше 0,8 з метою повного припинення їх функціонування на певний час.

На нашу думку, при прикритті групових (площинних) об'єктів від ударних БпЛА засоби РЕБ мають забезпечувати імовірність збереження об'єктів не нижче 0,6 за умови нанесення удару противником за допомогою БпЛА з імовірністю знищення об'єктів не менше 0.8, з метою дезорганізації функціонування об'єкту на короткий час (уражених елементів зі складу групового об'єкту менше 20%).

На нашу думку, при прикритті угруповань військ (сил) від ударних БпЛА засоби РЕБ мають забезпечувати імовірність збереження військ (сил) не нижче 0,6 за умови нанесення удару противником за допомогою БпЛА. Для вирішення всього кола визначених бойових завдань засоби РЕБ мають задовольняти таким вимогам:

Для *засобів постановки перешкод бортовим РЛС*:

1. Створювати прицільні за частотою і напрямку, загороджувальні за частотою квазібезперервні, імпульсні або прямошумові завади у відповідь.

2. Робочий діапазон частот – 8... 11 ГГц та 11... 18 ГГц.

3. Межі роботи за азимутом – 360°.

4. Межі роботи за кутом місця – від –10 до +50 .

5. Час безперервної роботи – не менше 24 год.

6. Час роботи на випромінювання – не менше 6 год.

Для засобів постановки завад авіаційним лініям УКХ радіозв'язку та передачі даних:

1. Виявлення радіоліній з псевдовипадковою перебудовою робочої частоти (далі – ППРЧ), шумоподібних сигналів (далі – ШПС) у діапазонах частот 100...450 МГц, 960...1216 МГц.

2. Автоматичне визначення параметрів радіосигналів, класифікацію радіовипромінювань та селекцію джерел радіовипромінювань каналів радіоуправління БПЛА та передачі даних.

3. Автоматична пеленгація джерел радіовипромінювань у діапазонах частот 100...450 МГц, 960...1216 МГц.

4. Створення прицільної за частотою перешкоди в діапазоні частот 100...450 МГц (для РЕП мереж з «повільною» ППРЧ).

5. Створення загороджувальної перешкоди в діапазонах частот 100...450 МГц, 960... 1216 МГц (для подавлення мереж із «швидкою» ППРЧ і ШПС).

Для *підсистеми управління* слід віднести вимоги до:

якості (повноти, точності, достовірності) виконання завдань за призначенням;

бойової готовності;

безперервності управління;

стійкості системи управління;

оперативності управління;

прихованості управління.

Далі охарактеризуємо наведені вимоги до підсистеми управління. Головною вимогою до бойової готовності підсистеми управління є випереджаюча готовність підсистеми відносно рівня бойової готовності підрозділів ураження. Іншими основними вимогами до безперервності управління є забезпечення управління за різних умов обстановки, в тому числі при веденні бойових дій. На нашу думку, час безперервної роботи має бути не менше 72 години. Водночас, коефіцієнт бойової готовності основних систем підсистеми управління має становити не нижче 0,98.

Вимоги до стійкості підсистеми управління та її елементів передбачають реалізацію властивостей системи зберігати або швидко відновлювати свою боєздатність з виконанням завдань управління за різних умов обстановки мирного та воєнного часу.

Основними вимогами до оперативності управління (оперативності функціонування системи управління) є забезпечення своєчасного (тобто в задані або існуючі терміни) виконання завдання управління з належною якістю.

Основними вимогами щодо прихованості управління є забезпечення збереження в таємниці від противника положення, стану та функціонування всіх елементів системи управління, зміст завдань управління та заходів, які проводяться з метою їх виконання.

Сьогодні в розвитку літальних апаратів, що використовуються для ведення повітряної розвідки та виконання бойових завдань, спостерігається низка тенденцій, а саме зменшення розмірів планера, використання композитних матеріалів та технологій «Стелс», перехід до безпілотного управління. Це приводить до зменшення ЕПР повітряних об’єктів що викликає зменшення дальності виявлення РЛС, та зменшує ефективність ведення радіолокаційної розвідки.

За результатами аналізу доведено, що суттєве зменшення ЕПР та зони виявлення РЛС спостерігається в сантиметровому діапазоні. Найбільш вигідний для виявлення малорозмірних повітряних об’єктів є метровий діапазон. Це зумовлено резонансним характером відбиття радіохвиль від малорозмірних об’єктів та малою ефективністю використання технологій «Стелс» в метровому діапазоні.

Традиційними (відомими) організаційними та технічними шляхами підвищення ефективності ведення радіолокаційної розвідки малорозмірних цілей є:

покращення характеристик виявлення в ТТХ РЛС;

ущільнення розташування РЛС на небезпечних напрямках (створення смуг виявлення маловисотних та малорозмірних цілей);

одночасне використання РЛС різних діапазонів частот тощо.

З іншого погляду, підходи до створення чергового РЛП вимагають зменшення кількості залучених РЛС та вартості утримання радіолокаційного поля. Виникає суперечність між традиційними заходами підвищення ефективності виявлення малорозмірних цілей та сучасними вимогами до побудови чергового РЛП. Вирішення цієї суперечності потребує пошуку нових методів підвищення ефективності виявлення малорозмірних цілей. Альтернативними (перспективними) шляхами підвищення ефективності виявлення малорозмірних цілей є:

використання енергій сторонніх джерел випромінювання та реалізації режимів рознесеного прийому;

використання властивості резонансного відбиття електромагнітних хвиль від повітряного об’єкта з довжиною хвилі, що співставна з лінійними розмірами цього об’єкта;

використання властивостей бістатичної ЕПР за рознесеного прийому.

Висновки й перспективи подальших досліджень

В роботі проведено формулювання та узагальнення вимог до системи боротьби з БпЛА на основі досвіду боротьби з БпЛА противника під час відбиття збройної агресії російської федерації проти України та розкриті деякі способи боротьби з ними.

Наведений у статті підхід дозволив визначити вимоги до системи боротьби з БпЛА невогневими засобами та структурувати їх за складовими

виявлення (оптичного, акустичного, власного радіовипромінювання, радіолокаційного), ураження, управління.

Визначені та структуровані вимоги до системи боротьби з БпЛА дозволили окреслити вимоги до засобів виявлення, ураження, управління, які, на відміну від існуючих, враховують як технічні характеристики засобів виявлення, ураження, управління, так й технічні характеристики об'єктів, що уражаються.

Наведені у статті дослідження є перспективними і потребують детального вивчення та розвитку, особливо під час формування системи прикриття військ (сил), об'єктів ЗС України і об'єктів критичної інфраструктури держави. Все це визначає завдання для військових науковців, яке полягає у аналізі способів як застосування БпЛА противником, так і боротьби з ними. Водночас, формування системи прикриття від БпЛА противника справа, по суті, не нова, а має лише певні особливості. Тому це потребує формування нормативних та керівних актів (документів), обґрунтування та визначення ефективних способів протидії із БпЛА. Такі підходи повинні включати аналіз інформації, отриманої від системи розвідки, вибір способів та засобів протидії, визначення тактики застосування систем зенітного ракетно-артилерійського прикриття, розподіл сил і постановку бойових завдань на знищення БпЛА противника.

Список бібліографічних посилань

1. Щипанський П. В., Сегеда С. П. Уроки антитерористичної операції. 2016 рік: монографія Київ: НУОУ, 2020. 242 с. **2. Корольов Р.В., Королюк Н. О., Петров О. В., Сюле К. В.** Аналіз сучасних засобів знищення безпілотних літальних апаратів. *Збірник наукових праць ХНУПС,* 2017. № 4(53). С. 23–30. **3. ВП7-00(03).01.** Методичні рекомендації «Боротьба з безпілотними літальними апаратами» (за досвідом проведення ООС (раніше АТО). Київ; ГШ ЗСУ, 2019. 124 с. **4. Жарик О. М.** Досвід створення і застосування ударних БПЛА багаторазового використання: сучасний стан та перспективи подальшого розвитку, визначення потреби Повітряних Сил. *Збірник «Наука і техніка Повітряних Сил Збройних Сил України»,* 2013. № 1. С. 30–38. **5. Мосов С. П., Погорельський М. В., Салій С. М.** Безпілотна авіація у військовій справі. Київ: Інтерсервіс, 2019. 324 с. **6. Кучеренко Ю. В., Науменко М. В., Кузнецова М. Ю.** Аналіз досвіду застосування літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій. Харків: ІСЗЗІ ХНУПС, 2018. С. 76-83. URL: http://nbuv.gov. ua/UJRN/soivt_2018_1_5pdf (дата звернення: 04.07.2023). **7. Методичні** рекомендації підрозділам щодо боротьби з безпілотними літальними апаратами іранського виробництва «Shahed – 136» («Герань-2»). Київ: КСВ ЗСУ, 2022. 154 с.

REQUIREMENTS FOR THE COMBAT SYSTEM WITH UAVS

Shevchuk Vitalii ***(Candidate of Millitary Sciences)***
Kryvosheiev Vitalii ***(Candidate of Millitary Sciences Docent)***
Shvets Mykola

The National Defence University of Ukraine

The article outlines a number of issues that actualise the existing problems in the requirements for a system to combat enemy unmanned aerial vehicles. The purpose of the article is to summarise the requirements for a system for combating unmanned aerial vehicles based on the experience of fighting enemy UAVs during the repulsion of the armed aggression of the Russian Federation against Ukraine and to reveal the ways to combat them. In writing this article, the author uses the method of analysing the experience of combating enemy unmanned aerial vehicles gained during the repulsion of the armed aggression of the Russian Federation against Ukraine in 2014-2023, namely, the analysis of the functioning of the elements of the system for combating unmanned aerial vehicles. This makes it possible to determine the requirements for the system of combating unmanned aerial vehicles in general and its components in particular. Specifying such requirements meets the main task of reducing the effectiveness of the enemy's use of unmanned aerial vehicles against the state's critical infrastructure, military facilities, and civilians. This approach makes it possible to further develop common views on the tactics of the Armed Forces of Ukraine in the fight against unmanned aerial vehicles and improve the technical component of the system for combating enemy unmanned aerial vehicles.

Keywords: *unmanned aerial vehicles, combat system, control.*

References

1. Chipanskii, P., Segeda, S., (2020). Lessons from the anti-terrorist operation. 2016 year. [monograph]. Kiev: NUOU, 242. **2. Korolev, R. V., Koroliuk, N. O., Petrov, O. V., Sule, K. V., (**2017). Analysis of modern means of destroying unmanned aerial vehicles. Kharkiv: Collection of Scientific Works of the National Academy of Sciences of Ukraine, 4(53), 23-30. **3. VP7-00(03).01,** (2019). Methodological recommendations «Combating unmanned aerial vehicles» (based on the experience of carrying out OOS (formerly ATO)). Kiev: General Staff of the Armed Forces of Ukraine, 124. **4. Zharyk, O. M.,** (2013). The experience of creating and using multi-use shock UAVs: the current state and prospects for further development, defining the pipeline of the Air Force. Science and technology of the Air Force of the Armed Forces of Ukraine, 1, 30-38. **5. Mosov, S. P, Pogorelskyi M. V., Saliy, S. M.,** (2019). Unmanned aviation in military affairs. Kiev: Interservice, 324. 6**. Kucherenko, Yu. V., Naumenko, M. V., Kuznetsova, M. Yu.,** (2018). Analysis of the experience of using aircraft and determining the direction of their further development in the conduct of network-centric operations. Kharkiv, 76-83. URL: http://nbuv.gov.ua/ UJRN/soivt_2018_1_5pdf (date: 04.07.2023)**.7. Methodical** recommendations to the divisions regarding the fight against unmanned aerial vehicles of Iranian production «Shahed-136» («Gheran-2»). Kiev: Armed Forces of Ukraine, 2022. 154.

DOI:**10.33099/2311-7249/2023-47-2-139-146**

УДК: 623.773.4, 004.89

Цибуля Сергій Анатолійович *(кандидат технічних наук, старший дослідник)* [1]
Волокита Артем Миколайович *(кандидат технічних наук, доцент)* [2]

[1] ***Національний університет оборони України, Київ, Україна***
[2] ***Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна***

СПОСОБИ МАСКУВАННЯ ВІЙСЬКОВИХ ОБ'ЄКТІВ ВІД ВИЯВЛЕННЯ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ

У роботі розглянуті наявні підходи впливу на роботу алгоритмів штучного інтелекту, зокрема машинного навчання, що застосовуються в системах комп'ютерного зору для виявлення, класифікації та ідентифікації об'єктів. На даний час найпопулярнішою та найперспективнішою технологією розпізнавання образів є штучні нейронні мережі. Комп'ютерний зір застосовується у військовій справі для виявлення візуальних об'єктів певних класів: людей, озброєння та військової техніки, військових об'єктів тощо. Вхідними даними для аналізу можуть бути: фотографії, відеокадри чи відео потік реального часу, що отримані з космічних, повітряних або наземних засобів розвідки. Для боротьби з системами автоматичного виявлення об'єктів можливо застосовувати підходи, що здатні впливати на моделі машинного навчання, які використовуються у цих системах. Атака на моделі машинного навчання – це спеціальні дії щодо впливу на її елементи з метою досягти бажаної поведінки системи або перешкодити її коректній роботі. За результатами аналізу досліджень різних авторів визначено, що майже кожен алгоритм машинного навчання має певні вразливості. Під час виконання завдань інженерної підтримки військ щодо маскування військових об'єктів, найбільш доступними способами впливу на системи комп'ютерного зору, для введення їх в оману, є зміна фізичних властивостей об'єкта, що маскується, шляхом нанесення на його поверхню спеціальних покриттів і матеріалів. У якості покриттів можливо використовувати згенеровані змагальні патч-зображення, шляхом накладання або наклеювання їх на об'єкт та які здатні вносити завади в роботу алгоритмів засобу розвідки, прицілювання або наведення. Це особливо важливо в перспективі створення автономних систем зброї, які здатні виявляти, ідентифікувати цілі та самостійно приймати рішення на їх ураження.

Ключові слова: *штучний інтелект, машинне навчання, нейронна мережа, комп'ютерний зір, виявлення, ідентифікація, класифікація, інженерна підтримка, маскування військових об'єктів, атака ухилення, патч-зображення, змагальний приклад, отруєння набору даних.*

Вступ

Починаючи з 2017 року у світі розпочалася гонитва за світове лідерство між провідними державами у сфері розвитку штучного інтелекту. Протягом 2017–2019 років понад 30 країн світу (наприклад, Канада, Китайська народна республіка, Федеративна республіка Німеччина, Французька Республіка, російська федерація тощо), розробивши відповідні національні стратегії, визначили розвиток технологій штучного інтелекту одним із важливих пріоритетів державної політики. Так, уряд КНР поставив перед країною амбіційні плани щодо досягнення світового лідерства в області штучного інтелекту до 2030 року. За останнє десятиліття КНР більш ніж утричі збільшила свої інвестиції у наукові дослідження за цим напрямом [1]. Ураховуючи зростаючу роль штучного інтелекту в сферах загальнодержавного значення, розпорядженням Кабінету Міністрів України від 02 грудня 2020 року № 1556-р була схвалена Концепція розвитку штучного інтелекту в Україні [2].

У травні 2020 року було опубліковано доповідь Організації НАТО з науки та технологій «Тенденції у науці й технологіях: 2020–2040», в якій окреслені тенденції розвитку технологій протягом наступних 20 років [3]. Документ базується на аналізі відкритих наукових джерел і досліджень та певних національних науково-дослідних програм, а також ґрунтується на висновках багатьох провідних вчених, інженерів та аналітиків. Цим документом визначаються новітні напрями розвитку науки і технологій, які можуть якісно змінити види озброєння і матимуть вплив на розвиток збройних сил, колективної безпеки та оборони країн членів НАТО [4]. До цього переліку входять технології штучного інтелекту, аналізу неструктурованих даних, автономних транспортних засобів та робототехніки.

Постановка проблеми. Поняття «штучний інтелект» (англ. Artificial intelligence (далі – AI)) його алгоритми і математичні моделі набуло

широкого використання у повсякденному житті людства, застосовується в багатьох галузях: медицині, банківській діяльності, біржовій торгівлі, військовій справі, наукових дослідженнях тощо. Нині новини, що містять такі поняття як «машинне навчання» (англ. Machine learning (далі – ML)), «штучні нейронні мережі» (англ. Artificial neural network (далі – ANN)), «згорткові нейронні мережі» (англ. Convolutional neural network (далі – CNN)), «мережі глибокого навчання» (англ. Deep neural network (далі – DNN)), «генеративні змагальні мережі» (англ. Generative adversarial network (далі – GAN)), «великі дані» (англ. Big data), «комп'ютерний зір» (англ. Computer vision) перебувають на передовиці всіх засобів масової інформації.

Зважаючи на вищевикладене зазначимо, що останнім часом питанню підвищення стійкості критичних систем, що використовують технології штучного інтелекту, надається все більше уваги. Одним із важливих його елементів є кібербезпека систем машинного навчання, як складової частини галузі штучного інтелекту.

Аналіз останніх досліджень і публікацій. Розпізнавання образів – важливе завдання комп'ютерного зору, яке застосовується для виявлення візуальних об'єктів певних класів (людей, озброєння та військової техніки, військових об'єктів тощо) на таких цифрових зображеннях як фотографії, скріншоти з відео чи відеокадри. Розпізнавання образів набуло широкого розповсюдження в таких сферах, як безпека та відеоспостереження, інтелектуальна відео хірургія, маркетинг та реклама, автономні транспортні засоби, доповнена реальність та пошук зображень. Тому і найбільше теоретичних досліджень щодо порушення роботи алгоритмів штучного інтелекту, зокрема, машинного навчання, присвячено саме питанню атаки на автоматичне розпізнавання образів. Атаки на системи машинного навчання, з метою отримання певного практичного зиску, з'явилися спочатку в контексті протидії статистичним фільтрам спаму, системам виявлення вірусів та детектування зловмисного трафіку в мережі [5; 6]. Але жодна з розглянутих атак не призначена для впливу на штучні нейронні мережі, які на даний час є найпопулярнішою та найперспективнішою технологією розпізнавання образів.

Термін, що описує алгоритми впливу на машинне навчання – «змагальне машинне навчання» (англ. Adversarial machine learning (далі – AML)), а самі дії отримали назву «змагальні атаки». До набуття поширення машинного навчання, дослідження щодо AML мали лише теоретичний характер. Першими звернули увагу на те, що шляхом невеликих змін системи розпізнавання образів можна змусити видавати неправильні результати, співробітники підрозділу Google AI [7]. Надалі з'явилось досить багато досліджень, що розглядають приклади впливу змагальних атак [8].

Аналіз понад 2000 наукових статей, що пов'язані з безпекою в галузі штучного інтелекту, який був проведений фахівцями компанії Adversa AI, показав, що майже кожен алгоритм машинного навчання потенційно вразливий і має певні проблеми щодо конфіденційності та безпеки [9].

Перше всебічне дослідження змагальних атак на глибоке навчання в системах комп'ютерного зору представлено у статті [10]. У ній проаналізовано значний перелік наукових статей та обґрунтовано, що змагальні атаки є реальною загрозою глибокому навчанню на практиці, особливо в критично важливих програмах безпеки.

Спробу створити таксономію змагальних атак, шляхом аналізу понад 150 літературних джерел, починаючи з 2016 року, зроблено у роботі [11]. Автори розглянули 41 підхід до виконання фізичних змагальних атак у трьох основних завданнях комп'ютерного зору: виявлення, ідентифікація та класифікація.

Свою таксономічну схему для класифікації наявних фізичних змагальних атак на DNN мережі, як популярну технологію в задачах комп'ютерного зору, запропоновано в роботі [12]. Автори розглянули загальні характеристики фізичних змагальних атак та обговорюються проблеми, які необхідно вирішити для запобігання цих атак.

Армією США впроваджується концепція «мереже-центричної війни» (Network-centric warfare) і «мульти-доменної операції» (Multi-Domain Battle), що передбачає проведення військових операцій у різних просторах (морський, повітряний, кібернетичний, інформаційний тощо), і які вимагають від військ високої мобільності та швидкого прийняття рішень. Для реалізації цієї вимоги всі складові елементи збройних сил (особовий склад, озброєння та військова техніка (далі – ОВТ), штаби тощо) мають бути пов'язані єдиною інформаційною мережею для обміну інформацією в ході бойових дій у режимі реального часу. Одним зі способів вирішення цього завдання стало застосування рішень, які отримали назву «інтернет-бойових речей» (англ. Internet of Battle Things (далі – IoBT)) [13]. Тому, з урахуванням розповсюдження та перспективи IoBT, цікавим є комплексний аналіз нападу та захисту у сфері комп'ютерного зору інтернет речей, що проведено у дослідженні [14]. В роботі зазначено, що поєднання штучного інтелекту і периферійних обчислень, забезпечує розгортання алгоритмів глибокого навчання на периферійних пристроях та робить їх об'єктами привабливими для атак.

Метою статті є визначення способів підвищення ефективності маскування озброєння і військової техніки та інших військових об'єктів від їх виявлення, класифікації та ідентифікації системами штучного інтелекту, шляхом впливу на роботу алгоритмів штучних нейронних мереж, які застосовуються в галузі комп'ютерного зору.

Виклад основного матеріалу дослідження

Атака на модель машинного навчання це спеціальні дії впливу на її елементи (тренувальні дані, алгоритм, тестові дані тощо) з метою досягнення бажаної поведінки системи або перешкодити її коректній роботі. В атласі MITER, який створений спільно з IBM, NVIDIA, Bosch, Microsoft та іншими компаніями, виділено більш ніж 30 методик атак на алгоритми машинного навчання, які розподіляються на три основні типи атак [15]:

на набори даних для навчання;

під час навчання моделі;

під час виконання моделлю завдань за призначенням.

Під час навчання моделей, атаці (спеціальній модифікації, отруєнню) можуть бути піддані тренувальні або тестові дані. Створення наборів даних для навчання (image's data set), а, особливо, таких специфічних даних як зображення озброєння та військової техніки, є часозатратним процесом. Тому привабливим варіантом для розробників є не створення власних наборів, а застосування загально доступних. Найбільший відомий набір даних комп'ютерного зору є ImageNet (image-net.org). Це проєкт зі створення великої бази даних розмічених зображень призначених для тестування методів розпізнавання образів та машинного зору, містить в собі зразки військової техніки. Він має певні обмеження для використання, але знаходиться у вільному доступі на torrent серверах. На платформі Kaggle, для змагань з аналітики та передбачувального моделювання, можливо завантажити готовий набір зображень танків різних країн та поколінь «Military tanks dataset (images) a collections of various military tank image». На сайті images.cv також можна завантажити набір зображень танків у розмірах (16×16, 32×32 тощо) з розподілом набору на тренувальні та перевірочні частини у необхідних пропорціях. Без попередньої перевірки не можливо зрозуміти, чи всі ці загальнодоступні набори даних є коректними, чи «отруєними».

Проблема ускладнюється тим, що на роботу моделі машинного навчання може вплинути навіть невеликий обсяг «шкідливих» даних. Так, дослідження оцінювання впливу на алгоритм дозування ліків для пацієнтів, що працює на основі нейронної мережі, продемонструвало, що додавши 8% шкідливих даних до навчального набору, було отримано 75% змін від дозування, запропонованого алгоритмом, що навчений на незараженому навчальному наборі [16]. Тому, без впевненості про чистоту загальнодоступних навчальних наборів даних, не можна їх використовувати у системах військового призначення. Принциповим моментом для систем машинного навчання є те, що система навчається та перевіряється на основі одних даних, а практично працює з іншими.

Атаки на саму модель є найбільш ефективними. Проте зазначені атаки в реальному житті зустрічаються рідко, адже для їх проведення необхідно мати інформацію про алгоритм моделі або доступ до її навчальних даних. Водночас, враховуючи те, що створення власної моделі машинного навчання потребує певних теоретичних знань та часу, розробники систем комп'ютерного зору часто використовують такі популярні моделі як YOLO, Single-Shot Detector (SSD), Mask Region-based Convolutional Network (Mask R-CNN) тощо. Також, з метою економії часу та коштів, а деякі складні архітектури нейронних мереж не можливо навчити на звичайному комп'ютері, розробники виконують навчання моделей в хмарних сервісах або використовують вже попередньо навчені моделі нейронних мереж шляхом заміни останніх прошарків мережі під необхідне завдання. За таких умов, основні параметри та вагові коефіцієнти залишаються без змін [17]. Відповідно, якщо початкова модель зазнала втручання, то підсумкова модель частково успадкує видачу неправильних результатів [18].

Здебільшого атаками, що можна практично здійснити, є атаки, які виконуються на етапі застосування нейронних мереж – це, так звані, «атаки ухилення» (evasion attack). Їх метою є примушення мережі видавати неправильні відповіді у певних ситуаціях. Як правило, для атак ухилення використовуються «змагальні приклади» (adversarial examples), суть яких полягає у зміні вхідних даних так, що модель не може їх правильно інтерпретувати.

Атаки ухилення (рис. 1) ділять на різні категорії або групи за:

бажаною відповіддю;

доступністю моделі;

способом підбору завад.

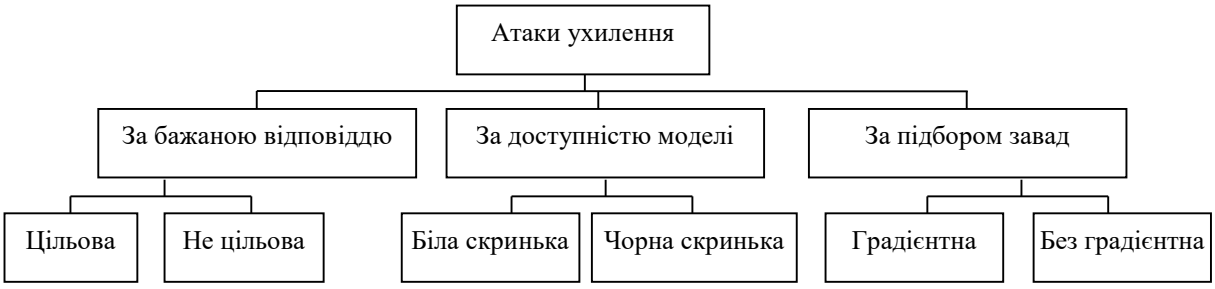


Рисунок 1 – Класифікація атак ухилення

Ця класифікація є лише однією із багатьох способів поділу атак ухилення на нейронні мережі. Класифікація атак може змінюватися з появою нових методів та відкриттям нових вразливостей нейронних мереж.

Атаки «за бажаною відповіддю» спрямовані на отримання певної відповіді від системи, та поділяються на два види:

нецільові (non-targeted), що виконуються з метою викликати будь-яку помилку або невірну класифікацію вхідних даних;

цільові (targeted), їх метою є отримання певних конкретних помилкових відповідей.

Атаки «за доступністю моделі» відображають рівень доступності до системи або моделі, що атакується. Під час атаки на білу скриньку (white-box) особа, що проводить атаку, має повний доступ до архітектури, параметрів та інформації про внутрішні процеси моделі. Під час атак на чорну скриньку (black-box) є обмежений або взагалі відсутній доступ до цієї інформації, вона може базуватися лише на зовнішніх спостереженнях та обміні даними з моделлю.

Атаки за способом «підбору завад» відображають методи, що використовуються для знаходження оптимальних завад або змін у вхідних даних. Атаки на основі градієнта (gradient-based) базуються на властивості моделей машинного навчання, що невеликі зміни вхідних даних можуть призводити до значних змін у вихідних результатах моделі. Градієнти використовуються для підрахунку змін, які максимізують або мінімізують функцію втрат, що призводить до помилкової класифікації. Безградієнтні (non-gradient-based) атаки використовують такі методи, як оптимізація, еволюційні алгоритми або генеративні моделі для пошуку оптимальних змін.

У реаліях військової справи, противник під час атаки на системи штучного інтелекту, не має доступу до цифрових вхідних даних (фотографій, відео) з безпілотних літальних апаратів, камер спостереження, головних частин самонаведення ракет і автономних боєприпасів, літаків розвідників або супутників. Також йому, зазвичай, не відомі моделі машинного навчання та їхня структура. Результати атаки можна оцінити лише за непрямими ознаками впливу або наступних дій противника. Тому, єдиним можливим способом перешкоджанню роботі систем комп'ютерного зору є атаки з фізичним впливом (physical attacks).

Атаки з фізичним впливом на нейромережі можна класифікувати за наступними напрямами:

вплив на середовище;

маніпуляція з вхідними даними;

вплив на систему обробки даних.

Під час атаки «впливу на середовище» змінюються або спотворюються дані, що надходять на сенсори системи. Це може бути фізична зміна навколишнього середовища (зміна освітлення, розміщення перешкод тощо) або зміна фізичних властивостей об'єкта (додавання спеціального покриття або матеріалу).

Під час «маніпуляції зі вхідними даними» змінюються дані, що надходять до системи. Це може бути фізична зміна зображення шляхом накладання спеціальних маркувань або спотворень.

Під час «впливу на систему обробки даних» відбувається прямий вплив на саму систему або її компоненти. Це може бути фізичне пошкодження, шляхом завдання вогневого удару по системі, або зміна її апаратної частини, вплив на сенсори (зміна поля зору або чутливості), зміна робочих параметрів, порушення роботи алгоритмів обробки даних або фізичне втручання у роботу нейромережі шляхом проведення кібератаки, маніпуляції з електричними сигналами, впровадження шуму та завад усередині системи за допомогою засобів РЕБ.

Узагалі, класифікація атак фізичного впливу на нейромережі є гнучкою і залежить від контексту, системи та цілей під час атаки. Ці типи атак можуть бути комбіновані або використовуватися у різних комбінаціях для досягнення бажаного ефекту.

Під час виконання завдань інженерної підтримки військ щодо маскування військових об'єктів найбільш доступними способами впливу на системи комп'ютерного зору є зміна фізичних властивостей об'єкта, що маскується, шляхом нанесення на його поверхню спеціальних покриттів і матеріалів. Як запропоновано в роботі [19], з метою маскування, на поверхню об'єкта нанести змагальне покриття з аерогелю. Щоб спростити та здешевити фізичну реалізацію, автори оптимізували змагальну текстуру покриття, створивши її подібною до QR-коду. Під час тестування на об'єкті з нанесеною текстурою, продуктивність детектора на основі моделі YOLOv3 знизилась на 64,6%.

Фізична зміна зовнішнього виду об'єкта можлива шляхом накладання на нього покриттів зі спеціально сформованих зображень, так званих змагальних патчей (англ. patch клаптик) (рис. 2).

Змагальний патч – це спеціально згенероване зображення з певними візерунками, яке можна прикріпити на поверхню цільового об'єкта. Його перевагою є те, що вони мають просте використання. Таке зображення можна роздрукувати на принтері, а потім наклеїти/повісити на необхідний об'єкт. Цей вид атак називається патч-атаки (patch attack).

Вперше патч-атаку було описано у роботі [20], де шляхом заміни локальної області зображення на оптимізовану текстуру вдалося досягти зниження ефективності роботи DNN мережі. Практичне застосування патч-зображень на фізичні об'єкти, було досліджено у роботі [21]. Автори, шляхом накладання наліпок на автомобіль Toyota Camry, домоглися порушити роботу нейромережі, що призвело до неможливості виявлення автомобіля

системою розпізнавання. Найбільш відомий приклад патч-атаки пов'язаний із розпізнаванням дорожніх знаків, процес розпізнавання яких вдалося порушити за допомогою декількох наліпок патч-зображень зроблених на знак [22]. Результати експерименту свідчать, що оптимізоване патч-зображення може значно знизити (до 47%) продуктивність детектора системи розпізнавання [23].

Застосування змагальних атак має широке коло використання, як для маскування об'єктів від автоматичного виявлення на аерофотознімках, так і на зображеннях дистанційного зондування Землі з космосу. Практичні дослідження щодо приховування від автоматичного розпізнавання літаків на аерофотознімках, шляхом нанесення змагального зображення на ділянки поверхні землі, де розміщений об'єкт (рис. 3), проведені у роботі [24]. Автори перевірили вплив цих змагальних зображень на роботу 16 популярних моделей класифікаторів (YOLO, SSD, Faster R-CNN, Swin Transformer, TOOD тощо). Результати дослідження засвідчили, що під час використання змагальних зображень ймовірність виявлення об'єктів деякими класифікаторами впала до 0.

(a) Camouflage net (b) Patch camouflage

Рисунок 2 – Маскування за допомогою маскувальної сітки (a) та накладанням патч-зображення (b) [23]

Рисунок 3 – Зліва розміщені літаки, для приховування яких використовуються змагальні патч-зображення [24]

Результати експериментів проведених щодо створення змагальних прикладів для тестувальних систем з аналізу зображень дистанційного зондування, показали вразливість CNN, ймовірність видачі неправильного результату якими досягала понад 80% [25]. Незважаючи на те, що застосування змагальних зображень показує задовільну ефективність атак на нейронні мережі є недоліки, що стримують ефективність такого типу атак:

лише певна область зображення є вирішальною для впливу на прийняття рішення системою розпізнавання, а зміна неспецифічних областей може мати зворотний ефект;

патч-зображення являють собою мозаїчний візерунок, який виглядає неприродньо та помітні для людини-спостерігача, що шкодить скритності об'єкта.

Враховуючи наведене, одним з напрямів розвитку таких атак є адаптивне коригування форми патчів. Наприклад, використання генеративних змагальних мереж для автоматичного створення зображень, малюнок яких буде найбільш наближеним до природних зображень.

На ефективність маскування впливають різні демаскуючі ознаки. Тінь від об'єкта, її контрастність, розмір, кольорова гамма тощо – можуть зробити об'єкт помітним або незвичним порівняно з навколишнім середовищем. Щоб розв'язати цю проблему в роботі [26] автори провели оптимізацію 2D-зображення об'єкта і трансформували його текстуру для наближення ефекту тіні та нанесли її на масштабовану модель Tesla Model 3, яку надалі роздрукували за допомогою 3D-принтера. Результати проведення експерименту свідчать про те, що середнє зниження продуктивності двох детекторів на базі моделей EfficientDetD0 і YOLOv4 становить 47,5%. Також результати підтвердилися моделюванням виявлення об'єктів у середовищі CARLA Simulator.

Одним із завдань маскування є імітація військових об'єктів [27]. Для цього застосовуються, як плоскі 2D горизонтальні та вертикальні макети, так макети у вигляді

3D-об'єктів, що мають вигляд реальних об'єктів ОВТ. Питання введення в оману та порушення розпізнавання нейронною мережею шляхом побудови 3D-об'єктів розглянуто у роботі [28]. Авторами запропонований алгоритм Expectation Over Transformation, який дозволяє побудувати змагальні 3D приклади через процес 3D-рендерінга. Результати цих досліджень дозволили генерувати змагальні приклади, які призводять до невірної роботи нейромереж з класифікації об'єктів. На рис. 4 показано приклад надрукованої на 3D-принтері черепахи, яка розпізнається класифікатором TensorFlow InceptionV3, як гвинтівка (де, зелена рамка – черепаха, червона – гвинтівка, чорна – не черепаха). Результати цієї роботи підтверджують, що змагальні атаки можуть застосовуватися для імітації 3D об'єктів.

Рисунок 4 – Результати роботи класифікатора InceptionV3 [27]

Таким чином, можна стверджувати, що під час використання змагальних атак на системи виявлення та класифікації об'єктів, які працюють на основі алгоритмів машинного навчання таких, як нейронні мережі, можна досягти успішних результатів цих атак:

1. Змагальне (маскувальне) зображення знижує ймовірність виявлення об'єкта, а ділянка розміщення об'єкта не пропонується системою або пропонується лише частково як можливий кандидат для класифікації.

2. Ділянка перебування об'єкта визначена, але невірно класифікована, або оцінка класифікації надто низька, щоб подолати порогове значення показника критерія прийняття рішення про виявлення.

3. Ділянка перебування об'єкта успішно визначена та класифікована, але сам об'єкт не має чіткої класифікації.

Висновки й перспективи подальших досліджень

У роботі розглянуті наявні підходи впливу на моделі машинного навчання, що застосовуються для виявлення та ідентифікації об'єктів системами комп'ютерного зору. За результатами проведеного аналізу, можна констатувати, що майже кожен алгоритм машинного навчання принципово вразливий і має проблеми з безпекою. Тому, кожний елемент системи штучного інтелекту військового призначення (математичні моделі, алгоритми машинного навчання та набори вхідних даних, що використовуються для навчання й тестування) спрямований на підвищення обороноздатності держави і зобов'язаний мати певні ступені обмеження розповсюдження та конфіденційності. Важливість цього питання зазначається у керівних документах як відомчого, так і загальнодержавного рівня [29; 30], де до інформації з обмеженим доступом відносяться: відомості про несекретне програмне забезпечення, що використовується під час виконання розвідувальних завдань; напрями, науково-технічні ідеї, результати, можливість застосування (реалізації) фундаментальних, пошукових прикладних наукових досліджень у системах або їх складових з метою підвищення ефективності технічної розвідки, засобів прицілювання або наведення, їх можливостей з виявлення об'єктів та цілей на фоні місцевості; покращення ефективності протидії засобам прицілювання або наведення зброї противника, зменшення можливостей з виявлення об'єктів та цілей.

Це є особливо важливим в перспективі створення автономних систем зброї, які будуть здатні виявляти, ідентифікувати та самостійно приймати рішення на ураження цілей.

Список бібліографічних посилань

1. America's eroding technological advantage: nds rdt&e priorities in an era of great-power competition with China. URL: https://govini.com/wp-content/uploads/2021/04/Govini_NDS-Priorities-RDTE.pdf (дата звернення: 26.05.2023). **2. Про схвалення** Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р (дата звернення: 26.05.2023). **3. Reding D.F., Eaton J.** Science & Technology Trends: 2020-2040. Exploring the S&T Edge. *NATO Science & Technology Organization*. Brussels. Belgium. 2020. P. 160. URL: https://www.sto.nato.int/pages/tech-trends.aspx. (дата звернення: 26.05.2023). **4. Войтовський К. Є.** Глобальні тренди розвитку науки і технологій: нові виклики і можливості. Київ : Національний інститут стратегічних досліджень, 2020. 6 с. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/globalni-trendi-rozvitku-nauki-i-tekhnologiy-novi-vikliki-i (дата звернення: 30.10.2022). **5. Lowd D., Meek C.** Good word attacks on statistical spam filters. *Proceedings of the second conference on email and anti-spam*, 2005. P. 1–8. **6. Biggio B., Nelson B.and Laskov P.** Poisoning attacks against support vector machines. Proceedings of 29th Int. Conf. Mach. Learn, 2012. P. 1467–1474. DOI: 10.48550/arXiv.1206.6389. **7. Szegedy C. et al.** Intriguing properties of neural networks. CoRR, abs/1312.6199. 2013. P. 10. DOI: 10.48550/arXiv.1312.6199. **8. Carlin N.** A Complete list of all (arXiv) adversarial example papers. URL: https://nicholas.carlini.com/writing/2019/all-adversarial-example-papers.html. (дата звернення: 26.05.2023). **9. Adversa AI.** URL: https://adversa.ai/report-secure-and-trusted-ai/ (дата звернення: 26.05.2023). **10. Akhtar N., Mian A.** Threat of Adversarial Attacks on Deep Learning in

Computer Vision: A Survey. *IEEE Access*. 2018. Vol. 6. P. 14410–14430. DOI: 10.1109/ACCESS.2018.2807385. **11. Wei Hui et al.** Physical Adversarial Attack meets Computer Vision: *A Decade Survey*. 2022. P. 32. DOI: 10.48550/arXiv.2209.15179. **12. Wang D., Yao W., Jiang T., Tang G. and Chen X.** A Survey on Physical Adversarial Attack in Computer Vision. *ArXiv abs/2209.14262*. 2022. P. 26. DOI: 10.48550/arXiv.2209.14262. **13. Niranjan S. et al**. Analyzing the applicability of Internet of Things to the battlefield environment. International *Conference on Military Communications and Information Systems*. Brussels, Belgium, 23 May, 2016. P. 1–8. DOI: 10.1109/ICMCIS.2016.7496574. **14. Liang H., He E., Zhao Y., Jia Z., Li H.** Adversarial Attack and Defense: A Survey. *Electronics*. 2022. № 11(8). P. 1283. DOI: 10.3390/electronics11081283. **15. MITRE ATLAS™** (Adversarial Threat Landscape for Artificial-Intelligence Systems). URL: https://atlas.mitre.org/ (дата звернення: 26.05.2023). **16. Jagielski M. et al.** Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. *IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, 2018. P. 19–35. DOI: 10.1109/SP.2018.00057. **17. Гонтаренко Я. Д., Красношлик Н. О.** Використання нейронних мереж для розпізнавання дій людини по відео. *Вісник Черкаського національного університету імені Б. Хмельницького. Серія «Прикладна математика. Інформатика».* 2019. № 2. С. 59–72. DOI: 10.31651/2076-5886-2019-2-59-72. **18. Gu T., Liu K., Dolan-Gavitt B. and Garg S.** BadNets: Evaluating backdooring attacks on deep neural networks. *IEEE Access*. 2019. Vol. 7. P. 47230-47244. DOI: 10.1109/ACCESS.2019.2909068. **19. Zhu X., Hu Z., Huang S., Li J. and Hu X.** Infrared invisible clothing: Hiding from infrared detectors at multiple angles in real world. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2022. P. 13317-13326. **20. Brown T., Mané D., Roy A., Abadi M. and Gilmer J.** Adversarial patch. 2017. *ArXiv:1712.09665*. **21. Zhang Y., Foroosh H., David P. and Gong B.** CAMOU: Learning physical vehicle camouflages to adversarially attack detectors in the wild. International Conference on Learning Representations. URL: https://openreview.net/pdf?id=SJgEl3A5tm. (дата звернення: 26.05.2023). **22. Eykholt K. et al.** Robust Physical-World Attacks on Deep Learning Visual Classification. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2018. P. 1625-1634. DOI: 10.48550/arXiv.1707.08945. **23. Hollander R. den et al.** Adversarial patch camouflage against aerial detection. *Artificial Intelligence and Machine Learning in Defense Applications II.* Vol. 11543. SPIE, 2020, P. 77–86. DOI: 10.1117/12.2575907. **24. Lian J., Wang X., Su Y., Ma M. and Mei S.** CBA: Contextual Background Attack Against Optical Aerial Detection in the Physical World. *IEEE Transactions on Geoscience and Remote Sensing*. 2023. Art no. 5606616. Vol. 61. P. 1–16. DOI: 10.1109/TGRS.2023.3264839. **25. Chen L. et al.** Attack Selectivity of Adversarial Examples in Remote Sensing Image Scene Classification. *IEEE Access.* 2020. Vol. 8. P. 137477–137489. DOI: 10.1109/ACCESS.2020.3011639. **26. Suryanto N. et al.** Dta: Physical camouflage attacks using differentiable transformation network. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2022. P. 15305–15-14. DOI: 10.48550/arXiv.2203.09831. **27. Керівництво** з виконання інженерних заходів маскування військ та об'єктів : наказ начальника Головного управління оперативного забезпечення Збройних сил України від 06.12.2017 № 90. Київ. 138 с. **28. Athalye A., Engstrom L., Ilyas A. and Kwok R.** Synthesizing Robust Adversarial Examples. 2017. arXiv:1707.07397. **29. Про затвердження** Переліку відомостей Міністерства оборони України, які містять службову інформацію (ПСІ – 2016) (зі змінами) : Наказ Міністерства оборони України від 27.12.2016 № 720. 31 с. **30. Про затвердження** Зводу відомостей, що становлять державну таємницю : Наказ Служби безпеки України від 23.12.2020 № 383. 121 с.

WAYS TO MASK MILITARY OBJECTS FROM DETECTION BY ARTIFICIAL INTELLIGENCE SYSTEMS

Tsybulia Serhii *(Candidate of Technical Sciences, Senior Researcher)* [1]
Volokyta Artem *(Candidate of Technical Sciences, Associate Professor)* [2]

[1] *The National Defence University of Ukraine, Kyiv, Ukraine*
[2] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine*

The paper examines available approaches to influence the work of artificial intelligence algorithms, in particular machine learning, used in computer vision systems for object detection, identification, and classification. Currently, the most popular and most promising pattern recognition technology is artificial neural networks. Computer vision is used in military affairs to detect visual objects of certain classes: people, weapons and military equipment, military objects, etc. The input data for the analysis can be: photographs, video frames or real-time video stream obtained from space, air or ground reconnaissance means. To combat automatic object detection systems, it is possible to apply approaches capable of influencing the machine learning models used in these systems. An attack on a machine learning model is a special action to influence its elements in order to achieve the desired behavior of the system or prevent its correct operation. Based on the results of the analysis of research by various authors, it was determined that almost every machine learning algorithm has certain vulnerabilities. During the execution of tasks of engineering support of the troops regarding the camouflage of military objects, the most accessible ways of influencing computer vision systems, in order to mislead them, is to change the physical properties of the masked object by applying special coatings to its surface and materials As coatings, it is possible to use generated adversarial patch images, by superimposing or pasting them on the object, and which are capable of interfering with the work of the

reconnaissance, aiming or guidance algorithms. This is especially important in the perspective of creating autonomous weapon systems capable of detecting, identifying targets and independently making decisions to destroy them.

Keywords: *artificial intelligence; machine learning; artificial neural networks; computer vision; detect; identify; classify; engineering support; camouflage of military objects; evasion attack; adversarial patch images; adversarial examples; data poisoning.*

References

1. America's eroding technological advantage: nds rdt&e priorities in an era of great-power competition with China. Avaible at: <https://govini.com/wp-content/uploads/2021/04/Govini_NDS-Priorities-RDTE.pdf> [Accessed 26 May 2023]. **2. Pro skhvalennja** Koncepciji rozvytku shtuchnogho intelektu v Ukrajini [On the approval of the Concept of the development of artificial intelligence in Ukraine]. Avaible at: <https://zakon.rada.gov.ua/laws/show/1556-2020-p> [Accessed 26 May 2023]. **3. Reding, D.F., Eaton, J.** 2020. Science & Technology Trends: 2020-2040. Exploring the S&T Edge. Avaible at: <https://www.sto.nato.int/pages/tech-trends.aspx> [Accessed 26 May 2023]. **4. Voitovsky, K. E.** 2020. Ghlobaljni trendy rozvytku nauky i tekhnologhij: novi vyklyky i mozhlyvosti [Global trends in the development of science and technology: new challenges and opportunities]. National Institute of Strategic Studies. Avaible at: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/globalni-trendi-rozvitku-nauki-i-tekhnologiy-novi-vikliki-i> [Accessed 26 October 2022]. **5. Lowd, D., Meek, C.** 2005. Good word attacks on statistical spam filters. Proceedings of the second conference on email and anti-spam (CEAS), pp. 1-8. **6. Biggio, B., Nelson, B. and Laskov, P.** 2012. Poisoning attacks against support vector machines. Proceeding 29th Int. Conf. Int. Conf. Mach. Learn, pp. 1467-1474. doi: 10.48550/arXiv.1206.6389. **7. Szegedy, C. et al.** 2013. Intriguing properties of neural networks. CoRR, abs/1312.6199. 10 p. doi: 10.48550/arXiv.1312.6199. **8. Carlin, N.A.** 2019. Complete list of all (arXiv) adversarial example papers. Avaible at: <https://nicholas.carlini.com/writing/2019/all-adversarial-example-papers.html> [Accessed 26 May 2023]. **9. Adversa**, AI. Avaible at: <https://adversa.ai/report-secure-and-trusted-ai/> [Accessed 26 May 2023]. **10. Akhtar, N., Mian, A.** 2018. Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey. IEEE Access, vol. 6, pp. 14410-14430. doi: 10.1109/ACCESS.2018.2807385. **11. Wei Hui et al.** 2022. Physical Adversarial Attack meets Computer Vision: A Decade Survey. doi: 10.48550/arXiv.2209.15179. **12. Wang, D., Yao, W., Jiang, T., Tang, G. and Chen, X.** 2022. A Survey on Physical Adversarial Attack in Computer Vision. ArXiv abs/2209.14262. doi: 10.48550/arXiv.2209.14262. **13. Suri, N. et al.** 2016. Analyzing the applicability of Internet of Things to the battlefield environment. International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, May 23, pp. 1-8, doi: 10.1109/ICMCIS.2016.7496574. **14. Liang, H., He, E., Zhao, Y., Jia, Z., Li, H.** 2022. Adversarial Attack and Defense: A Survey. Electronics, no. 11(8): 1283. doi: 10.3390/electronics11081283. **15. MITRE** ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems). Avaible at: <https://atlas.mitre.org/> [Accessed 26 May 2023]. **16. Jagielski, M. et al.** 2018. Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. IEEE Symposium on Security and Privacy, San Francisco, USA. pp. 19-35. doi: 10.1109/SP.2018.00057. **17. Ghontarenko, Ja.D., Krasnoshlyk, N.O.** 2019. Vykorystannja nejronnykh merezh dlja rozpiznavannja dij ljudyny po video [Using neural networks to recognize human actions on video.] Visnyk Cherkasjkogho nacionaljnogho universytetu imeni B. Khmeljnycjkogh, no № 2, pp. 59-72. doi: 10.31651/2076-5886-2019-2-59-72. **18. Gu, T., Liu, K., Dolan-Gavitt, B., and Garg, S.** 2019. BadNets: Evaluating backdooring attacks on deep neural networks. IEEE Access, vol. 7, pp. 47230-47244. doi: 10.1109/ACCESS.2019.2909068. **19. Zhu, X., Hu, Z., Huang, S., Li, J. and Hu, X.** 2022. Infrared invisible clothing: Hiding from infrared detectors at multiple angles in real world. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 13317-13326. **20. Brown, T., Mané, D., Roy, A., Abadi, M. and Gilmer, J.** 2017. Adversarial patch. arXiv:1712.09665. **21. Zhang, Y., Foroosh, H., David, P. and Gong, B.** 2018. CAMOU: Learning physical vehicle camouflages to adversarially attack detectors in the wild. International Conference on Learning Representations. Avaible at: <https://openreview.net/pdf?id=SJgEl3A5tm> [Accessed 26 May 2023]. **22. Eykholt, K. et al.** 2018. Robust Physical-World Attacks on Deep Learning Visual Classification. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 1625-1634. doi: 10.48550/arXiv.1707.08945. **20. Hollander, R. et al.** 2020. Adversarial patch camouflage against aerial detection. Artificial Intelligence and Machine Learning in Defense Applications II, vol.11543. SPIE, pp. 77-86. doi: 10.1117/12.2575907. **24. Lian, J., Wang, X., Su, Y., Ma, M. and Mei, S.** 2023. CBA: Contextual Background Attack Against Optical Aerial Detection in the Physical World. IEEE Transactions on Geoscience and Remote Sensing, vol. 61, pp. 1-16, Art no. 5606616. doi: 10.1109/TGRS.2023.3264839. **25. Chen, L. and al.** 2020. Attack Selectivity of Adversarial Examples in Remote Sensing Image Scene Classification 2020. IEEE Access, vol. 8, pp. 137477-137489. doi: 10.1109/ACCESS.2020.3011639. **26. Suryanto, N. et al.** 2022. Physical camouflage attacks using differentiable transformation network. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 15305–15314. doi: 10.48550/arXiv.2203.09831. **27. Guidelines** for the implementation of engineering measures for the camouflage of troops and objects. 2018. Kyiv: Main Department of Operational Support of the Armed Forces of Ukraine. 6 Dec. № 90. **28. Athalye, A., Engstrom, L., Ilyas A. and Kwok, R.** 2017. Synthesizing Robust Adversarial Examples. arXiv:1707.07397. **29. On approval** of the List of information of the Ministry of Defense of Ukraine, which contains official information. 2016. Kyiv: Ministry of Defense of Ukraine. 27 Dec. № 720. **30. On approval** of the Compendium of information constituting a state secret. 2020. Kyiv: Security Service of Ukraine. 23 Dec. № 383.

DOI:**10.33099/2311-7249/2023-47-2-147-154**

УДК: 355.424.4

Шкурат Богдан Жоржович

Національний університет оборони України, Київ, Україна

МЕТОДИКА ДИНАМІЧНОГО РОЗПОДІЛУ РЕСУРСІВ У СПІЛЬНИХ ДІЯХ НАЗЕМНИХ І ПОВІТРЯНИХ ЗАСОБІВ ПРОТИПОВІТРЯНОЇ ОБОРОНИ

Досвід російсько-української війни та інших сучасних збройних конфліктів у світі свідчить, що протиповітряна оборона відіграє значну роль під час бойових дій. Зазвичай, до складу системи протиповітряної оборони входять вогневі засоби наземного і повітряного базування, спільні дії яких дають змогу забезпечити потрібний рівень ефективності її функціонування. Але обмежена координація спільних дій може не лише знизити їх ефективність, а й призвести до конфліктних ситуацій або таких небезпечних явищ як «дружній вогонь». Існуючі дослідження стосовно особливостей реалізації спільних проєктів виконавцями в умовах невизначеності, не можуть напряму бути використані під час планування та ведення бойових дій різнорідними вогневими засобами, особливо за таких динамічних змін обстановки, якими супроводжується протиповітряна оборона. Відповідно, постає завдання вирішення конфлікту інтересів вогневих складових системи протиповітряної оборони, який може полягати в раціональному розподілі ресурсів між ними. В статті розроблено методику визначення оптимальних обсягів ресурсів, які доцільно розподілити наземним і повітряним вогневим засобам протиповітряної оборони під час спільного виконання ними завдань в динаміці бойових дій, а звідси, і потрібної для цього кількості наземних і повітряних вогневих засобів. Під ресурсом у статті розуміється час та (або) простір, які характеризують межі виконання завдань. Зазначена методика використовує методи теорії прийняття рішень, теорії ігор, управління проєктами та комплексно враховує не лише середній ресурс, в якому здатний виконувати завдання один вогневий засіб, але розглядає показники раціональності його використання та ризиків, викликаних відхиленням від призначеного вогневим засобам обсягу ресурсу. На підставі означених показників формуються пріоритети під час розподілу ресурсів, що будуть визначати частку завдань, виділену на окремий вогневий засіб, а звідси і на наземну та повітряну складові системи протиповітряної оборони. Крім того, для врахування можливих відхилень у процесі визначення часток участі наземних і повітряних засобів у спільному виконанні завдань з протиповітряної оборони, обґрунтовано спосіб визначення області оптимального розподілу ресурсу під час розрахування потрібної кількості вогневих засобів. Наведена методика може бути застосована в алгоритмах систем підтримки прийняття рішень, зокрема, під час визначення варіантів розподілу зусиль між наземними та вогневими засобами протиповітряної оборони під час їхніх спільних дій.

Ключові слова: *протиповітряна оборона, вогневий засіб, зенітні ракетні війська, винищувальна авіація, спільні дії, взаємодія, розподіл ресурсів, конфлікт інтересів.*

Вступ

Постановка проблеми. Російсько-українська війна довела необхідність розгортання та підтримання функціонування системи протиповітряної оборони (далі – ППО), яка була б здатна ефективно знищувати наявні та перспективні засоби повітряного нападу. Складові системи ППО, такі як підсистеми прикриття об'єктів наземними та повітряними вогневими засобами (відповідно зенітного ракетно-артилерійського та авіаційного прикриття), можуть виконувати завдання як окремо, так і спільно. В останньому випадку простір спільного виконання завдань зазвичай обмежується зоною дії наземних вогневих засобів ППО. Спільне застосування наземних і повітряних вогневих засобів дає змогу не тільки забезпечити визначений рівень ефективності системи ППО, але й за певних умов може призвести до так званого «синергетичного» ефекту. Разом з тим, недостатньо якісна організація спільного застосування в одній зоні різних вогневих засобів може не тільки знизити ефективність виконання спільних завдань (наприклад, шляхом обмеження дій вогневих засобів–партнерів), але й призвести до таких небезпечних явищ, як «дружній вогонь».

Отже, між складовими системи ППО може виникнути конфлікт інтересів під час розподілу ресурсів. Водночас, під ресурсом доцільно розуміти «запаси чого-небудь, які можна використати в разі потреби; засіб, можливість, якими можна скористатися в разі необхідності» [1] або «щось, що може бути використане для досягнення мети; корисна або цінна властивість чи

якість, що мають людина або організація» («something that can be used to help achieve an aim; a useful or valuable possession or quality that a person or organization has») [2]. Тому, це можуть бути будь-які вимірювальні засоби, що потрібні для виконання завдань і підлягають розподілу між виконавцями. Оскільки розглядаються вогневі складові системи ППО під час виконання завдань (веденні бойових дій стосовно відбиття ударів повітряного противника), то до ресурсів слід віднести: особовий склад, озброєння, боєприпаси, цілі, час та простір.

Водночас озброєння та боєприпаси для наземних і повітряних вогневих засобів різні та підлягають розподілу тільки між однотипними підрозділами, а особовий склад має підготовку на конкретні типи озброєння. Тому завданням особи, яка приймає рішення під час управління системою ППО, буде розподіл інших типів ресурсів: цілей, часу та простору. Але слід зауважити, що цілі є нестабільним ресурсом, кількість якого важко спрогнозувати, тому він буде підлягати розподілу тільки по мірі їх виявлення, що є окремим об'єктом для вивчення. До того ж, одночасна робота по цілях наземних і повітряних вогневих засобів ППО в одній зоні супроводжується високою ймовірністю «дружнього вогню».

Тому в подальшому дослідженні будуть розглядатися такі типи ресурсу, як простір і час. Їх особливістю під час ведення бойових дій є потреба повного розподілу, оскільки існуючий нерозподілений простір або час можуть призвести до того, що цим скористається противник у своїх інтересах.

Аналіз останніх досліджень і публікацій. Завдання розподілу ресурсів між виконавцями розглядається у джерелах як військової [3–6], так і цивільної спрямованості, зокрема в економічній сфері [7] та сфері інформаційних технологій [8]. Але вказані джерела не можуть бути напряму використані для розподілу ресурсів між наземними та повітряними вогневими засобами. Так, в [3] враховується динаміка бойових дій та вплив втрат від противника, але розглядається в першу чергу розподіл бойових засобів між підрозділами, які є однорідними, що не зовсім підходить для ситуації застосування різнорідних сил. У [7] розглядається такий важливий показник, як ефективність використання ресурсів виконавцем, а також штрафи за відхилення використаних ресурсів від заявлених. Але виконавці в цьому випадку теж є однорідними. До того ж не розглядаються ризики, викликані взаємним впливом виконавців один на одного. Автором [8] запропоновано врахування фактору невизначеності (новизни) у процесі планування термінів спільного проєкту для групи виконавців і викликаних цим ризиків. Проте вказаний підхід більше стосується етапу планування проєкту і не розглядає можливі зміни в динаміці його виконання. Отже, існує ряд досліджень стосовно особливостей спільного виконання завдань виконавцями в умовах невизначеності, але запропоновані в них підходи не можуть бути напряму застосовані у процесі планування та ведення спільних дій різнорідними вогневими засобами, особливо за таких динамічних змінах обстановки, якими супроводжується ППО. Адже, під час виконання завдань щодо ураження противника, зокрема повітряного противника, розглядаються зазвичай розподіл озброєння, боєприпасів, особового складу, і частково – часу. Разом із тим, простір як ресурс не розглядається, а розподіляється директивно з урахуванням існуючих нормативів та методик. Розподіл часу при плануванні бойових дій здійснюється зазвичай вручну, спираючись на середньостатистичні показники та нормативи. Тому, подальший розвиток науково-методичного апарату, з метою можливості його використання під час розподілу ресурсів між різнорідними засобами ППО у процесі виконання ними спільних завдань, є важливим науковим завданням.

Метою статті є розроблення методики динамічного розподілу ресурсів між наземними та повітряними вогневими засобами протиповітряної оборони під час їх спільних дій для подальшого застосування в алгоритмах систем підтримки прийняття рішень при визначенні варіантів розподілу зусиль між наземними та вогневими засобами протиповітряної оборони.

Виклад основного матеріалу дослідження

Розподіл ресурсів в економіці та сфері інформаційних технологій (далі – ІТ) зазвичай починається з отримання заявок від виконавців (визначення потрібних ресурсів в ІТ). Водночас слід враховувати, що виконавці в своїх інтересах будуть прагнути до найбільшої кількості заявленого ресурсу [7; 8].

На відміну від цієї ситуації, командири вогневих підрозділів будуть одночасно прагнути максимальної кількості озброєння та боєприпасів для виконання завдань, але мінімальної частки залучення у виконанні спільних завдань для найточнішого їх виконання з мінімальною витратою боєприпасів та збереження готовності до подальших бойових дій.

В обох випадках перед особою, що приймає рішення (керівником, командиром, командувачем, в подальшому – командувач) постає завдання – розподілити наявний ресурс так, щоб були задіяні всі учасники за оптимальної ефективності реалізації проєкту (тобто забезпеченні ефективності ППО). Тому для подальшого дослідження доцільно уточнити поняття ефективності.

Загально прийнято визначати ефективність як співвідношення між досягненим результатом та використаними ресурсами [9], а за умови, що результатом роботи системи ППО буде кількість уражених повітряних цілей, то ефективність системи ППО доцільно визначати за виразом:

$$E_{ППО} = \frac{N_ц}{R}, \quad (1)$$

де $N_ц$ – кількість уражених цілей;

R – витрачений ресурс.

Для подальшого дослідження доцільно ввести такі обмеження та припущення:

керівництво силами та засобами ППО у процесі відбиття удару повітряного противника здійснюється централізовано однією особою, яка приймає рішення, в тому числі на розподіл ресурсу між наземними та повітряними вогневими одиницями (далі – ВО);

в зоні бойових дій наземні ВО одного типу розташовані рівномірно;

повітряні засоби ППО, попередньо виведені в точку обстрілу цілі, або час їх виведення на ціль розраховуються заздалегідь так, що в потрібний момент бойових дій вони здатні виконувати поставлені завдання без додаткових затримок;

підтримка прийняття рішень і постановка завдань підлеглим силам та засобам здійснюється із застосуванням автоматизованих систем управління або спеціалізованого програмного забезпечення, тому час на постановку завдань вогневим одиницям не враховується;

під час спільних дій наземних та повітряних засобів ППО можливі ризики втрат своїх ВО, в тому числі від «дружнього вогню».

Оскільки угруповання ППО складається з наземних і повітряних вогневих засобів, то сукупний ресурс буде розподілятися між ними та мати такий вигляд:

$$R = R_{нз} + R_{пз}, \quad (2)$$

де $R_{нз}$ – ресурс, виділений наземним вогневим засобам;

$R_{пз}$ – ресурс, виділений повітряним вогневим засобам.

Ураховуючи критерій оптимальності, командувач буде прагнути до максимізації сукупної ефективності ППО:

$$E_{ППО} = E_{нз}(R_{нз}) + E_{пз}(R_{пз}) \to \max \quad (3)$$

де $E_{нз}$ – вклад наземних вогневих засобів в сукупну ефективність;

$E_{пз}$ – вклад повітряних вогневих засобів в сукупну ефективність.

Але необґрунтоване збільшення призначеного кожній складовій ресурсу в цьому випадку призведе до падіння ефективності за однакової кількості знищених цілей. Ураховуючи приблизно постійне значення ресурсу (розміри зони бойових дій або час бойових дій), графік ефективності кожної складової ППО залежно від призначеного їй ресурсу, в узагальненому і спрощеному випадку, буде мати вигляд, наведений на рис. 1.

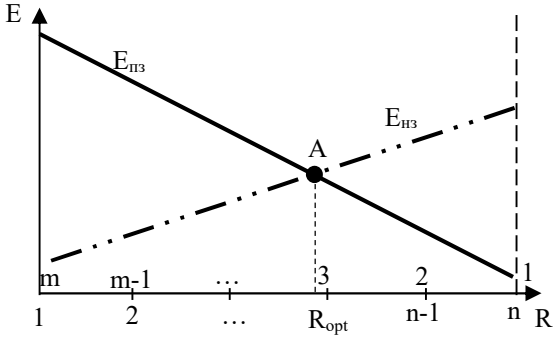


Рисунок 1 – Залежність ефективності ППО від виділеного вогневим засобам ресурсу

Тобто ресурс (призначений простір, час) поділено на однакові частини, починаючи з 1 (оскільки з нульовим ресурсом вираз (1) не має ані математичного, ані логічного розв'язання), для наземних засобів пронумерованих під горизонтальною віссю (від 1 до *n* ВО), а для повітряних – над нею (від 1 до *m* ВО). Ефективність кожної складової $E_{нз}$, $E_{пз}$ в одиниці ресурсу може приймати різне значення, що відображається нахилом відповідної лінії на графіку. Тоді в певній точці (А) буде спостерігатися оптимальне співвідношення виділених (призначених) для кожної складової ресурсів.

На практиці ефективності застосування вогневих засобів на одиницю ресурсу навряд чи будуть мати лінійну залежність, ураховуючи, що кількість знищених цілей $N_ц$ має випадковий характер і її доречно замінити на математичне очікування кількості знищених цілей $M_ц$.

Крім того, розподіл ресурсу, що відповідає точці А, не завжди можна реалізувати на практиці, оскільки складові системи ППО мають різні бойові можливості. Це буде впливати на їх часові та просторові показники, відповідно кількість частин ресурсу для цих складових буде відрізнятись ($n \neq m$), тому доцільно розглядати не точне значення оптимального розподілу ресурсу R_{opt} для точки А, а певну область ΔR_{opt}, в межах якої можна здійснити оптимальний розподіл ресурсу без суттєвого впливу на сукупну ефективність ППО (рис. 2).

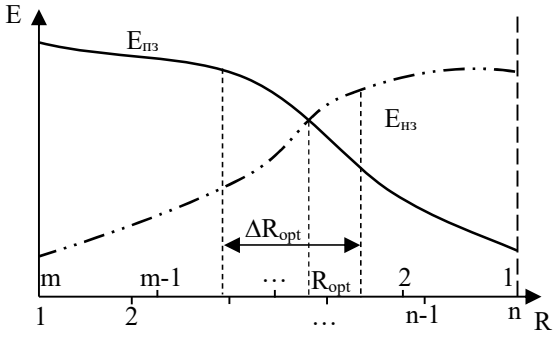


Рисунок 2 – Визначення оптимальної області розподілу ресурсу

Але не варто забувати про взаємний вплив наземних та повітряних засобів один на одного у процесі спільних дій в одній зоні, який може виражатися у взаємних обмеженнях, а у випадку недостатньо якісної організації – в небезпеці «дружнього вогню». Отже, потрібно прагнути такої рівноваги в розподілі ресурсу, після досягнення якої учасникам ППО буде невигідно (і небезпечно) перевищувати свою виділену частку ресурсу. За таких умов припускається, що кожен учасник дотримуватиметься (принаймні, до наступного керівного впливу) визначеної стратегії, що призводить до доцільності застосування критерію рівноваги Неша [10]. Одночасно, необхідність оптимізації в певній області рішень указує на потребу визначити величину цієї області.

Отже, величина оптимальної області розподілу ресурсу буде залежати від просторових, часових бойових можливостей вогневих засобів ППО. Також, у процесі її визначення доцільно враховувати ймовірні витрати (втрати) озброєння та боєприпасів під час бойових дій, що може призвести до тимчасового виходу з ладу окремих вогневих засобів. Тому, у випадку розподілу простору між *n* наземними засобами і *m* повітряними засобами протиповітряної оборони

$$\Delta R_{opt} = \Delta V_{opt} = f\left(V_{нз\,i}, V_{пз\,j}, M_{нз}^{втр}, M_{пз}^{втр}\right), \quad (4)$$

а для розподілу часу:

$$\Delta R_{opt} = \Delta T_{opt} = f\left(T_{цу\,нз\,i}, T_{цу\,пз\,j}, M_{нз}^{втр}, M_{пз}^{втр}\right), \quad (5)$$

де $V_{нз\,i}$ – об'єм простору, в якому діє і-й наземний вогневий засіб ($i = \overline{1,n}$). Цей об'єм є зоною ураження наземного вогневого засобу;

$V_{пз\,j}$ – об'єм простору, в якому діє j-й повітряний вогневий засіб ($j = \overline{1,\ m}$);

$T_{цу\,нз\,i}$ – середній цикл управління і-м наземним вогневим засобом;

$T_{цу\,пз\,j}$ – середній цикл управління j-м повітряним вогневим засобом;

$M_{нз}^{втр}$ – математичне очікування втрат (виходу з ладу, витрат) наземних вогневих засобів ($M_{нз}^{втр} \in \mathbb{N}^0$);

$M_{пз}^{втр}$ – математичне очікування втрат (виходу з ладу, витрат) повітряних вогневих засобів ($M_{пз}^{втр} \in \mathbb{N}^0$).

Для випадку розподілу простору (об'єму) між складовими ППО справедливим є вираз (6):

$$\Delta V_{opt} = \begin{cases} \max\left(\sum\limits_{i=1}^{M_{нз}^{втр}} V_{нз\,i}; \sum\limits_{j=1}^{M_{пз}^{втр}} V_{пз\,j}\right) \text{ при } M^{втр} > 0 \\ \max\left(V_{нз\,i}; V_{пз\,j}\right) \text{ при } M^{втр} = 0 \end{cases}. \quad (6)$$

Для розподілу часу – вираз (7):

$$\Delta T_{opt} = \begin{cases} \max\left(M_{нз\,i}^{втр} \cdot T_{цу\,нз\,i}; M_{пз\,j}^{втр} \cdot T_{цу\,пз\,j}\right) \text{ при } M^{втр} > 0 \\ \max\left(T_{цу\,нз\,i}; T_{цу\,пз\,j}\right) \text{ при } M^{втр} = 0 \end{cases} \quad (7)$$

Вирази (6) і (7) мають сенс за умов потрапляння в область оптимального розподілу ресурсу цілої кількості вогневих засобів (наземних і повітряних). Використання ресурсу кожним учасником ППО можна характеризувати коефіцієнтом раціонального використання призначеного ресурсу, а саме:

$\gamma_{нз\,i}$ – для наземних вогневих засобів;

$\gamma_{пз\,j}$ – для повітряних вогневих засобів ($\gamma = \overline{0,1}$),

а кожному підрозділу виділяється кількість ресурсу $r_{нз\,i}$ та $r_{пз\,j}$ відповідно. Тоді вираз (3) буде мати вигляд:

$$E_{ППО} = \sum_{i=1}^{n} E_{нзi}(r_{нз\,i}, \gamma_{нз\,i}) + \sum_{j=1}^{m} E_{нз\,j}(r_{нз\,j}, \gamma_{нз\,j}) \quad (8)$$

Водночас потрібно дотримуватись умови повного використання ресурсу:

$$\sum_{i=1}^{n} \gamma_{нз\,i} \cdot r_{нз\,i} + \sum_{j=1}^{m} \gamma_{нз\,j} \cdot r_{нз\,j} = R \quad (9)$$

Спираючись на раціональність використання ресурсу вогневим засобом, під час розподілу ресурсу для кожного учасника ППО доцільно встановити пріоритет ε_k ($\varepsilon_k = \overline{0,1}$), згідно з яким можна ранжирувати всіх учасників, зокрема побудувати чергу за цією ознакою: чим вище пріоритет, тим більше ресурсу отримає вогневий засіб. У найпростішому випадку пріоритет ε_k буде визначатися як нормована величина потрібного ресурсу для k-го вогневого засобу ППО ($k = \overline{1,(n+m)}$):

$$\varepsilon_k = \frac{\gamma_{нз\,k} \cdot r_{нз\,k}}{\sum\limits_{i=1}^{n} \gamma_{нз\,i} \cdot r_{нз\,i} + \sum\limits_{j=1}^{m} \gamma_{нз\,j} \cdot r_{нз\,j}} = \frac{\gamma_{нз\,k} \cdot r_{нз\,k}}{R} \quad (10)$$

або окремо для і-го (наземного) і j-го (повітряного) засобів:

$$\varepsilon_i = \frac{\gamma_{нз\,i} \cdot r_{нз\,i}}{\sum\limits_{i=1}^{n} \gamma_{нз\,i} \cdot r_{нз\,i}}; \ \varepsilon_j = \frac{\gamma_{нз\,j} \cdot r_{нз\,j}}{\sum\limits_{j=1}^{m} \gamma_{нз\,j} \cdot r_{нз\,j}} \quad (11)$$

З урахуванням пріоритету розподілу, середній ресурс, призначений k-му засобу ППО, $\overline{r_k}$, можна визначити за виразом:

$$\overline{r_k} = \min[r_k; \varepsilon_k R] \quad (12)$$

У випадку, коли сукупний ресурс, використаний учасниками ППО, менше встановленого (R), є небезпека не тільки зменшення ефективності виконання спільного завдання, але й недосягнення мети бойових дій у цілому, по причині того, що повітряний противник може скористатися наявними прогалинами в просторі або часі, подолати систему ППО і виконати свої завдання. Перебільшення призначеного кожній складовій системи ППО ресурсу може призвести до зниження ефективності через необхідність заборони дій вогневих засобів угруповання-партнера в просторі (часі), який перебільшується, або до знищення дружніх засобів ППО. Отже, обидва випадки відхилення від призначеного ресурсу супроводжуються певними усередненими ризиками $\overline{\delta}$ ($\overline{\delta} = \overline{0{,}1}$). В умовах динамічних змін обстановки, вказані ризики будуть існувати та впливати на ефективність спільних дій таким чином:

$$E_{ППО} = \sum_{i=1}^{n}(1-\overline{\delta_{нз}})E_{нзi} + \sum_{j=1}^{m}(1-\overline{\delta_{пз}})E_{пз\,j} \quad (13)$$

де $\overline{\delta_{нз}}$ – усереднений ризик, викликаний відхиленням від використання ресурсу наземними засобами;

$\overline{\delta_{пз}}$ – усереднений ризик, викликаний відхиленням від використання ресурсу повітряними засобами.

Визначення зазначених ризиків підлягає окремому дослідженню, як і доцільність їх усереднення або потреби враховування ризику для кожного вогневого засобу окремо. У процесі вивчення вказаного питання, також необхідно враховувати наявну статистику виконання спільних завдань наземними та повітряними засобами ППО під час російсько-української війни.

Як видно з виразу (13), ефективність учасників ППО знижується пропорційно до наявних ризиків відхилення від зазначеного обсягу ресурсів. Отже, пріоритет окремого *k*-го вогневого засобу ППО, в цьому випадку, буде залежати від зменшеної, залежно від ризику, ефективності його дій:

$$\varepsilon_k = \frac{(1-\delta_k E_k)\gamma_{нз\,k}\cdot r_{нз\,k}}{\sum_{i=1}^{n}(1-\overline{\delta_{нз}}E_{нз\,i})\gamma_{нз\,i}\cdot r_{нз\,i} + \sum_{j=1}^{m}(1-\overline{\delta_{пз}}E_{пз\,j})\gamma_{нз\,j}\cdot r_{нз\,j}}. \quad (14)$$

В такому випадку вираз (12) прийме вигляд:

$$\overline{r_k} = \min[r_k; \varepsilon_k R] = \min\left[r_k; R\frac{(1-\delta_k E_k)\gamma_{нз\,k}\cdot r_{нз\,k}}{\sum_{i=1}^{n}(1-\overline{\delta_{нз}}E_{нз\,i})\gamma_{нз\,i}\cdot r_{нз\,i} + \sum_{j=1}^{m}(1-\overline{\delta_{пз}}E_{пз\,j})\gamma_{нз\,j}\cdot r_{нз\,j}}\right]. \quad (15)$$

Враховуючи зазначене, методику визначення оптимальної кількості наземних і повітряних вогневих засобів, за виконання спільних завдань, доцільно реалізувати за алгоритмом, що наведений на рис. 3.

Методика реалізується за таким порядком:

1. Під час планування та перед початком бойових дій формуються вихідні дані (блок 1), що включатимуть склад та характеристики сил та засобів, залучених до ведення ППО. Також оцінюються геометричні параметри прогнозованої зони бойових дій, імовірний склад і тривалість ударів повітряного противника. З огляду на отримані дані, визначається раціональність використання простору та часу кожним типом залучених засобів, а в ідеальному випадку – кожним вогневим засобом окремо, зважаючи на його бойову готовність, забезпеченість засобами ураження, іншими матеріально-технічними засобами, підготовкою особового складу обслуги тощо. Зазначені дані, за необхідності, періодично уточняються (блок 2).

2. Шляхом послідовного перебору від 1 до n наземних та від m до 1 повітряних вогневих засобів за виразом (13) визначається $\max(E_{ППО})$ (блоки 3-6 методики). Фіксуються значення n наземних та m повітряних вогневих засобів для максимальної ефективності, які будуть брати участь в бойових діях. Ці ж значення n та m беруться для подальших розрахунків і розподілу ресурсів.

3. За виразом (14) визначається середній ресурс на один вогневий засіб $\overline{r_k}$ (окремо $\overline{r_i}$ для наземних та $\overline{r_j}$ для повітряних вогневих засобів), блоки 7–8 методики.

4. За виразами (6) або (7), залежно від типу ресурсу, що розподіляється, в блоці 9 знаходиться оптимальна область розподілу ресурсу ΔR_{opt}, в межах якої уточняється кількість наземних і повітряних вогневих засобів.

5. Визначаються ризики $\overline{\delta_{нз}}$, $\overline{\delta_{пз}}$ (за окремими методиками), блок 10.

6. За можливості, з метою підтримання

визначеного рівня ефективності в блоці 11,наст визначається розмір резерву наземних та повітряних вогневих засобів залежно від ризиків:

$$n_{рез} = ent\left(M_{нз}^{втр} + n \cdot \overline{\delta_{нз}}\right) \quad (16)$$

для наземних вогневих засобів, та

$$m_{рез} = ent\left(M_{пз}^{втр} + m \cdot \overline{\delta_{пз}}\right) \quad (17)$$

для повітряних вогневих засобів.

7. Протягом бойових дій, вказані вище показники будуть змінюватися залежно від втрат, зміни ступеню бойової готовності вогневих засобів тощо (блоки 2, 12, 13). Тому необхідно їх періодично (до закінчення удару чи бойових дій, $T_{бд}$) уточнювати залежно від досягнутих результатів, змін обстановки та необхідності розширення (зменшення) просторових характеристик або часу ведення бою.

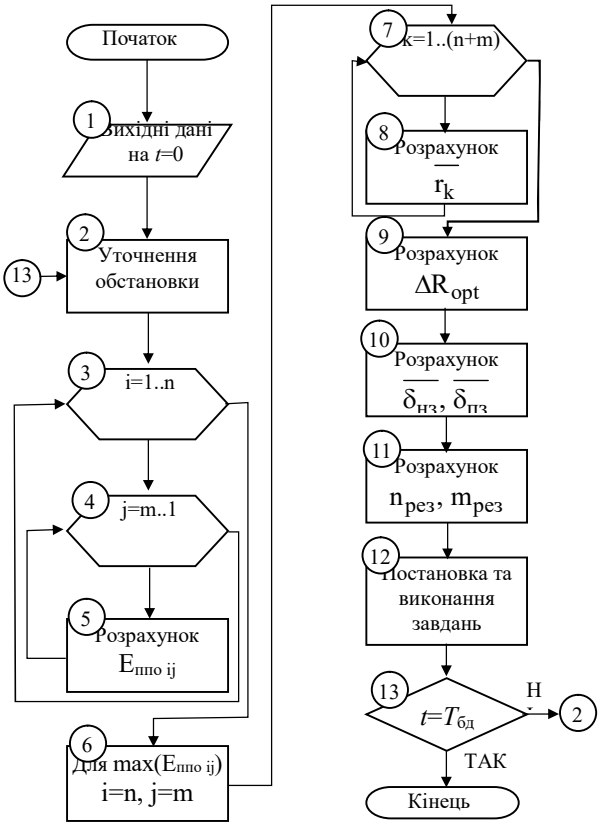


Рисунок 3 – Блок-схема реалізації методики визначення кількості наземних та повітряних вогневих засобів

Для оцінювання результатів, отриманих за методикою, проведено ряд розрахунків для умовної зони бойових дій, в якій знаходяться один тип наземних та один тип повітряних ВО, які відрізняються раціональністю використання виділеного їм ресурсу залежно від підготовленості обслуг (екіпажів), наявності засобів ураження, боєздатності техніки тощо (табл. 1), де НВО – наземна вогнева одиниця, ПВО – повітряна вогнева одиниця.

Для проведення розрахунків прийнято такі обмеження:

тривалість удару повітряного противника – до 60 хвилин;

кількість засобів повітряного нападу, що беруть участь в ударі – до 40;

площа зони бойових дій – до 6000 км^2;

всі засоби повітряного нападу противника виконують завдання на малих висотах без завад та можуть бути обстріляні наземними і повітряними вогневими засобами;

втрати можуть становити до однієї наземної ВО ($M_{нз}^{втр} = 1; M_{пз}^{втр} = 0$);

ресурс за часом для повітряних ВО обмежується часом вильоту та прийнятий 30 хв без урахування зльоту, посадки та часу виходу в зону бойових дій;

ресурс за часом для наземних ВО обмежується часом роботи від автономних засобів живлення та прийнятий 100 хв без урахування часу розгортання.

Таблиця 1

Вихідні дані для розрахунків

Номер ВО	Дальня межа зони ураження, км	Коефіцієнт раціонального використання часу	Коефіцієнт раціонального використання простору
НВО1	18	0,3	0,6
НВО2	18	0,3	0,6
НВО3	18	0,25	0,5
НВО4	18	0,25	0,5
НВО5	18	0,3	0,6
НВО6	18	0,2	0,4
ПВО1	40	0,25	0,05
ПВО2	40	0,2	0,04
ПВО3	40	0,3	0,03
ПВО4	40	0,2	0,4

На етапі визначення максимальної кількості залучених наземних та повітряних засобів ППО логічно пропонується залучити всі наявні ВО. Проте у випадку виконання спільних завдань під час розподілу зусиль за простором майже однакову ефективність показують випадки залучення 3 і 4 повітряних ВО, а також від 3 до 6 наземних ВО (рис. 4).

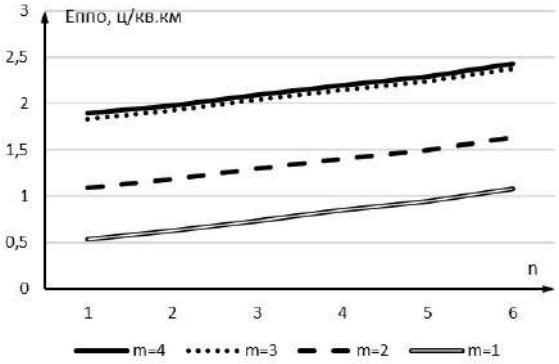


Рисунок 4 – Залежність Еппо від кількості наземних та повітряних засобів ППО під час розподілу зусиль за простором

Під час розподілу зусиль за часом доцільно залучити всі 4 повітряні та від 5 до 6 наземних засобів ППО (рис. 5).

Під час визначення середнього ресурсу на один вогневий засіб у процесі розподілу зусиль за простором отримуються наступні значення:

$\overline{r_{нз}} = 9{,}6\,км^2$; $\overline{r_{пз}} = 5{,}2\,км^2$.

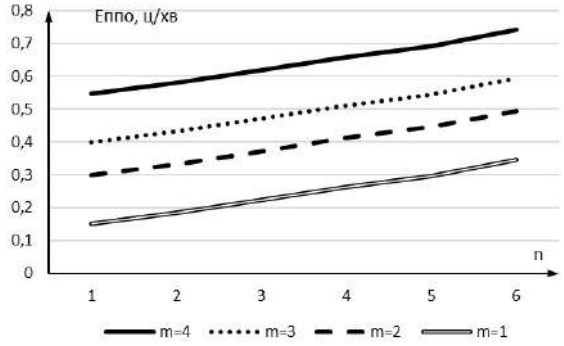


Рисунок 5 – Залежність Еппо від кількості наземних та повітряних засобів ППО під час розподілу зусиль за часом

В свою чергу, у процесі розподілу зусиль за часом середній ресурс на вогневу одиницю, відповідно, становитиме:

$\overline{r_{нз}} = 27$ хв; $\overline{r_{пз}} = 7$ хв.

З урахуванням можливих втрат область раціонального розподілу ресурсу складатиме (для простору та часу відповідно):

$\Delta V_{opt} = 9{,}6\,км^2$; $\Delta T_{opt} = 1{,}5$ хв.

За умови прийняття середнього ризику втрат від «дружнього вогню» $\overline{\delta_{нз}} = 0$, $\overline{\delta_{пз}} = 0{,}12$ на етапі визначення резерву ВО отримуються такі значення:

$n_{рез} = 1$; $m_{рез} = 0$,

які в цілому не суперечать даним, отриманим на етапі визначення кількості залучених засобів ППО.

Застосування наведеної методики може надати виграш в ефективності ППО у спільних діях наземних та повітряних ВО у розмірі від 5% до 10% у процесі розподілу зусиль між ними за часом, та від 6 до 15% під час розподілу зусиль за простором.

Висновки й перспективи подальших досліджень

Отже, одним з основних завдань, що стоїть перед особою, яка приймає рішення на спільні дії наземних і повітряних засобів протиповітряної оборони, є розподіл зусиль між ними, а також постійне коригування прийнятого рішення в умовах динамічних змін повітряної обстановки. Для ефективного вирішення цього завдання є розгляд часу та простору як ресурсів, які потрібно розподілити між наземними та повітряними засобами протиповітряної оборони, враховуючи раціональність їх використання.

У статті розроблено методику динамічного розподілу наявних ресурсів між наземними та повітряними вогневими засобами протиповітряної оборони під час їх спільних дій і, як наслідок, потрібної для виконання завдань кількості наземних і повітряних вогневих засобів. Також, обґрунтований спосіб визначення оптимальної області розподілу ресурсу в процесі визначення потрібної кількості засобів.

Запропонована методика, на відміну від існуючих, враховує показники середнього ресурсу на один вогневий засіб, раціональності його використання та ризиків, викликаних відхиленням від призначеного вогневим засобам обсягу ресурсу. Методика може бути застосована в алгоритмах систем підтримки прийняття рішень під час визначення варіантів розподілу зусиль між наземними та повітряними вогневими засобами протиповітряної оборони.

Список бібліографічних посилань

1. Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В. Т. Бусел. Київ; Ірпінь: Перун, 2005. VIII. 1728 с. **2. Cambridge** Dictionary. URL : https://dictionary.cambridge.org/dictionary/english/resource (date of access: 01.07.2023). **3. Гузченко С., Поплавець С., Гатченко Є., Явтушенко В., Козлов Д., Дроль О.** Визначення розподілу різнорідних засобів протиповітряної оборони по враженню повітряних цілей. *Scientific Collection «InterConf»*. № 145. С. 430–438. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/2641 (date of access: 01.07.2023). **4. Рєзнік Д. В.** Можливість використання моделі узгодженої взаємодії для оцінки ефективності взаємодії військ. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2014. № 2(20). С. 88–92. **5. Rieznik D., Levchenko M., Patalakha V., Melnichenko V., Kitik S., Shkurat B.** Method of the Effort Coordination Chart Creation. *International Journal of Advanced Trends in Computer Science and Engineering.* 2020. № 5. P. 7610-7617. URL: https://doi.org/10.30534/ijatcse/2020/100952020 (date of access: 01.07.2023). **6. Rieznik D., Levchenko M., Patalakha V., Kitik S., Shkurat B., Globa O.** Using a Model of Coordinated Interaction for Estimation of Troops Joint Missions Effectiveness. *Short Paper Proceedings of the 2nd International Conference on Intellectual Systems and Information Technologies co-located with 1st International Forum «Digital Reality».* 2021. P. 233–237. **7. Гринченко М. А., Чернишова М. О.** Технологія розподілу ресурсів у проєкті між виконавцями. *Відкриті інформаційні та комп'ютерні інтегровані технології.* 2013. № 58. С. 155-166. **8. Гриша О. В.** Динамічний розподіл ресурсів проєкту на основі оптимізації змішаної стратегії. *Адаптивні системи автоматичного управління.* 2006. №9(29). С. 50–54. **9. ДСТУ** ISO 9000:2015. Системи управління якістю. Основні положення та словник термінів. Київ :ДП «УкрНДНЦ», 2016. 49 с. **10. Барановська Л. В.** Теорія ігор. курс лекцій : Навчальний посібник. Київ : КПІ, 2022. 245 с.

THE METHODOLOGY OF DYNAMIC RESOURCE ALLOCATION FOR JOINT ACTIONS OF GROUND-BASED AND AIR-BASED AIR DEFENSE MEANS

Shkurat Bohdan

National Defence University of Ukraine, Kyiv, Ukraine

As the experience of the russian-Ukrainian war and recent armed conflicts in the world shows, air defense plays the significant role during hostilities. Usually, the air defense system includes both ground-based and air-based fire means, the joint actions of which allow to ensure the required level of effectiveness of its functioning. But poor organization of joint actions can not only reduce their effectiveness, but also lead to conflict situations and such dangerous phenomena as "friendly fire". Existing studies on the peculiarities of the implementation of joint projects by performers in conditions of uncertainty cannot be directly applied to the planning and conduct of combat operations with different fire means, especially in such dynamic situation changes, by which the air defense is accompanied. Thus, the task of resolving the conflict of interests of the air defense system fire components arises. One of the ways to solve this task is the rational resources allocation between fire means. In the article the methodology developed for determining the optimal amount of resources that should be allocated to ground and air fire components of air defense when they perform joint tasks in the dynamics of hostilities, and hence the necessary number of ground and air fire means. The resource definition is understood as time and (or) space, which characterize the boundaries of task performance. The methodology applies the methods of decision-making theory, game theory, project management, and comprehensively takes into account not only the average resource in which one fire mean is able to perform the task, but also considers indicators of the rationality of its resource use and risks caused by deviation from the amount of resource assigned to it. On the basis of the specified indicators, priorities are formed during distribution, which will determine the share of tasks allocated to a separate fire mean, and hence to the ground and air components of the air defense system. In addition, a method of determining the area of optimal allocation of the resource when calculating the required number of fire means is proposed in order to take into account possible deviations when determining the shares of ground and air-based means participation in the task. In the technique proposed the subjects for further discussing are: the methods of determining the loss of fire means, including those caused due to the risks of deviation from the designated resource, as well as the procedure for determining the rationality of the time or space using by fire means. The methodology developed can be applied in the algorithms of decision-making support systems, in particular, when determining options for the efforts distribution between ground-based and air-based air defense means during their joint actions.

Key words: *air defense, fire means, anti-aircraft missile forces, fighter aircraft, joint actions, interaction, distribution of resources, conflict of interests.*

References

1. Busel, V.T., (2005). A large explanatory dictionary of the modern Ukrainian language. Kyiv, Irpen: Perun, T. VIII, 1728. **2.** Cambridge Dictionary [online]. Available at: https://dictionary.cambridge.org/dictionary/english/resource [Accessed : 01 July 2023]. **3. Huzchenko, S.,** Poplavets, S., Hatchenko, Ye., Yavtushenko, V., Kozlov, D., Drol, O., (2023). Determination of the distribution of heterogeneous means of anti-aircraft defense against air targets. *Scientific Collection «InterConf»*, (145), 430–438 [online]. Available at: https://archive.interconf.center/index.php/conference-proceeding/article/view/2641 [Accessed : 01 July 2023]. **4. Rieznik, D. V.,** (2014). Possibility of using coordinated interaction model for evaluation of troops interaction efficiency. *Modern Information Technologies in the Sphere of Security and Defence.* 2(20), 88-92. **5. Rieznik, D.,** Levchenko, M., Patalakha, V., Melnichenko, V., Kitik, S., Shkurat, B., (2020). Method of the Effort Coordination Chart Creation. *International Journal of Advanced Trends in Computer Science and Engineering,* 5, 7610-7617. doi.org/10.30534/ijatcse/2020/100952020 [Accessed : 01 July 2023]. **6. Rieznik, D.,** Levchenko, M., Patalakha, V., Kitik, S., Shkurat, B., Globa, H., (2021). Using a Model of Coordinated Interaction for Estimation of Troops Joint Missions Effectiveness. *Short Paper Proceedings of the 2nd International Conference on Intellectual Systems and Information Technologies co-located with 1st International Forum «Digital Reality»,* 233-237. **7. Hrynchenko, M.A.,** Chernyshova M.O., (2013). Technology of distribution of resources in the project between performers. *Open information and computer integrated technologies,* 58, 155-166. **8. Hrysha, O. V**., (2006). Dynamic allocation of project resources based on mixed strategy optimization. *Adaptive automatic control systems*, 9(29), 50-54. **9.** Derzhspozhyvstandart Ukrainy, (2015). *Quality management systems. Basic provisions and glossary of terms*. DSTU ISO 9000:2015. Kyiv: Vyd. ofits. 49. **10. Baranovska, L. V.,** (2022). Game theory. course of lectures: Study guide. Kyiv : KPI, 245.

DOI:**10.33099/2311-7249/2023-47-2-155-166**

УДК: 358.1

Репіло Юрій Євгенович *(доктор військових наук, професор)*
Приміренко Володимир Миколайович *(кандидат військових наук)*
Дем'янюк Андрій Володимирович

Національний університет оборони України, Київ, Україна

МЕТОДИКА ВИЗНАЧЕННЯ ПРІОРИТЕТНОСТІ ОБ'ЄКТІВ ПРОТИВНИКА ДЛЯ ПРИЙНЯТТЯ ЇХ ЯК МОЖЛИВИХ ЦІЛЕЙ З МЕТОЮ ВОГНЕВОЇ ПІДТРИМКИ З ВИКОРИСТАННЯМ МАТРИЦІ CARVER

Відомо, що під час вогневої підтримки засобів ураження і ресурсів завжди менше ніж потрібно для враження усіх виявлених об'єктів противника. Виходячи з цього, визначення пріоритетності об'єктів противника, які в подальшому можуть ідентифікуватися як цілі для ураження, щоб забезпечити ефективне використання обмежених ресурсів, є актуальним науковим завданням. У статті наведено розроблену методику визначення пріоритетності об'єктів противника для прийняття їх як можливих цілей з метою вогневої підтримки з використанням матриці CARVER. Суть методики полягає в аналізі об'єктів противника з урахуванням їх потенційного впливу на виконання завдань з ураження їх засобами артилерії. На відміну від існуючих, у розробленій методиці передбачено оцінювання об'єктів противника на основі багатьох критеріїв, що забезпечує ефективне використання обмежених ресурсів. Це дає змогу ідентифікувати об'єкти як важливі цілі для подальшого прийняття обґрунтованих рішень щодо пріоритетності їх ураження. Використання запропонованої методики визначення пріоритетності об'єктів противника для прийняття їх як можливих цілей з метою вогневої підтримки з використанням матриці CARVER через визначення пріоритетів цілей, на основі таких факторів як критичність, доступність, здатність до відновлення, вразливість, ефект і впізнаваність, на практиці дає змогу забезпечити використання обмежених ресурсів для досягнення цілей по всіх ланках військового управління. Під час написання статті застосовано методи експертних оцінок, аналізу ієрархій та теорії важливості критеріїв. Зазначений методологічний підхід в подальшому планується як складова методики підтримки прийняття рішення бойового застосування артилерії на основі застосування геоінформаційних технологій та штучного інтелекту. Означене, в свою чергу, дає змогу підвищити ефективність бойового застосування артилерії, завдяки скороченню часу на прийняття рішення бойового застосування артилерії під час вогневої підтримки загальновійськових формувань та забезпеченню використання обмежених ресурсів з метою досягнення цілей у всіх ланках військового управління.

Ключові слова: *пріоритетність, об'єкти противника, матриця CARVER, вогнева підтримка, ранг важливості, критичність, доступність, здатність до відновлення, вразливість, ефект і впізнаваність.*

Вступ

Під час планування вогневої підтримки (далі – ВгП) в збройних конфліктах вкрай важливим є визначення пріоритетності об'єктів ураження противника з метою найшвидшого зниження бойового потенціалу його угруповання в цілому та нанесення максимально можливих втрат в найкоротший проміжок часу. Актуальність зазначеного завдання, по-перше, пов'язане з наявністю значної кількості особливостей, що впливають на показники ефективності ураження цілей під час вогневого впливу на противника, починаючи з достовірності розвіданого об'єкту враження і до показника критичності цього об'єкта для виконання операції в цілому з можливими відмінностями їх функціонального призначення, а по-друге, з обмеженим ресурсом ракетних військ і артилерії, що виділяються для їх ураження. В таких умовах, важливість пріоритетності враження цілей противника (лат. *prior* «перший, старший» – поняття, що свідчить про черговість виконання дій (операцій) визначеними дійовими особами або засобами та визначає порядок їх виконання в часовому просторі) постає найважливішим фактором правильного вибору об'єктів ураження противника та розподілу їх між засобами враження, що і обумовлює *актуальність* цієї статті.

Постановка проблеми. Проблема, яка розглядається в цій статті, потребує системного та об'єктивного методу визначення пріоритетності об'єктів противника як можливих цілей для подальшого враження під час вогневої підтримки бойових дій. Традиційний метод встановлення

пріоритетів цілей часто спирається на суб'єктивні оцінки [9; 14–16], що призводить до неоптимального розподілу обмежених ресурсів і потенційно ставить під загрозу досягнення мети операції. Тому, існує потреба в розробленні метода, який би враховував численні критерії, такі як важливість цілі, ризик побічної шкоди та потенційний вплив на загальну місію. Такий метод має гарантувати, що найважливіші цілі матимуть відповідний пріоритет у процесі прийняття рішень. Для цього пропонується використовувати матрицю CARVER як інструмент прийняття рішень. Цей підхід дає змогу збалансувати важливість різних критеріїв та враховувати їх вплив на виконання місії, сприяючи оптимальному використанню ресурсів під час бойових дій.

За досвідом російсько-українського збройного конфлікту [1; 19] кінцеве оцінювання пріоритетності враження цілей проводиться на основі значення бойових потенціалів об'єктів противника або за коефіцієнтами їх важливості, який визначається за кількома методами, але не завжди містить особливості різних факторів, що впливають на пріоритетність ураження об'єктів у загальній системі угруповання противника.

Аналіз останніх досліджень і публікацій. Результати проведених попередніх досліджень [1–9] показують, що на цей час у теорії та практиці управління артилерією в аспекті її застосування в сучасних умовах та на перспективу до 2030 року виникла невідповідність між зростанням кількості об'єктів противника з одного боку та можливістю прийняття їх як можливих цілей для подальшого їх ураження в ході вогневої підтримки. Як свідчить досвід російсько-української війни [1; 19], сьогодні відсутнє єдине розуміння процесу визначення пріоритетності об'єктів противника, як можливих цілей для подальшого їх ураження, особливо під час планування вогневої підтримки артилерією загальновійськових підрозділів на початковому етапі операції.

Це надає можливість стверджувати, що на сьогодні існує ряд підходів до оцінювання пріоритетності об'єктів противника та визначення коефіцієнтів їх цінності або важливості. Дані дослідження запропоновували структуру для встановлення пріоритетів цілей, яка використовувала методи аналітичного ієрархічного процесу [2–3, 8–9] і метод визначення переваги порядку за подібністю до ідеального рішення [6]. Інший метод Делфі (Delphi) був ефективним у створенні пріоритетного списку цілей, що підкреслило необхідність чіткого керівництва та загального розуміння критеріїв, які використовуються для визначення пріоритетів [7].

Дослідження [6–10; 13–17] підкреслюють необхідність загального розуміння критеріїв, що використовуються для встановлення пріоритетів, і ефективного використання багатьох методів для досягнення пріоритетного списку цілей.

Отже, систематизація та об'єктивне оцінювання об'єктів противника на основі багатьох критеріїв, що дають змогу ефективно використовувати обмежені ресурси в сучасних військових операціях, а також висвітлення переваг використання матриці CARVER [18] для встановлення пріоритетів цілей є важливим науковим завданням.

Метою статті є розроблення методики для визначення пріоритету об'єктів противника як потенційних цілей з метою подальшого ураження у процесі вогневої підтримки, з використанням матриці CARVER та методу експертного оцінювання критичних уразливостей цих об'єктів. У межах розробленої методики, пропонується застосовувати систематизований та об'єктивний спосіб оцінювання об'єктів противника на основі визначених критеріїв, що сприятиме ефективному використанню обмежених ресурсів у сучасних військових операціях. Крім того, метою статті є висвітлення переваг використання матриці CARVER для встановлення пріоритетів цілей.

Виклад основного матеріалу дослідження

Під час прийняття рішення щодо вибору найкращого засобу та способу досягнення визначеної мети виникає проблема оцінювання їх за кількома факторами з відповідними критеріями, що визначають бажаність у визначеному інтервалі значень (наприклад, від 1 до 10). Під час аналізу об'єкта враження для прийняття рішення стосовно визначення його ціллю, пропонується окреслити фактори, які будуть впливати на пріоритетність ураження вибраних цілей елементами розвідувально-вогневої системи в оборонній операції. Для прикладу взято фактори матриці CARVER (від англ. Criticality – Критичність, Accessibility – Доступність, Recuperability – Відновлюваність, Vulnerability – Вразливість, Effect – Ефект, Recognizability – Впізнаваність), що була розроблена військами спеціального призначення США під час війни у В'єтнамі [10].

У статті розглянуто елементи матриці CARVER з критеріями необхідними для визначення важливості об'єкта ураження елементами РВС в операції. Першим ключовим елементом, для визначення пріоритетності ураження цілі є їх *критичність* для оцінювання об'єктів противника (далі – ОП), як можливих цілей для подальшого ураження. ОП є критичним, якщо його знищення або пошкодження має значний вплив на військові, політичні чи економічні фактори операції [11; 15–16].

Всі об'єкти враження в системі варто розглянути зважаючи на взаємозв'язок з іншими елементами цільової системи. Цінність ОП буде змінюватися в міру розвитку ситуації, що вимагає використання чутливих до часу методів, які реагують на зміни ситуації. Наприклад, коли у вас мало залізничних ешелонів, залізничні мости

можуть бути менш критичними як цілі. Однак захист мостів може мати вирішальне значення для маневрування звичайними силами або підвезення боєприпасів для артилерії, які потребують використання таких мостів. Як свідчать дані [2–9], критичність залежить від кількох чинників:

Час: як швидко результат обстрілу ОП вплине на хід операції?

Якість: який відсоток угруповання військ противника або його об'єктів тилу та інфраструктури буде скорочено через завдання успішного вогневого впливу по зазначеній цілі (об'єкту ураження)?

Ефективність: як це вплине на вирішення поставленого завдання операції?

Теорія відносності: скільки є цілей? Які їхні позиції? Як визначається їх відносна вартість? Що буде відбуватися в системі або комплексному «потоці»?

Виходячи з цього, пропонується здійснити ранжування критеріїв за якими приймається рішення щодо прийняття цілі до ураження. Так, у таблиці 1 наведено ранжування критеріїв критичності об'єктів противника.

Таблиця 1

Ранжування критеріїв критичності об'єктів противника

Критерії критичності	Ранг важливості
Вирішальне значення для загального успіху операції.	10
Важливе значення для успіху поточних бойових дій.	9
Вчасні та переконливі наслідки для поточних бойових дій.	8
Істотно впливає на хід бойових дій.	7
Посередній внесок в бойові дії, не має вирішального значення для успіху.	6
Не застосування цілеспрямованих дій, може негативно ускладнити операцію.	5
Вимагає цілеспрямованості майбутніх планів.	4
Не здійснення вогневого впливу, при-зведе до залучення більшої кількості сил і засобів.	3
Ефект, який забезпечує об'єкт, може бути не реалізований в майбутньому.	2
Здебільшого не важливий, наслідки не перешкоджатимуть бойовим діям.	1

Як видно з даних табл.1, ранг важливості цілі (від 1 до 10) напряму залежить від ступеня її впливу на хід бойових дій. Тому, враховуючи, що результат вогневого впливу на противника з достатньою кількістю засобів та особового складу можливо досягти через доступність об'єкта, наступним елементом, для оцінювання об'єктів пропонується прийняти його *доступність*, який показує можливість елементу вогневої підтримки досягти успішного результату вогневого впливу на противника з достатньою кількістю засобів та особового складу [11; 15–16]. Це оцінювання передбачає визначення та вивчення критичних шляхів, які має пройти операційний елемент. У нашому випадку це засіб вогневої підтримки, необхідний для досягнення успішного впливу на противника. Також важливим аспектом є врахування чинників, що можуть перешкоджати або сприяти ефективному завданню ураження цілям.

Як видно з [10–17] існують чотири основні кроки визначення доступності, а саме можливість:

завдання враження об'єкта без прямої загрози з боку противника;

визначення результатів вогневого впливу;

завдання враження без пошкодження інфраструктури навколишнього середовища;

враження всього об'єкта, а не окремих його елементів.

Фактори, що враховуються під час оцінювання доступності, можуть включати, але ними не обмежуються:

активні та пасивні системи раннього попередження (засоби протиповітряної оборони, радіолокаційні станції наземної розвідки, контрбатарейні радари та ін.);

наявність елементів радіоелектронного подавлення (для використання високоточних боєприпасів);

тип місцевості та її використання;

система фортифікаційного обладнання;

приховування та прикриття окремих елементів цілі;

розташування об'єкта в населених пунктах, де неможливе застосування окремих засобів ураження;

інші природні або синтетичні перешкоди або бар'єри;

різкі зміни кліматичних погодних умов.

Доступність вимірюється з погляду відносної легкості або складності, які виникають під час реалізації комплексу заходів, спрямованих на ліквідацію цілі. Враховуючи це, рекомендується здійснити ранжування цих критеріїв, які в подальшому будуть враховуватися під час оцінки об'єктів ураження, що будуть прийматись як можливі цілі для вогневої підтримки. Так, у таблиці 2 наведено ранжування критеріїв доступності об'єктів противника.

Як видно табл. 2, ранг важливості цілі (від 1 до 10) виявляє прямопропорційну залежність від ступеня відкритості та спостережуваності даного

об'єкта, а також від складності місцевості, на якій він розташований. Враховуючи те, що на оцінювання об'єкта противника, який в подальшому може прийматись як ціль для вогневої підтримки буде впливати його можливість відновлення або своєчасна заміна, наступним елементом, для його оцінювання рекомендується прийняти його є *відновлюваність*, що вимірюється в часі [11; 15–16]. Тобто скільки часу знадобиться для заміни, ремонту або обходу руйнування чи пошкодження цілі? Можливість відновлення залежить від джерел і типу цільових компонентів, а також від наявності запасних частин. Фактори, що слід враховувати під час оцінювання реабілітації, включають, але не обмежуються, доступністю:

такого підручного обладнання, як залізничні крани, сухі доки та зняття справних деталей і агрегатів з пошкодженої техніки для ремонту пошкоджених зразків озброєння;

відновлення та заміщення через скорочення;

наявності запчастин;

еквівалентні комплекти ремонтного обладнання, що забезпечують резервне копіювання критичного обладнання чи компонентів, а також наслідків економічних ембарго та трудових заворушень.

Таблиця 2

Ранжування критеріїв доступності об'єктів противника

Критерії доступності	Ранг важливості
Стаціонарний, повністю доступний, відсутні системи раннього попередження системи раннього попередження, визначення результатів вогню.	10
Стаціонарний, доступний. Недостатність інформації про радіоелектронне подавлення, природні перешкоди відсутні.	9
Доступний, достовірно розвіданий, тип місцевості частково ускладнює доступ до об'єкту.	8
Доступний, окремі елемент за штучними перешкодами. Рельєф частково впливає на застосування окремих засобів ураження.	7
Частково доступний, окремі елементи фортифікаційно укриті. Необхідне залучення високоточних засобів ураження.	6
Частково доступний, можливе не достовірне уточнення структури об'єкту, є ймовірність систем раннього попередження або елементів радіоелектронного подавлення.	5
Частково доступний, є природні або штучні перешкоди, висока ймовірність систем раннього попередження або радіоелектронного подавлення, є ймовірність контрбатарейної боротьби з боку противника.	4
Складно-доступна, потребує значних сил і засобів, складна місцевість, окремі елементи приховані. Неможливо використати окремі засобів ураження.	3
Доступний з великими складнощами та витратою великого ресурсу сил і засобів. Об'єкт уражається лише певними видами засобів ураження.	2
Мінімальна доступність, достовірно розвідано системи раннього попередження (контрбатарейні радари), елементи об'єкта приховані або в населеному пункті.	1

Отже, враховуючи різну відновлюваність об'єкта ураження в часі, пропонується здійснити ранжування цих критеріїв, які в подальшому будуть враховуватись під час оцінювання об'єктів ураження. Так, у табл. 3 наведено ранжування критеріїв відновлюваності об'єктів противника.

З огляду на табл. 3, ранг важливості цілі (від 1 до 10) буде збільшуватися залежно від часу на який буде виведений з ладу даний об'єкт противника. Виходячи з даних таблиці, також виникає закономірна залежність чутливості визначеного об'єкта ураження до вогневого впливу, який завдають засоби ракетних військ і артилерії, однаковою кількістю засобів ураження. Тому для оцінювання пропонується прийняти його *вразливість*, що характеризується як нездатність витримувати вплив вогневих засобів противника та наявності значної кількості слабких місць одного або декількох елементів цілі (об'єкта ураження). Цей фактор показує на скільки об'єкт ураження чутливий до вогневого впливу засобів ракетних військ і артилерії, а також які наслідки можливо завдати однаковою кількістю боєприпасів (ракет) [11; 15–16].

Під час визначення вразливості цілі пропонується порівнювати масштаб критичного компонента з можливостями атакуючого елемента знищити або пошкодити його. Загалом, атакуючий елемент може мати тенденцію до:

вибору спеціальних компонент;

заподіяння постійної шкоди;

запобігання або припинення ефекту канібалізації (донорства окремих елементів для інших об'єктів);

максимізації ефектів за рахунок використання матеріалів на місці;

змушення цілі до самознищення.

Зокрема, вразливість залежить від:

характеру і конструкції цілі;

необхідної кількості пошкоджень;

наявних активів (наприклад, персонал, експертиза, мотивація, зброя, вибухові речовини та обладнання).

Враховуючи зазначене, пропонується здійснити ранжування критеріїв за якими випливає залежність заподіяної школи об'єкту ураження, що в майбутньому приймається до ураження. Так, у таблиці 4 наведено ранжування критеріїв вразливості об'єктів противника.

Таблиця 3

Ранжування критеріїв відновлюваності об'єктів противника

Критерії (для відновлення (заміни, ремонту або заміщення) потрібно	Ранг важливості
1 місяць або більше	10
2-3 тижні	9
до 2 тижнів	8
1 тиждень	7
5-6 днів	6
3-4 дні	5
до 72 год.	4
до 48 год.	3
в той самий день або наступний.	2
до 12 год.	1

Таблиця 4

Ранжування критеріїв вразливості об'єктів противника

Критерії вразливості	Ранг важливості
Об'єкт (основні окремі його елементи) будуть уражені уламками в ході вогневого впливу	10
Окремі елементи об'єкта є критичними, вразливі окремі елементи (відкрита жива сила)	9
Окремі елементи об'єкта критичні, об'єкт вразливий до окремих елементів.	8
Об'єкт вразливий для всіх засобів ураження, зокрема, артилерією загальної підтримки та всіх видів реактивних систем залпового вогню.	7
Об'єкт вразливий для більшої частини засобів ураження, зокрема артилерією та мінометами.	6
Об'єкт вразливий для окремих видів засобів ураження, зокрема, далекобійною артилерією та реактивними системами залпового вогню середньої та дальньої дії.	5
Об'єкт невразливий до окремих видів засобів ураження, потребує постійного вогневого впливу. Можливе залучення високоточних ЗУ.	4
Об'єкт невразливий до частини засобів ураження, але може бути заподіяна шкода потужним вогневим впливом сил і засобів.	3
Об'єкт невразливий до більшої частини засобів ураження, можливе ураження реактивними системами залпового вогню дальньої дії та частково силами і засобами артилерії загальної підтримки.	2
Об'єкт невразливий до всіх засобів ураження, окрім застосування тактичного ракетного комплексу та реактивних систем залпового вогню дальньої дії.	1

Як свідчить таблиця 4, ранг важливості об'єкта (від 1 до 10) прямо залежить від здатності витримувати вогневий вплив різних видів засобів ураження та кількості залучення боєприпасів для її ураження. Враховуючи намір та мету вогневого впливу на противника, а також можливі наслідки такого впливу, пропонується прийняти до оцінювання фактор *ефекту*, який буде посідати одне з основних місць у процесі оцінювання об'єкта (групи об'єктів) під час використання матриці CARVER і він тісно пов'язаний з показником критичності об'єктів [10–12]. Ефект вогневого впливу є мірою можливих військових, політичних, економічних, психологічних і соціологічних впливів не лише на об'єкт, а й за його межами. Тип і величина бажаних ефектів допоможуть у процесі планування вогневої підтримки вибрати об'єкт та його основні елементи для атаки. Ефект у цьому контексті стосується всіх значних ефектів, бажаних чи ні, які можуть виникнути після атаки на вибраний об'єкт ураження.

Наприклад, основним ефектом знищення двох суміжних радіолокаційних станцій великої дальності в системі раннього попередження (система протиповітряної оборони (далі – ППО) або протиракетної оборони (далі – ПРО) може бути відкриття діри в системі, яка має достатній розмір і тривалість, щоб дозволити засобам ракетних військ або повітряного нападу застосувати успішний повітряний або ракетний удар по найбільш важливим об'єктам в системі оперативної побудови військ противника. Ефекти також можуть включати:

ініціювання контрзаходів;

небоєздатність сил і засобів;

репресії проти мирного населення;

побічний збиток для інших об'єктів.

Можливі наслідки можуть бути гіпотетичними і мають бути позначені як припущення. Наслідки однієї атаки можуть бути досить різними на тактичному, оперативному та стратегічному рівнях. Наприклад, руйнування підстанції може не вплинути на місцеве електропостачання, але припиняє все живлення сусіднього регіону. Тому даний фактор часто відіграє одну з важливих ролей у прийнятті військових рішень [12]. Враховуючи зазначене, рекомендується здійснити ранжування цих критеріїв, які в подальшому будуть враховуватись під час оцінювання об'єктів противника, що будуть прийматись як можливі цілі для вогневої підтримки. Так, у таблиці 5 наведено ранжування критеріїв ефекту від ураження об'єктів противника.

Як показує таблиця 5, ранг важливості об'єкту (від 1 до 10) буде збільшуватися залежно від ефекту на результати операції, який буде прогнозуватися від ураження зазначеного об'єкту противника. Також, значущим є те, наскільки давно та якими засобами розвідки було розвідано об'єкт противника. Ця інформація буде свідчити про достовірність розвідувальної інформації щодо об'єкту ураження. Тому пропонується також враховувати фактор *розпізнаваності* цілі під час застосування матриці CARVER. Цей фактор являє собою ступінь, до якого об'єкт може бути розпізнаний різними засобами розвідки, в першу чергу, засобами артилерійської розвідки, за різних умов [11; 15–16]. Погода має очевидний і значний вплив на видимість об'єктів ураження, які не виявляють себе активним випромінюванням або звуковим та хвильовим випромінюванням. Дощ, сніг і ґрунтовий туман можуть заважати спостереженню. Відрізки доріг з рідкісною рослинністю та прилеглі височини створюють чудові умови для хорошого спостереження. Слід також враховувати відстань, світло та пору року.

Таблиця 5

Ранжування критеріїв ефекту від ураження об'єктів противника

Критерії ефекту (від ураження об'єкта)	Ранг важливості
Дасть максимально можливий позитивний ефект на результати операції.	10
Дасть позитивний ефект на результати операції.	9
Дасть позитивний ефект на окремі етапи операції.	8
Дасть посередній ефект на результати операції.	7
Дасть незначний позитивний ефект на загальну обстановку в районі бойових дій.	6
Не дасть істотного позитивного ефекту на загальну обстановку в районі бойових дій.	5
Не призведе позитивних ефектів на етапи операції, надмірне використання ресурсу.	4
Мало значних позитивних ефектів, можливий негативний вплив на операцію.	3
Не дасть позитивних ефектів, прогнозуються негативні ефекти від його ураження.	2
Не дасть істотних позитивних ефектів для операції, прогнозуються негативні ефекти.	1

Інші чинники, що впливають на розпізнавання, включають розмір і структурну складність цілі, присутність її характерних ознак, наявність маскування або камуфляжу, а також технічну складність і підготовку фортифікаційного обладнання. Факт активного радіовипромінювання з місця розташування об'єкта ураження, може свідчити про його непереміщеність та присутність у зоні попереднього розвідування.

Отже, враховуючи вид розвідки, яким було розвідано об'єкт, час який пройшов від його виявлення та певні погодні умови, пропонується здійснити ранжування критеріїв упізнаваності, які в подальшому будуть враховуватися під час загального оцінювання об'єктів ураження за матрицею CARVER. Так, у таблиці 6 наведено ранжування критеріїв упізнаваності об'єктів противника.

Як свідчить таблиця 6, ранг важливості об'єкту (від 1 до 10) залежить від якості виду розвідки, яким він був розвіданий, достовірності розвідувальних даних про нього та можливість спостереження в реальному часі, що в свою чергу дасть можливість спостерігати за результатами вогневого впливу на даний об'єкт противника.

Для прикладу, розглянемо визначення пріоритетності вибору об'єктів ураження в ході оборонної операції в смузі оборони оперативно-тактичного угруповання військ [20]. Так, припустимо, що силами і засобами всіх видів розвідки в смузі оборони оперативно-тактичного угруповання військ розвідано 10 таких типів об'єктів ураження противника на глибину ураження засобами далекобійної артилерії та РСЗВ середньої дальності («Ураган») до 25 км:

командний пункт бригади;

командний пункт батальйону;

взвод 220-мм РСЗВ на вогневій позиції;

батарея 152-мм гармат на вогневій позиції;

батарея 120-мм мінометів на вогневій позиції;

ЗРК системи ППО С-300В;

станція радіоелектронної боротьби «Житель»;

радіолокаційна станція польової артилерії (Зоопарк-1М);

мотострілецький взвод батальйону 1 ешелону;

танковий взвод батальйону 1 ешелону.

Таблиця 6

Ранжування критеріїв упізнаваності об'єктів противника

Критерії впізнаваності	Ранг важливості
Чітко спостерігається засобами розвідки, всі елементи об'єкта згруповані.	10
Спостерігається засобами розвідки в даний час або раніше, об'єкт продовжує свою діяльність в даному районі.	9
Розвідано джерелом артилерійської розвідки, об'єкт виявляє себе різного роду випромінюванням.	8
Розвідано з високим ступенем надійності, характерні ознаки стверджують, що об'єкт не змінив місця.	7
Розвідано з терміном до 1 год, малорухомий, з можливістю переміщення. можлива дорозвідка.	6
Розвідано терміном до 3 годин, окремі елементи змінені на місцевості, маломаневрений.	5
Розвідано агентурною розвідкою, складні погодні умови заважають надійності розвідки.	4
Розвідано нещодавно, маневрений, відсутність дорозвідки або можливість дезінформації.	3
Розвідано з тривалим терміном, погодні умови не дають ідентифікувати об'єкт.	2
Розвідано давно, розвідувальних ознак не виявляє, можливе переміщення об'єкту.	1

Враховуючи вихідні дані прикладу, що розглядається, на основі досвіду авторів, методом експертних оцінок було оцінено кожен тип об'єктів ураження противника. Результати роботи експертів усереднені та округлені до цілого числового значення наведено в таблиці 7.

Таблиця 7

Результати оцінювання експертами об'єктів противника, як можливих цілей для подальшого їх ураження

Приклад застосування системи матриці CARVER							
Цільова система	C	A	R	V	E	R	Загальна
Командний пункт бригади	9	7	7	8	10	6	47
Командний пункт батальйону	8	6	7	8	9	6	45
Взвод 220-мм Реактивних систем залпового вогню на вогневій позиції	8	5	7	6	7	6	39
Батарея 152-мм причіпної гармати на вогневій позиції	7	5	6	5	7	6	36
Мінометна батарея на вогневій позиції	5	6	5	5	5	5	31
Приклад застосування системи матриці CARVER							
Цільова система	C	A	R	V	E	R	Загальна
Зенітний ракетний комплекс С-300В	7	5	8	6	6	7	39
Станція радіоелектронної боротьби «Житель»	6	7	9	6	6	7	41
Радіолокаційна станція «Зоопарк-1М»	7	7	9	8	7	8	46
Мотострілецький взвод 1 ешелону	5	8	3	4	4	4	28
Танковий взвод 1 ешелону	6	7	3	2	3	4	25

Поточна методологія CARVER має прогалини в здатності визначати пріоритети в області критеріїв. Підхід, який пропонується, дозволяє усунути погрішності даної методології завдяки здатності командира (групи об'єднаної вогневої підтримки) зважувати критерії за допомогою методу попарного порівняння. В таблиці 7, відображено підсумкову суму рядків, що використовуються для визначення пріоритетності (ранжування) альтернативних об'єктів. Це такі:

командний пункт бригади – 47;

командний пункт батальйону – 45;

взвод 220-мм РСЗВ на вогневій позиції – 39;

батарея 152-мм гармат на вогневій позиції – 36;

батарея 120-мм мінометів на вогневій позиції – 31;

зенітний ракетний комплекс системи протиповітняної оборони С-300В – 39;

станція радіоелектронної боротьби «Житель» – 41;

радіолокаційна станція польової артилерії (Зоопарк-1М) – 46;

мотострілецький взвод батальйону 1 ешелону – 28;

танковий взвод батальйону 1 ешелону – 25;

У цьому методі передбачено, що всі критерії CARVER є рівно вагомими. З погляду аналітики, суттєвим недоліком є припущення про рівноважність вагомості того, що всі фактори у матриці CARVER однаково зважені відділом об'єднаної вогневої підтримки та мають коефіцієнти важливості в критеріях.

Таке ствердження полягає в тому, що майже у всіх операціях (бойових діях) ці елементи критеріїв насправді не будуть рівноцінними. А якщо вони не рівні, тоді відділ об'єднаної вогневої підтримки має призначати ваги відповідно до вказівок командира щодо завдання операції або визначити коефіцієнт важливості кожного критерію за відповідним математичним апаратом.

Методи визначення коефіцієнтів важливості та схеми зважування, що поширені в науковій

літературі, є занадто складними. Водночас, завдання з цілевиявлення мають часові обмеження і більша частина методик є громіздкими. Разом із тим, використання ймовірностей, які можуть бути не своєчасними, може не відобразити намір командира (начальника відділу об'єднаної вогневої підтримки).

Прийняття рішення за численними атрибутами – це структурований процес ранжування альтернатив порядку за допомогою набору критеріїв і ваги, наданої цим критеріям. Тому, для пришвидшення процесу визначення коефіцієнтів важливості (вагових коефіцієнтів) на основі контексту ситуації пропонується використання шкали попарних порівнянь, що описана Сааті [8].

Метод попарного порівняння Сааті є одним із найпоширеніших методів [2–3; 7], що використовуються в дослідженнях стосовно прийняття рішення, тому виваження таких рішень пропонується здійснювати методом аналізу ієрархій. Тоді, для врахування ваги кожного критерію матриці CARVER проаналізуємо кожний з них за допомогою методу аналізу ієрархій. Суть методу складається в наступному. Для того щоб вирішити проблему, в нашому випадку, пропонується надати кожному критерію свій коефіцієнт важливості. Виходячи з цих коефіцієнтів, здійснюється обчислення значень вагового показника розвіданих об'єктів противника, які підлягають ураженню вогневими засобами [13]. Для цього сформуємо спочатку матрицю попарних порівнянь для рівня 2. У цій матриці визначається важливість кожного з критеріїв відповідно до шкали відносної важливості, яка буде застосована, згідно з матрицею показаною з в табл.8.

Таблиця 8

Матриця експертних оцінок (парних порівнянь)

Елементи	$П_1$	$П_2$	…	$П_k$	…	$П_m$
$П_1$	1	φ_1/φ_2	…	φ_1/φ_k	…	φ_1/φ_m
$П_2$	φ_2/φ_1	1	…	φ_2/φ_k	…	φ_2/φ_m
…	…	…	1	…	…	…
$П_k$	φ_k/φ_1	φ_k/φ_2		1	…	φ_k/φ_m
…	…	…	…	…	1	…
$П_m$	φ_m/φ_1	φ_m/φ_2		φ_m/φ_k	…	1

Матриця парних порівнянь має властивість оберненої симетричності:

$$\frac{\varphi_i}{\varphi_j} - \frac{1}{\varphi_i/\varphi_j}; при \quad i = j \frac{\varphi_i}{\varphi_j} - 1 \qquad (1)$$

Матрицю попарних порівнянь пропонується заповнювати або кожним експертом індивідуально, або на підставі консенсусу між експертами. В першому випадку результати заводяться до матриці на підставі середнього геометричного. Де відношення φ_k/φ_m пропонується визначати за формулою:

$$\varphi_k \Big/ \varphi_m = \sqrt[P]{\prod_p \left(\varphi_k/\varphi_m\right)_p}; \quad p = \overline{1,P} \qquad (2)$$

де, φ_k/φ_m – судження p-го експерта;

P – кількість експертів.

Заповнення числових значень до матриці попарних порівнянь здійснюється з використанням шкали рівня переваги в попарних порівняннях (шкали Сааті) [8], яка наведена в таблиці 9.

Таблиця 9

Шкала рівня переваги в попарних порівняннях (шкала Сааті)

Рівень переваги	Визначення	Пояснення
1	Відсутність переваги	Внесок альтернатив до цілі однаковий
2	Слабка перевага	
3	Посередня перевага	Досвід та судження незначно сприяють одній з альтернатив над іншою
4	Більш ніж посередня перевага	
5	Значна перевага	Досвід та судження значною мірою підтримують перевагу однієї з альтернатив над іншою
6	Більш ніж значна перевага	
7	Вагома або продемонстрована перевага	Вагома перевага на користь однієї з альтернатив, її домінування продемонстровано на практиці
8	Надто вагома перевага	
9	Екстремальна перевага	Докази, що сприяють одній з альтернатив над іншою є найвищим можливим порядком підтвердження
1,1–1,9	Значення, близькі до відсутності переваги	Коли альтернативи дуже близькі, додавання знаків після коми дозволяє показати наявність різниці

Окремі значення критеріїв матриці CARVER зважуються відносно до змінних середовища та мети операції (бойових дій), начальник центру об'єднаної вогневої підтримки (командир структурного підрозділу управління) може сформувати важливість критеріїв на основі своїх пріоритетів і прийняти більш обґрунтоване рішення. Начальник центру (командир) може підкреслити певні критерії на основі пріоритетів, тобто критичності над доступністю або вразливістю. Начальник центру (командир) також може зменшити акцент на критеріях, які не є такими доречними через можливості, а саме впізнаваність менше ніж здатність до відновлювання. Критерії ваги залежатимуть від контексту та базуватимуться на можливостях, що доступні начальнику (командиру). В таблиці 10, на основі досвіду авторів, надані значення попарних рішень для критеріїв у матриці CARVER.

Обчислюємо вектори пріоритетів для матриці попарних порівнянь. Для чого із групи матриць попарних порівнянь формується набір локальних пріоритетів, які виражають відносний вплив безлічі елементів на елемент верхнього рівня. Знайдемо відносну величину кожного окремого об'єкта через рішення матриць, кожна з яких володіє зовнішньосиметричними властивостями. Для цього обчислимо безліч власних векторів для кожної матриці, а потім нормалізуємо результат до одиниці, одержуючи тим самим вектор пріоритетів [13].

Таблиця 10

Матриця експертних оцінок (парних порівнянь)

Критерії	Критичність	Доступність	Відновлення	Вразливість	Ефект	Впізнаваність
Критичність	1	6	3	6	2	5
Доступність	1/6	1	1/4	1	1/5	1/2
Відновлення	1/3	4	1	4	1/2	3
Вразливість	1/6	1	1/4	1	1/5	1/3
Ефект	1/2	5	2	5	1	4
Впізнаваність	1/5	2	1/3	3	1/4	1

Для визначення важливості кожного критерію пропонується обчислювати власний вектор матриці оцінок. Для чого компоненти рядків матриці перемножуються і потім добувається корінь р-го ступеня, за формулою:

$$\alpha_i = \sqrt[p]{\frac{\varphi_1}{\varphi_1} \times \frac{\varphi_1}{\varphi_2} \ldots \frac{\varphi_1}{\varphi_m}}; \qquad (3)$$

Далі здійснимо нормування геометричних середніх (визначається оцінка вектора пріоритетів):

$$b_i = \frac{a_i}{\sum_i a_i}; \; i = \overline{l,m}; \; \sum_i b_i = 1; \qquad (4)$$

Обчислення оцінок векторів пріоритетів за формулами (3), (4) з точністю до четвертого знаку дали наступні результати, що наведені в таблиці 11.

Таблиця 11

Оцінки векторів пріоритетів

b_i	b_1	b_2	b_3	b_4	b_5	b_6
Значення	0.3892	0.0489	0.1718	0.0456	0.2617	0.0828

Проведемо перевірку за формулою:

$$\sum_{i=1}^{n} x_i = 1 \qquad (5)$$

$$\sum_{i=1}^{n} x_i = 0,3892 + 0,0489 + 0,1718 + \\ + 0,0456 + 0,2617 + 0,0828 = 1$$

Методом адаптивних ваг з використанням простих алгоритмів проведемо визначення рангів важливості кожного критерію визначимо ваговий коефіцієнт кожного об'єкта ураження помноживши значення кожного критерію на його відповідну вагу (табл. 12).

Таблиця 12

Матриця CARVER з урахуванням рангів кожного критерію

Зразок застосування стратегічної системи матриці CARVER								
Цільова система\ коеф. критерію	C	A	R	V	E	R	Середнє значення	Рейтинг
	0,3892	0,0489	0,1718	0,0456	0,2617	0,0828		
КП бригади	9	7	7	8	10	6	7,8333	1
	3,5028	0,3423	1,2026	0,3648	2,617	0,4968	8,5263	1
КП батальйону	8	6	7	8	9	6	7,5000	3
	3,1136	0,2934	1,2026	0,3648	2,3553	0,4968	7,8265	2
взв 220-мм РСЗВ на ВП	8	5	7	6	7	6	6,5000	5
	3,1136	0,2445	1,2026	0,2736	1,8319	0,4968	7,1630	4
батр 152-мм ПГ на ВП	7	5	6	5	7	6	6,0000	7
	2,7244	0,2445	1,0308	0,228	1,8319	0,4968	6,5564	7
мінбатр на ВП	5	6	5	5	5	5	5,1666	8
	1,946	0,2934	0,859	0,228	1,3085	0,414	5,0489	8
ЗРК С-300В	7	5	8	6	6	7	6,5000	5
	2,7244	0,2445	1,3744	0,2736	1,5702	0,5796	6,7667	5
ст. РЕБ «Житель»	6	7	9	6	6	7	6,8333	4
	2,3352	0,3423	1,5462	0,2736	1,5702	0,5796	6,6471	6
РЛС «Зоопарк-1М»	7	7	9	8	7	8	7,6666	2
	2,7244	0,3423	1,5462	0,3648	1,8319	0,6624	7,4720	3
мсв 1 ешелону	5	8	3	4	4	4	4,6666	9
	1,946	0,3912	0,5154	0,1824	1,0468	0,3312	4,4130	9
тв 1 ешелону	6	7	3	2	3	4	4,1666	10
	2,3352	0,3423	0,5154	0,0912	0,7851	0,3312	4,4004	10

Зміст абревіатур у таблиці: КП – командний пункт; ВП – вогнева позиція; ПГ – причіпна гармата; ЗРК – зенітний ракетний комплекс; РЕБ – радіоелектронна боротьба; РЛС – радіолокаційна станція; *батр* – батарея; *мінбатр* – *мінометна батарея мсв* – мотострілецький взвод; *тв* – танковий взвод.

В нашому випадку, група експертів у складі 9 осіб органу об'єднаної вогневої підтримки оперативної ланки визначила вектори локальних пріоритетів критеріїв матриці «CARVER» з наступними ваговими коефіцієнтами:

Критичність	0,3892
Доступність	0,0489
Відновлення	0,1718
Вразливість	0,0456
Ефект	0,2617
Впізнаваність	0,0828

Провівши обчислення критеріїв важливості з урахуванням оцінок векторів пріоритетів кожного критерію, спостерігаємо зміну середнього значення вагового коефіцієнту кожного типу об'єктів противника, що, в свою чергу, змінює пріоритетність їх ураження в ході вогневої підтримки. Зміни середніх значень та рейтингу об'єктів наведені на рис. 1, де в лівій частині наведено значення кожного типу об'єктів при однакових коефіцієнтах кожного критерію матриці CARVER, а в правій частині – з коефіцієнтами відповідно до векторів пріоритетів для кожного критерію.

Проаналізувавши графік, показаний на рисунку 1, що відображає зміни коефіцієнтів важливості між загальним значенням матриці CARVER та значенням з врахуванням ваги кожного критерію, можна зробити висновок, що врахування ваги критеріїв методом попарних порівнянь значно впливає на пріоритет об'єктів в угрупованні противника. Крім того, після врахування векторів локальних пріоритетів матриці, об'єкти в угрупованні противника, які взято до ураження, значно змінили своє місце в таблиці пріоритетності. Так, коефіцієнт пріоритету РЛС «Зоопарк-1М» збільшився та випередив КП батальйону. Коефіцієнти пріоритету взводу 220-мм РСЗВ на вогневій позиції та зенітного ракетного комплексу С-300В, у цьому випадку теж збільшились з випередженням значень для станції РЕБ «Житель». В свою чергу, танковий та мотострілецький взводи батальйону 1 ешелону під час розрахунків практично зрівняли свої показники пріоритетності.

Отже, провівши розрахунки за допомогою наведеної методики стає очевидною зміна рейтингу пріоритетності об'єктів противника, як можливих цілей, для подальшого їх ураження від початкового вагового рейтингу.

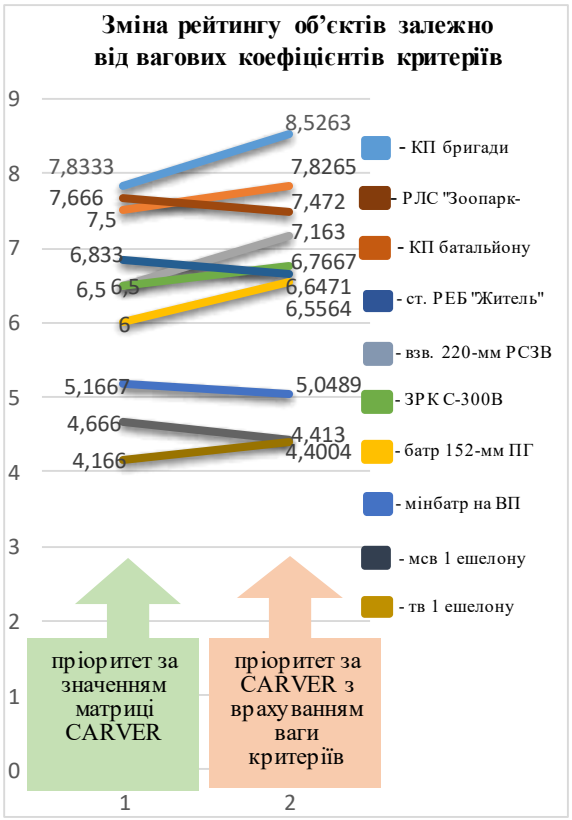


Рисунок 1 – Зміна рейтингу об'єктів залежно від вагових коефіцієнтів критеріїв

Висновки й перспективи подальших досліджень

Використання розробленої методики визначення пріоритетності об'єктів противника для прийняття їх як можливих цілей з метою подальшого ураження під час вогневої підтримки, використовуючи матрицю CARVER для визначення пріоритетів об'єктів, з урахуванням таких факторів як критичність, доступність, здатність до відновлення, вразливість, ефект і впізнаваність, на практиці забезпечує використання обмежених ресурсів для досягнення цілей на всіх рівнях військового управління.

Перспективами подальших досліджень є вивчення ефективності використання матриці CARVER під час реальних бойових операцій, а також можливість її інтеграції з іншими передовими інструментами і технологіями прийняття рішень (штучний інтелект, нейронні мережі тощо) в умовах впливу на них людських факторів і ситуаційної обізнаності.

Список бібліографічних посилань

1. Приміренко В. М., Дем'янюк А. В. Методологічний підхід визначення пріоритетності ураження цілей на основі визначення важливості критеріїв матриці CARVER. *Науково-практична конференція* : зб. мат. НПК м. Львів, 17 листопада 2022 р. Львів: НАСВ, 2022. С. 108. **2. Олійник В. В., Данилюк І. А.,** Оцінювання важливості об'єктів противника в ході планування рейдових дій з використанням методу аналізу ієрархії. *Сучасні інформаційні технології у сфері безпеки та оборони.* Київ, 2020. Вип.2 (38). С. 107–112.

DOI: 10.33099/2311-7249/2020-38-2-107-112.
3. Сааті Р. В. Процес аналізу ієрархії – що це таке і як він використовується. *Математична модель* 1987; 9: С. 161-176. DOI: 10.1016/0270-0255(87)90473-8. **4. Пеніваті К.** Критерії оцінки групового прийняття рішень. *Математичні комп'ютерні моделі.* 2007. Вип. 46: С. 935–947, DOI:10.1016/j.mcm.2007.03.005. **5. Репіло Ю., Абед А., Животовський Р., Шишацький А., Гогонянц С., Кравченко С., Живило І., Дєнєжкін М., Протас Н., Щепцов О.** Удосконалення методу оцінювання та прогнозування стану об'єкта моніторингу в інтелектуальних системах з підтримкою прийняття рішень. *Східно-Європейський журнал підприємницьких технологій*. 2021. Вип. 3(112), С. 43-55, DOI: 10.15587/1729-4061.2021.237996. **6. Гао Ш, Жанг З., Као Ч.** Методи обчислення ваг з використанням повних і неповних матриць. *Журнал Програмне забезпечення* 2010. № 5: С. 304–311. DOI: https://doi.org/10.4304/ jsw.5.3.304-311 **7. Сонг Б., Кан С.** Метод призначення ваг за допомогою ранжування та неієрархічного порівняння. Adv Decis Sci. 2016. Article ID 8963214, С. 107-119. DOI:10.1155/2016/8963214. **8. Сааті Т.** Аналітичний процес ієрархії. Нью-Йорк: *McGraw-Hill Book Company*, 1980. С. 104. **9. Фокс В., Томпсон Н**. Поетапне виявлення терористичних атак: спрощення складності за допомогою аналітичного процесу ієрархії. *Журнал управління обороною*, 2014. № 5. С. 57–64. DOI: 10.4172/2167-0374.1000116 **10. Гердес Дж., Сперо Е.** Компактний огляд багатокритеріальних методів аналізу невизначеності рішень. ARL-TR-6340. *Армійські науково-дослідні лабораторії.* 2013. С. 30. URL: https://apps.dtic.mil/sti/tr/pdf/ADA582195.pdf. (дата звернення 18.01.2023). **11. Штаб**, управління армії. FM 34–36: Операції розвідки Сил спеціальних операцій та радіоелектронної боротьби, Додаток D, 1991. 212 с. **12. Лабай Л., Бенсі Л.** The CARVER. Цільовий аналіз і методологія оцінки вразливості: практичний посібник для оцінки вразливості безпеки. 2018, 188 с. **13. Грейвер Б., Реабе Л., Фокс В., Баркс Р.** CARVER 2.0: інтеграція багатоатрибутної схеми зважування процесу прийняття рішень аналітичного ієрархічного процесу для аналізу вразливості центру ваги для сил спеціальних операцій США. *Журнал оборонного моделювання та симуляції*, 2018. № 15. С. 111–120. DOI: 10.1177/1548512917717054 **14. Алінежад А., Аміні А.** Аналіз чутливості техніки TOPSIS: результати зміни ваги одного атрибута в підсумковому рейтингу альтернатив. *Журнал оптимізації в промисловому машинобудуванні*, 2011. № 7. С. 23–28. **15. Фокс В.** TOPSIS в бізнес-аналітиці. *Енциклопедія бізнес-аналітики та оптимізації.* 2014. С. 1762–1771. URL:https://www-users.york.ac.uk/~vjh5/myPapers/hodge%20article_wang_ency_2014.pdf. (дата звернення: 03.02.2023). **16. Гайджинасс.** Матриця CARVER: Тактичний аналіз цілей, URL: https://gaijinass.com/2010/03/11/carver-matrix-tactical-target-analysis/, 2010. (дата звернення: 24.02.2023). **17. Гайджинасс.** Використовуйте матрицю CARVER для керування. 2009.URL:https://gaijinass.com/2009/09/07/use-the-carver-matrix-for-management/. (дата звернення: 18.01.2023). **18. Ріман О., Приміренко В., Цвєтков Є.** Організація планування вогневої підтримки на тактичному рівні. *Навчальний посібник,* 2023. Київ. С. 26–27. **19. Баранов С., Таранець С.** Грім з небес. Вплив застосування підрозділів РВіА на результати бойових дій., Київ, 2023, 16 с. URL: https://sprotyvg7.com /ua/wp-content/uploads/2023/03//grim_z_nebes-1_spr.pdf (дата звернення 16.04.2023). **20. Оперативно**-стратегічне завдання для проведення командно-штабної воєнної гри зі слухачами випускних курсів Національного університету оборони України. Київ : НУОУ, 2021. 102 с.

THE METHODOLOGY FOR PRIORITIZING ENEMY TARGETS FOR ACCEPTANCE AS POSSIBLE TARGETS FOR FIRE SUPPORT USING THE CARVER MATRIX

Repilo Iurii ***(Doctor of Military Sciences, Professor)***
Prymirenko Volodymyr ***(candidate of military sciences)***
Demianiuk Andrii

National Defence University of Ukraine, Kyiv, Ukraine

It is known that in the course of fire support, munitions and resources are always less than necessary to destroy all identified enemy targets. Based on this, the task of prioritizing enemy targets that can be further identified as targets for destruction in order to ensure the efficient use of limited resources becomes extremely relevant. The article describes a methodology for prioritizing enemy objects for acceptance as possible targets for fire support using the CARVER matrix. The essence of the methodology is to analyze enemy targets for their potential impact on the fulfillment of the tasks of destroying them with artillery fire. Unlike the existing ones, it provides for the evaluation of enemy targets based on multiple criteria, which ensures the efficient use of limited resources. This makes it possible to identify objects as important targets for further making informed decisions on the priority of their destruction. The use of the proposed methodology for prioritizing enemy objects for acceptance as possible targets for fire support using the CARVER matrix by prioritizing targets based on factors such as criticality, availability, recovery capability, vulnerability, effect and recognizability, in practice, allows to ensure the use of limited resources to achieve goals in all levels of military command. In writing this article, the methods of expert evaluation, hierarchy analysis, and the theory of criteria importance were used. This methodological approach is further planned as a component of the decision support methodology for the combat use of artillery based on the use of geographic information technologies and artificial intelligence. This, in turn, makes it possible to increase the effectiveness of artillery combat employment by reducing the time for making

decisions on the combat use of artillery during fire support of combined arms formations and ensuring the use of limited resources to achieve goals in all levels of military command and control.

Keywords: *priority, matrix CARVER, operation, combat, fire support, missile and artillery units, importance rank, Saaty scale, expert evaluation matrix, criteria weighting methodology.*

References

1. Prymirenko, V., Demianiuk, A., (2022). Methodological approach to determining the priority of hitting targets based on determining the importance of CARVER matrix criteria. *Scientific and practical conference: coll. mate*., 1(39), 108. **2. Oliynyk, V. V., Danyliuk, I. A.,** (2020). Estimating the importance of enemy objects during raid planning using the hierarchy analysis method. Modern information technologies in the field of security and defense. 2 (38). 107–112 DOI: https://doi.org/10.33099/2311-7249/2020-38-2-107-112. **3. Saaty, R. W.**, (1987). The analytic hierarchy process—what it is and how it is used. *Math Model*; 9: 161–176. DOI: https://doi.org/10.1016/0270-0255(87)90473-8. **4. Peniwati, K.** (2007). Criteria for evaluating group decision making. *Math Comput Model*; 46, 935–947. DOI:10.1016/j.mcm.2007.03.005. **5. Repilo, I., Abed, A., Zhyvotovskyi, R., Shyshatskyi, A., Hohoniants, S., Kravchenko, S., Zhyvylo, I., Dieniezhkin, M., Protas, N., Shcheptsov, O.,** (2021) Improvement of the method of estimation and forecasting of the state of the monitoring object in intelligent decision supported systems. Eastern-European Journal of Enterprise Technologies, 3(112), 43-55, DOI: https://doi.org/10.15587/1729-4061.2021.237996. **6. Gao, S, Zhang, Z, Cao, C.,** (2010). Calculating weights methods using complete matrices and incomplete matrices. J Software; 5, 304–311. DOI: https://doi.org/10.4304/jsw.5.3.304-311. **7. Song, B, Kan, S.,** (2016). A method of assigning weights using a ranking and nonhierarchical comparison. *Adv Decis Sci*. 107-119. DOI:https://doi.org/10.1155/2016/8963214 **8. Saaty, T.,** (1980). The analytic hierarchy process. New York: *McGraw-Hill Book Company*, 1980. 104. **9. Fox, W., Thompson, N.,** (2014). Phase targeting of terrorist attacks: simplifying complexity with analytical hierarchy process. *Int J Decis Sci*, 5, 57–64. DOI: 10.4172/2167-0374.1000116. **10. Gerdes, J., Spero, E.,** (2013). A compact review of multi-criteria decision analysis uncertainty techniques. *Army Research Laboratories*, 2013, 64-72. [online] Available at:URL: https://apps.dtic.mil/sti/tr/pdf/ADA582195.pdf [Accessed : 18 January 2023]. **11. Headquarters**, Department of the Army, (1991). FM 34–36: Special Operations Forces Intelligence and Electronic Warfare Operations, Appendix D, 212. **12. Labaj, L., Bencie, L.,** (2018). The CARVER. Target Analysis and Vulnerability Assessment Methodology: A practical guide for Evaluatihg security Vulnerability, 188. **13. Greaver, B., Raabe, L., Fox, WP., Burks, RE.,** (2018). CARVER 2.0: integrating the Analytical Hierarchy Process's multi-attribute decision-making weighting scheme for a center of gravity vulnerability analysis for US Special Operations Forces. *The Journal of Defense Modeling and Simulation,* 15, 111-120. DOI:https://doi.org/10.1177/1548512917717054 **14. Alinezhad, A., Amini, A.,** (2011). Sensitivity analysis of TOPSIS technique: the results of change in the weight of one attribute on the final ranking of alternatives. *J Optimiz Ind Eng*, 7, 23–28. **15. Fox, W.,** (2014). TOPSIS in business analytics. *Encyclopedia of business analytics and optimization.* 2014, 1762-1771. [online] Available at: URL: https://www-users.york.ac.uk/~vjh5/myPapers/hodge%20article_wang_ency_2014.pdf/ [Accessed : 03 February 2023]. **16. *Gaijinass.*** (2010). CARVER Matrix: Tactical Target analysis, [online] Available at: URL:https://gaijinass.com/2010/03/11/carver-matrix-tactical-target-analysis/. [Accessed : 24 February 2023]. **17. *Gaijinass,*** (2009). Use the CARVER matrix for management, [online] Available at: URL:https://gaijinass.com/2009/09/07/use-the-carver-matrix-for-management/. [Accessed : 18 January 2023]. **18. Riman, O., Prymirenko, V., Tsvetkov, E.,** (2023). Organization of the fire support planning at the tactical level. *Training manual.* 2023, Kyiv, 117. **19. Baranov, S. M., Taranets, S. V.,** (2023). Thunder from Heaven. The impact of the use of RViA units on the results of hostilities. Kyiv, 16 [online] Available at: URL: https://sprotyvg7.com/ua/wp-content/uploads/2023/03/grim_z_nebes-1_spr.pdf **20. An operational**-strategic task for conducting a command and staff war game with students of the final courses of the National Defense University of Ukraine, (2021). Kyiv: NUOU, 102.

Шановні колеги!

Запрошуємо до участі в науковому журналі
«Сучасні інформаційні технології у сфері безпеки та оборони».
Видавець: Національний університет оборони України.
Наказом Міністерства освіти і науки України №409 від 17.03.2020 р. та №886 від 02.07.2020 р. журнал включено до Переліку наукових фахових видань України категорії «Б» в галузях «технічні науки» та «військові науки», спеціальності – 122, 124, 253, 255.

ВИМОГИ
до публікацій у журналі «Сучасні інформаційні технології у сфері безпеки та оборони» Національного університету оборони України

ОСНОВНІ ТЕМАТИЧНІ НАПРЯМИ ЖУРНАЛУ

1. Військова кібернетика та системний аналіз.
2. Протиборство у кіберпросторі.
3. Військово-космічні та геоінформаційні технології.
4. Інтелектуальні інформаційні технології і робототехніка в сфері безпеки та оборони.
5. Інформаційно-аналітична діяльність у сфері безпеки та оборони.
6. Розвиток теорії та практики створення інформаційно-телекомунікаційних систем.
7. Інтерактивні моделі розвитку науково-освітнього простору.
8. Високотехнологічні аспекти воєнного мистецтва.
9. Історичний дискурс розвитку високих оборонних технологій.
10. Стратегічні комунікації та когнітивні системи спеціального призначення

.

ЗАГАЛЬНА ІНФОРМАЦІЯ

Подавати статтю до журналу потрібно через сайт журналу (sit.nuou.org.ua) або через електронну пошту sitnuou@ukr.net, у текстовому форматі doc. Назва файлу має містити прізвища авторів (Наприклад, «Прізвище.doc»).

Обсяг статті має бути не менше 4 аркушів основного тексту (від розділу «Вступ» до розділу «Висновки і перспективи подальших досліджень» включно). В середньому кожен автор має опрацювати 2 сторінки основного тексту статті.

Одночасна подача роботи у декілька видань *заборонена*, оскільки вважається порушенням публікаційної етики.

Редколегія залишає за собою право відмови у публікації статті, що: не відповідає проблематиці журналу; не оформлена згідно з цими Вимогами; містить більше 35 % плагіату; не отримала позитивні відгуки за результатами незалежного рецензування; має більше 3-х осіб авторського колективу (у разі менше 6 сторінок основного тексту статті).

З питань оплати за публікацію статті потрібно звертатись до редакції журналу.

Обов'язковими етапами роботи редакційної колегії з опрацювання статей перед публікацією є:

перевірка на предмет дотримання вимог до редакційного оформлення згідно з державними стандартами України (ДСТУ 3008-2015 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»;

ДСТУ 8302:2015 «Бібліографічне посилання. Загальні положення та правила складання»;

ДСТУ 3582:2013 «Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила»;

перевірка тексту на дотримання вимог українського правопису згідно Постанови Кабінету міністрів України від 22 травня 2019 року № 437 «Питання українського правопису»;

здійснення редколегією внутрішнього та зовнішнього рецензування статей відповідно до Наказу МОН України від 15 січня 2018 року № 32 «Про затвердження Порядку формування Переліку наукових фахових видань України»;

перевірка статей на плагіат (пп. 5, 6, 7 ст. 28^1 Закону України «Про наукову і науково-технічну діяльність»;

ст. 53 Закону України «Про авторське право і суміжні права».

СТРУКТУРА І ВИМОГИ ДО ОФОРМЛЕННЯ СТАТТІ

Обсяг рукопису має становити від 4 до 20 аркушів основного тексту формату А4 українською або англійською мовами.

Рекомендована максимальна кількість джерел у Списку бібліографічних посилань до 20 позицій.

Під час роботи з текстовою частиною статті, заборонено: використовувати для форматування тексту (встановлення абзацу) пропуски, табуляцію тощо; встановлювати ручне перенесення слів; використовувати колонтитули; використовувати для набору формул графічні об'єкти, кадри й таблиці; розміщувати кольорові та фонові рисунки.

Основний текст статті набирати шрифтом Times New Roman, кегель 10, міжрядковий інтервал 1.

Рекомендовано викладати текст статті від третьої особи.

Формат аркуша: А4 (21 × 29,7 см).

Текстовий редактор: Microsoft Word.

Параметри сторінки (поля): зліва – 3 см; справа – 2 см; зверху – 2 см; знизу – 2 см.

National Defence University of Ukraine

СХЕМА-ЗРАЗОК ОФОРМЛЕННЯ СТАТТІ

DOI (*вирівнювання за лівим краєм, Arial, жирне пряме підкреслене накреслення, кегль – 11 пт*)

←— 1 пустий рядок – 10 пт

УДК (*вирівнювання за лівим краєм, Arial, жирне пряме підкреслене накреслення, кегль – 11 пт*)

←— 1 пустий рядок – 10 пт

Прізвище ім'я по-батькові 1-го автора ***(наукова ступінь, вчене звання)*** [1]
Прізвище ім'я по-батькові 2-го автора ***(наукова ступінь, вчене звання)*** [2]
(мовою статті, вирівнювання за лівим краєм, одинарний інтервал, Times New Roman, жирне курсивне накреслення, кегль – 11 пт (у дужках кегль – 8 пт))

←— 1 пустий рядок –10 пт

[1] Назва організації де працює 1-й автор, місто її розташування, країна
[2] Назва організації де працює 2-й автор, місто її розташування, країна
(мовою статті, вирівнювання за лівим краєм, одинарний інтервал, Times New Roman, жирне курсивне накреслення, кегль – 11 пт)

←— 1 пустий рядок – 10 пт

ЗАГОЛОВОК СТАТТІ *(мовою статті, вирівнювання за правим краєм, всі заголовні букви, одинарний інтервал, Arial, жирне пряме накреслення, кегль – 14 пт)*

←— 1 пустий рядок – 10 пт

Текст анотації (мовою статті, перший абзацний відступ – 1 см, далі без абзаців, вирівнювання за шириною, одинарний інтервал, Times New Roman, курсивне накреслення, кегль – 10 пт).

Ключові слова: *(мовою статті, перший абзацний відступ – 1 см, далі без абзаців, вирівнювання за шириною, одинарний інтервал, Times New Roman, жирне курсивне накреслення, кегль – 10 пт) слово 1, слово 2, слово 3…(мовою статті, без абзаців, вирівнювання за шириною, одинарний інтервал, Times New Roman, курсивне накреслення, розділяти комою, кегль – 10 пт).*

←— розрив розділу «Без розриву»

Далі текст статті розташовується за розділами і пишеться від третьої особи *(у два стовпчики шириною 7,75 см. Відстань між ними – 0,5 см. Текстівка статті подається мовою статті, з абзацами, абзацний відступ – 0,5 см, вирівнювання за шириною, одинарний інтервал, Times New Roman, пряме накреслення, кегль – 10 пт).*

Вступ

(вирівнювання по центру, жирне пряме накреслення, кегль – 12 пт)

Постановка проблеми. *(Жирне пряме накреслення, кегль – 10 пт).* Текстівка *(пряме накреслення, кегль – 10 пт).*

Аналіз останніх досліджень і публікацій. *(Жирне пряме накреслення, кегль – 10 пт).* Текстівка *(пряме накреслення, кегль – 10 пт).*

Мета статті (постановка завдань). *(Жирне пряме накреслення, кегль – 10 пт).* Текстівка *(пряме накреслення, кегль – 10 пт).*

Виклад основного матеріалу дослідження

(вирівнювання по центру, жирне пряме накреслення, кегль – 12 пт)

Текстівка *(пряме накреслення, кегль – 10 пт).*

Висновки

(вирівнювання по центру, жирне пряме накреслення, кегль – 12 пт)

Текстівка *(пряме накреслення, кегль – 10 пт)*

←— розрив розділу «Без розриву»

Список бібліографічних посилань

(вирівнювання по центру, жирне пряме накреслення, кегль – 12 пт)

Список бібліографічних посилань *(без абзаців, вирівнювання за шириною, з виділенням жирним накресленням номера за порядком, прізвищ та ініціалів авторів або назви документа, Times New Roman, кегль – 9 пт).*

Див. зразок оформлення на сайті sitnuou@ukr.net.

←— розрив розділу «Без розриву»

ARTICLE TITLE

(переклад англійською (українською) мовою, вирівнювання по центру, всі заголовні букви, Arial, жирне пряме накреслення, кегль – 10 пт)

←— 1 пустий рядок – 10 пт

Surname First name of the 1st author ***(academic degree, academic title)*** [1]
Surname First name of the 2nd author ***(academic degree, academic title)*** [2]
(переклад англійською (українською) мовою імен і прізвищ авторів та їхніх наукових даних, вирівнювання по центру, Times New Roman, жирне курсивне накреслення, кегль – 10 пт (у дужках кегль – 8 пт))

←— 1 пустий рядок – 10 пт

[1] Name of the organization where the 1st author works, city of its location, country
[2] Name of the organization where the 2nd author works, city of its location, country
(*переклад англійською (українською) мовою назв організацій, міста, країни, вирівнювання по центру, Times New Roman, жирне курсивне накреслення, кегль – 10 пт)*

←— 1 пустий рядок – 10 пт

Текст анотації (англійською (українською) мовою, перший абзацний відступ – 1 см, далі без абзаців, вирівнювання за шириною, Times New Roman, курсивне накреслення, кегль – 10 пт).

Keywords: *(переклад англійською (українською) мовою ключових слів за вимогами українського варіанту).*

←— розрив розділу «Без розриву»

References

(вирівнювання по центру, жирне накреслення, кегль – 12 пт)

Список «References» *(у стилі Harvard, назви джерел подаються англійською мовою. Інші елементи опису – у транслітерації, без абзаців, вирівнювання за шириною, з виділенням жирним накресленням номера за порядком, прізвищ та ініціалів авторів або назви документа, Times New Roman, кегль – 9 пт).*

Увага! *Остання сторінка статті заповнюється не менше ¾ її обсягу. У статті рекомендована парна кількість аркушів.*
На окремому аркуші українською та англійською мовами наводять відомості про авторів: прізвище, ім'я та по-батькові; посада повністю; вчена ступінь та вчене звання; ORCID; контактний телефон; електронна пошта.

Засновник і видавець Національний університет оборони України.
Св-во КВ № 20490-10290ПР. Адреса редакції: 03049, м. Київ, Повітрофлотський пр-т, 28. Тел. (044) 271-07-31.
Підписано до друку 21.08.2023. Формат 60×84 ⅛. Ум. друк. а. 21. Тираж 100 прим.
Надруковано у друкарні Національного університету оборони України.